DETERMINISTIC AND RANDOMIZED POLYNOMIAL-TIME APPROXIMATION OF RADII

ANDREAS BRIEDEN, PETER GRITZMANN, RAVINDRAN KANNAN, VICTOR KLEE, LÁSZLÓ LOVÁSZ AND MIKLÓS SIMONOVITS

Abstract. This paper is concerned with convex bodies in n-dimensional l_p spaces, where each body is accessible only by a weak separation or optimization oracle. It studies the asymptotic relative accuracy, as $n \to \infty$, of polynomial-time approximation algorithms for the diameter, width, circumradius, and inradius of a body K, and also for the maximum of the norm over K.

In the case of l_2 (Euclidean n-space), a 1987 result of *Bárány* and *Füredi* severely limits the degree of relative accuracy that can be guaranteed in approximating K's volume by any deterministic polynomial-time algorithm. This led to a similarly severe limit on the relative accuracy of deterministic polynomial-time algorithms for computing K's diameter. However, these limitations on the accuracy of deterministic computation were soon followed by the work of *Dyer*, *Frieze* and *Kannan* showing that, for volume approximation, arbitrarily good accuracy can be attained with the aid of suitable randomization. It was therefore natural to wonder whether the same is true of the diameter.

The first main result of this paper is that, in contrast to the situation for the volume, *randomization does not help in approximating the diameter.* The same limitation on accuracy that applies to deterministic polynomial-time computation still applies when randomization is permitted. This conclusion applies also to the width, circumradius, and inradius of a body, and to maximization of the norm over K.

The second main result is that, for each of the five "radius" measurements just mentioned, the inapproximability results for deterministic polynomial-time approximation are optimal for width and inradius when $1 \leqslant p \leqslant 2$, are optimal for diameter, circumradius, and norm-maximization when $2 \leqslant p \leqslant \infty$, and in the remaining cases are within a logarithmic factor of being optimal. In particular, all are optimal when $p = 2$. The optimality is established by producing deterministic polynomial-time approximation algorithms whose accuracy is bounded below by a positive constant multiple (independent of the dimension n) of the upper bounds on accuracy.

Since the bodies are assumed to be presented by a weak oracle, our approach belongs to the algorithmic theory of convex bodies initiated by *Grötschel*, *Lovász* and *Schrijver*. In the deterministic case we sharpen and extend l_2 results due to these authors, and in the randomized case we refine some ideas presented earlier by *Lovász* and *Simonovits*. The algorithms that establish lower bounds on accuracy use certain polytopal approximations of l_p unit balls that

[MATHEMATIKA, **48** (2001), 63–105]

are obtained by polarizing and extending an l_2 method of *Kochol*. The argumentation for upper bounds requires, in addition to extending the l_2 approach of *Bárány* and *Füredi*, a careful treatment of some results on entropy numbers used by *Carl* and *Pajor*. It is closely related to some questions concerning sphere coverings.

§0. *Introduction.* As the term is used here, a *convex body* (or simply *body*) in $\mathbb{R}^n$ is an n-dimensional compact convex set. The collection of all such bodies is denoted by $\mathscr{K}^n$. Though our main concern is with general bodies, a special role is played by bodies K that are 0-*symmetric*, meaning that $K = -K$. Translates of 0-symmetric bodies are simply called *symmetric*.

This paper arises from a general interest in the computation or approximation of important measurements of a body $K \in \mathscr{K}^n$ with respect to various norms. Here we consider K's diameter, width, circumradius, and inradius, and the maximum of $\|x\|$ as x ranges over K, and we use the general term *radii* to refer to all of these measurements. The l_p norms are of special interest, and in view of the applications described in [GK93], the focus is primarily on large (and variable) n. Hence our emphasis is on the computational complexity of these measurements for the case in which the dimension n is part of the input, and (since exact computation is in many cases $\mathbb{NP}$-hard) on the task of describing the rapidity with which the relative accuracy of the best polynomial-time approximation decreases as the dimension n increases.

The task of approximating radii is approached here in the realm of the *Algorithmic Theory of Convex Bodies* developed by Grötschel, Lovász and Schrijver [GLS93], and we make frequent use of results from that book. The theory applies not only to polytopes but to more general bodies as well. Bodies are assumed to be given by *oracles* that solve certain specified sorts of problems and can be used as subroutines by any algorithm. Using the binary Turing machine augmented by such oracles, an algorithm is called an *oracle-polynomial-time* algorithm if it is polynomial in the usual sense, with the understanding that the time required by each call to the oracle is only what is needed to write the call's question onto and read the oracle's answer from a tape of the Turing machine.

A 1987 result of Bárány and Füredi [BF87] showed (in the oracle model) that no deterministic polynomial-time algorithm can approximate the diameter or width of a body K in Euclidean n-space (l_2) with a relative error less than $O(\sqrt{n/\log n})$. From basic results in convex geometry it follows easily that this statement holds also for the other radii considered here. A first natural question raised by this result is whether the implied inapproximability bound on accuracy can be overcome if deterministic algorithms are replaced by randomized ones. This question is especially appropriate in view of the striking improvements in volume computation attained in [DFK89] and [KLS98] with the aid of randomization. It turns out that, while [BF87]'s upper bound on accuracy is easy to *attain* with the aid of the randomization, randomization *does not help to overcome the bound.* That is the main result of the first part of this paper.

The second main part of this paper is devoted to deterministic algorithms. It shows that, in l_2 spaces, the upper bound on accuracy can in fact be attained by deterministic algorithms, and that (with a lot of extra work) the underlying idea can be applied to arbitrary l_p-spaces for $1 \leqslant p \leqslant \infty$. The presented results on order of accuracy are all sharp (asymptotically optimal) when $p = 2$, are sharp for width and inradius when $1 \leqslant p \leqslant 2$, are sharp for diameter, circumradius, and norm-maximization when $2 \leqslant p \leqslant \infty$, and in the remaining cases are within a logarithmic factor of being sharp.

The stated results imply that, for computation of radii, in marked contrast to the situation for volume computation, the asymptotic relative accuracy of randomized algorithms is not superior to that of deterministic algorithms. However, it does turn out, as explained in a final section comparing the deterministic and randomized approaches, that the degree of the polynomial measuring the complexity of the algorithms can be improved when randomization is allowed.

Our algorithms arise from the observation that the oracle complexity of approximating the radii is closely related to the problem of covering a sphere with a prescribed number of caps, or, equivalently, of approximating a sphere with proper polytopes. This connection enables us to invoke basic results on the measure of caps, along with a construction of Kochol [Koc94].

Another way of viewing the results is that, rather than approximating the body K by another body (such as an ellipsoid in the approach of [GLS93]), 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 radii can be computed in polynomial time with arbitrary accuracy. This approach makes it possible, by using techniques of Carl and Pajor [Car85, CP88] involving entropy in Banach spaces, and combining these with a generalization of Kochol's construction, to obtain both lower and upper bounds on the accuracy of deterministic polynomial-time approximations of radii in an arbitrary finite-dimensional l_p space. These results yield quantitative information on how the error in polynomial-time approximation of radii is influenced by the extent to which a Minkowski space deviates from being polytopal.

Our main results are expressed in terms of *relative accuracy*, a function of the dimension n that describes, in terms of worst-case behaviour, how far an algorithm deviates from giving a precise measurement. For an exact algorithm, the accuracy is 1 in all dimensions. In most of the problems considered here, the accuracy approaches 0 as $n \to \infty$, and the problem is that of estimating the rapidity of this approach for the best possible oracle-polynomial-time algorithms. For more formal definitions, see Section 1.D.

Table 1 summarizes results obtained, in the paper's second main part, for the accuracy of deterministic oracle-polynomial-time approximations with respect to the l_p norm. There, p is either ∞ or an arbitrary rational number with $1 \leqslant p < \infty$, and p' is defined by the equation $1/p + 1/p' = 1$, where $1/\infty$ is defined to be 0. $\mathbb{DOP}$ indicates that a measurement can be deterministically approximated with arbitrary accuracy in oracle-polynomial time. (The reason for using $\mathbb{P}$ instead of P is simply that we usually use P to denote a polytope.)

Note that, in the Euclidean case, our estimate $\Theta(\sqrt{(\log n)/n})$ applies to all five of the measurements considered. As a lower bound, our $\Omega(\sqrt{\log n)/n})$

Table 1. Accuracy bounds for deterministic oracle-polynomial-time approximation of radii.

p	1	$1<p\leq 2$	$2\leq p<\infty$	∞
inradius, width	$\mathbb{DOP}$	$\Theta\left(\left(\frac{\log n}{n}\right)^{1/p'}\right)$	$\Omega\left(\frac{(\log n)^{1/p}}{n^{1/2}}\right)$	$\Omega\left(\frac{1}{n^{1/2}}\right)$
			$\Omega\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$
circumradius, diameter, norm-maximum	$\Omega\left(\frac{1}{n^{1/2}}\right)$	$\Omega\left(\frac{(\log n)^{1/p'}}{n^{1/2}}\right)$	$\Theta\left(\left(\frac{\log n}{n}\right)^{1/p}\right)$	$\mathbb{DOP}$
	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$		

improves the $\Omega(1/\sqrt{n})$ provided by Grötschel, Lovász, and Schrijver [GLS93] for approximating the circumradius and the diameter, and also improves their $\Omega(1/((n+1)\sqrt{n}))$ for the inradius and the width. For $p=2$, the upper bound $O(\sqrt{(\log n)/n})$ was already proved by Bárány and Füredi [BF87].

It should be re-emphasized that our focus is on the case of varying dimension—*i.e.*, the dimension n is part of the input—and on oracle-polynomial-time approximation algorithms in which the same polynomial bound on running time must apply *simultaneously to all* n. The results are dramatically different for the same approximation problems in an arbitrary fixed dimension, for then the problems can be solved with arbitrary accuracy. See [Gru93] for theoretical and [GMR94, GMR95] for additional computational results concerning the initial step of our algorithms—approximating l_p unit balls by polytopes.

Our section headings are below. Since the material of this paper may be of interest from several viewpoints, we have included an unusually long background section. However, some readers will be able to skip this entirely, and others, depending on their interests and knowledge, will want to skip parts of it. Specific suggestions appear at the beginning of the next section.

1. Background.
   - 1.A Convex geometry.
   - 1.B Some properties of l_p-spaces.
   - 1.C Oracles.
   - 1.D Accuracy.

2. Randomization does not help!
   - 2.A Bounds for the fractional covering number of the Euclidean sphere.
   - 2.B Randomized algorithms for approximating radii.
   - 2.C Inapproximability results for randomized approximation.

3. Deterministic approximation.
   - 3.A Solutions with respect to polytopal norms.
   - 3.B Approximation of l_p unit balls by polytopes.
   - 3.C Deterministic algorithms for approximating radii.
   - 3.D Entropy numbers, Rademacher type, and volume ratios.
   - 3.E Inapproximability results for deterministic approximation.

4. Randomized versus deterministic approximation—a comparison.

§1. *Background.* Workers in classical convex geometry may skip Subsection 1.A. Readers who are interested only in Euclidean spaces may skip Subsections 1.B and 3.D. Readers who are familiar with the oracular approach to convex bodies may skip Subsections 1.A, 1.C, and 1.D.

§1.A. *Convex geometry.* In the case of a general finite-dimensional normed space, the norm is denoted by $\|\cdot\|$, the unit ball by $\mathbb{B}$, and the unit sphere by $\mathbb{S}$. The ambient dimension is usually assumed to be n, and often the notation is simplified by not using any explicit index to indicate this. (Dimension indices are used mainly for emphasis, and to avoid confusion while working in two different dimensions at the same time.)

Our primary concern is the approximation of radii with respect to the classical l_p-norms. For $x=(\xi_1,\dots,\xi_n)^T\in\mathbb{R}^n$, these norms are given by

$$\|x\|_p=\left(\sum_{i=1}^{n}|\xi_i|^p\right)^{1/p},\qquad \text{for } 1\leqslant p<\infty,$$

$$\|x\|_\infty=\max_{1\leqslant i\leqslant n}|\xi_i|.$$

For computational reasons, attention is often restricted to rational values of p and to $p=\infty$. Thus it is convenient to elect ∞ as a special rational, and to agree that such phrases as "for rational $p\in[1,\infty]$" will refer to $p=\infty$ as well as to rational $p\in[1,\infty[$.

The unit ball and unit sphere of an l_p space are denoted by $\mathbb{B}_p$ and $\mathbb{S}_p$ respectively. Note that the balls $\mathbb{B}_1$ and $\mathbb{B}_\infty$ are polytopes. More generally, any full-dimensional 0-symmetric polytope P induces a *polytopal norm* $\|\cdot\|_P$ given by $\|x\|_P=\min\{\lambda\geqslant 0: x\in\lambda P\}$, and P is then the unit ball of the induced norm. If the polytope is $\mathcal{V}$*-presented* (given as the convex hull of its vertices—more precisely, a string $(n,m;v_1,\dots,v_m)$, with $n,m\in\mathbb{N}$ and $v_1,\dots,v_m\in\mathbb{Q}^n$, is given such that $P=\operatorname{conv}\{v_1,\dots,v_m\}$), or $\mathcal{H}$*-presented* (given as the intersection of closed halfspaces described by linear inequalities—more precisely, a string $(n,m;A,b)$ is given, where $n,m\in\mathbb{N}$, A is a rational $m\times n$ matrix, $b\in\mathbb{Q}^m$, and the set $P=\{x\in\mathbb{R}^n: Ax\leqslant b\}$ is bounded), the norm is denoted by $\|\cdot\|_{\mathcal{V}}$ or $\|\cdot\|_{\mathcal{H}}$ and the unit ball by $\mathbb{B}_{\mathcal{V}}$ or $\mathbb{B}_{\mathcal{H}}$.

The conjugate space, indicated by *, consists of all the linear functionals on the original space, and the norm of a functional is the maximum of its values on the unit ball. The *polar* K° of a body K is the set of all functionals f in the conjugate space such that $f(x)\leqslant 1$ for all $x\in K$.

With respect to the chosen norm and its unit ball $\mathbb{B}$, the *inradius* $r(K)$ of a body K is the radius of a largest ball that is contained in K, and the *circumradius* $R(K)$ is the radius of a smallest ball that contains K. The *width* $w(K)$ is the minimum of the distances between parallel supporting hyperplanes of K, and the *diameter* $d(K)$ is the maximum of the distances realized between two points of K. The maximum $N(K)$ of the norm on K is the smallest positive λ such that $K\subset\lambda\mathbb{B}$. For simplicity, we refer to all of these functions as *radii*. Furthermore, we often use an index to denote the underlying norm, *e.g.*, d_2 denotes the diameter defined with respect to the Euclidean norm.

In the case of polytopes, the complexity of radius computations depends heavily on the way in which the polytope is presented. For example, if a polytope K is (rationally) $\mathscr{V}$-presented, then finding the maximum of a given norm on K can be accomplished by evaluating a suitable monotone function of the norm at each vertex. On the other hand, when a polytope K is rationally $\mathscr{H}$-presented, computing the pth power of $\max_{x\in K}\|x\|_p$ is $\mathbb{NP}$-hard for each $p\in\mathbb{N}$, even for the special case in which K is a 0-symmetric n-parallelotope [BGKL90]. (Here there are 2^n vertices, but the $\mathscr{H}$-presentation requires only $2n$ inequalities.) Similar comments apply to other radius computations. Consider, for example, the problem of computing the square of a radius of a rationally presented symmetric polytope in an l_2 space. When "radius" means "diameter" or "circumradius", the problem is approximable with arbitrary accuracy in polynomial time for $\mathscr{V}$-presentations and is $\mathbb{NP}$-hard for $\mathscr{H}$-presentations, but the role of $\mathscr{V}$ and $\mathscr{H}$ is reversed when "radius" means "width" or "inradius" [GK94].

In the present paper, we deal with bodies more general than polytopes, and we approach them in terms of the oracles described in Section 1.C. In a sense, the oracular approach unifies the treatment of $\mathscr{V}$- and $\mathscr{H}$-polytopes.

We often use the following basic properties of the radii of a body K (see [GK92]).

PROPOSITION 1.1. *$w(K)\geq 2r(K)$ and $d(K)\leq 2R(K)$, with equalities when K is symmetric.*

PROPOSITION 1.2. *Width and diameter are invariant under central symmetrization, i.e., $w(K)=\frac{1}{2}w(K-K)$ and $d(K)=\frac{1}{2}d(K-K)$, where $K-K$ denotes the difference body of K.*

PROPOSITION 1.3. *If $K=-K$, then $r(K)\mathbb{B}\subset K\subset R(K)\mathbb{B}$.*

PROPOSITION 1.4. *If $K=-K$, then $R(K)r(K^\circ)=1$.*

In Euclidean space, the following theorem for circumscribed balls (see [Jun01, DGK63]) can be used by our approximation algorithms.

JUNG'S THEOREM. If $K\in\mathscr{K}$, then $\frac{1}{2}d_2(K)\leq R_2(K)\leq\sqrt{n/2(n+1)}\,d_2(K)$.

It follows that any approximation algorithm for the (Euclidean) diameter yields an only slightly worse approximation for the circumradius, and vice-versa. An analogous result holds for inscribed balls (see[Ste22]), but there the upper bound for the ratio of width and inradius is $O(\sqrt{n})$ rather than the $O(1)$ that appears in Jung's theorem. Hence the case of the inradius requires separate attention.

Similar results also hold when the Euclidean norm is replaced by other norms (see [DGK63] for references). However, in the general case, we develop specific algorithms for each of the measurements in question, for it is then possible to derive almost exact algorithms in several cases.

§1.B. *Some properties of l_p spaces.* We use the following relationship among l_p norms, which can be proved by a routine application of Lagrange multipliers.

PROPOSITION 1.5. *If $n\in\mathbb{N}$ and $1\leq p\leq q\leq\infty$, then $\|x\|_q\leq\|x\|_p\leq n^{1/p-1/q}\|x\|_q$ for each $x\in\mathbb{R}^n$. (Here, $1/\infty:=0$.)*

We also use the well-known formula for the volume of the n-dimensional l_p unit ball $\mathbb{B}_p^n$ (see p. 11 of [Pis88]).

PROPOSITION 1.6. *If $n\in\mathbb{N}$ and $1<p<\infty$, then*

$$\mathrm{vol}(\mathbb{B}_p^n)=2^n\frac{(\Gamma(1+1/p))^n}{\Gamma(1+n/p)}.$$

Finally, we need upper bounds on volume ratios which, in Subsection 3.E, lead to bounds on ratios of radii and eventually to our upper bounds on the accuracy of oracle-polynomial-time approximations of radii in l_p spaces. The bounds in the following proposition are our versions of bounds that were proved by Carl [Car85] and Carl and Pajor [CP88] with the aid of the notion of entropy numbers, and an interaction between this and the concept of the Rademacher type of a Banach space. These concepts are briefly reviewed in Subsection 3.D, in order to make it clear that the results from [Car85] and [CP88] that are used here do indeed serve the purpose for which we need them. The essential point is that certain "constants" in their papers, while being constant in the sense that they require, are nevertheless dependent on the ambient dimension n, and for our purposes this dependence must be examined more closely.

PROPOSITION 1.7. *For each $p\in[1,\infty]$, for each choice of h, $n\in\mathbb{N}$ with $20\log((h/n))+1)\leq n\leq h$, and for each 0-symmetric n-polytope $P\subset\mathbb{B}_p^n$ with at most $2h$ vertices, it is true that*

$$\left(\frac{\mathrm{vol}\,(P)}{\mathrm{vol}\,(\mathbb{B}_p^n)}\right)^{1/n}\leq 24\cdot 20^{1-1/p}\left(\frac{\log((h/n)+1)}{n}\right)^{1-1/p},\qquad \text{for } 1\leq p\leq 2,$$

$$\left(\frac{\mathrm{vol}\,(P)}{\mathrm{vol}\,(\mathbb{B}_p^n)}\right)^{1/n}\leq 24\cdot 40^{1/2}\left(\Gamma\left(\frac{1+p}{2}\right)\Big/\Gamma\left(\frac{1}{2}\right)\right)^{1/p}\times\left(\frac{\log((h/n)+1)}{n}\right)^{1/2},\qquad \text{for } 2<p<\infty,$$

$$\left(\frac{\mathrm{vol}\,(P)}{\mathrm{vol}\,(\mathbb{B}_\infty^n)}\right)^{1/n}\leq 24\cdot(20e)^{1/2}(1+\ln n)^{1/2}\left(\frac{\log((h/n)+1)}{n}\right)^{1/2}.$$

As it turns out, the bounds for $p<\infty$ are optimal for our purpose but, as pointed out by Pajor and Schechtmann, they can be improved in the case $p=\infty$ by the following argument. Consider any 0-symmetric n-polytope $P\subset\mathbb{B}_\infty^n$ with at most a polynomial number of vertices. Then the polytope

$P' = 1/\sqrt{n}P$ is contained in $\mathbb{B}_2^n$ and Proposition 1.7 can be applied. Using the facts that the volume is homogenous of degree n, $\mathrm{vol}\,(\mathbb{B}_2^n)^{1/n} = \Omega(1/\sqrt{n})$, and $\mathrm{vol}\,(\mathbb{B}_\infty^n)^{1/n} = 2$, we obtain

$$\left(\frac{\mathrm{vol}\,(P)}{\mathrm{vol}\,(\mathbb{B}_\infty^n)}\right)^{1/n} = O\left(\left(\frac{\log n}{n}\right)^{1/2}\right).$$

In the l_2 case, a close relative of Proposition 1.7 appears in [BF87]. In detail, the proofs for general l_p-spaces are quite different from those for l_2. However, the underlying geometric ideas are similar. As we see later, the previous result uses a covering of a polytope with simplices all of which have the same upper bound for their circumradii, while the argument of [BF87] uses the fact that each point contained in a simplex is, for suitable $j \in \mathbb{N}$, "close" to at least one of its j-dimensional faces. This extended an idea of Elekes [Ele86] using the covering of a simplex by balls centred at its vertices.

A result concerning the polar problem, estimating the volume of a polytope containing the unit ball and given by a linear inequality system, was proved by Ball and Pajor [BP90]. There an $\mathscr{H}$-polytope is interpreted as the intersection of a lower-dimensional subspace with a higher-dimensional unit cube, and a lower bound for the volume of that intersection is derived by using an extension of a theorem of Vaaler [Vaa79].

§1.C. *Oracles.* For deterministic computation, our underlying model is the usual binary Turing machine (*cf.* [GJ79]). In discussing randomization, we assume further that the Turing machine has distinguished coin-tossing states—*i.e.*, in prescribed situations two different transitions of the Turing machine are possible, and the choice between them is made by tossing a fair coin (see [Gil77]). In all other states the next step is decided deterministically.

For our purposes, both the deterministic Turing machine and its probabilistic relative must be augmented by certain oracles that are described in detail below. The machine can write information on a specified tape, the oracle takes this information as the input to a certain problem, and writes the solution back onto the tape. Though nothing is assumed about the manner in which the oracle produces its output (it operates as a "black box"), it is assumed that the size of the oracle's output is bounded by a polynomial in the size of its input. An algorithm that involves calls on the oracle is then called an *oracle-polynomial-time algorithm* if it is polynomial in the usual sense, with the understanding that each oracle call is measured by the time necessary to write its input and to read its output. In particular, any oracle-polynomial-time algorithm can use at most a polynomial number of calls to the given oracles.

An important consequence of the above definition is that any oracle-polynomial-time algorithm can be turned into a genuinely polynomial algorithm for any situation in which the oracle's action can be carried out in polynomial time. In other words, for any problem Π that can be solved in oracle-polynomial time, a polynomial-time algorithm for the oracle's function immediately yields a polynomial-time algorithm for Π. And vice versa, if Π turns out to be, say $\mathbb{NP}$-hard, then the same holds for the problem solved by the oracle.

A way to deal algorithmically with a general body K was introduced and extensively studied in [GLS93]. There it is assumed that only a small amount

of *a priori* information about K is available, and that all further information about K must be obtained from an algorithm (called an *oracle*) that answers certain sorts of questions about K. It is usually assumed here that each body K is *circumscribed*, *i.e.*, a rational number $\bar{R}$ is given explicitly such that $K \subset \bar{R}\mathbb{B}_2$. (Thus $\bar{R}$ is an upper bound for K's circumradius in l_2.) The *size* of K is then defined by size $(K) := n + \text{size}(\bar{R})$. It is usually necessary to assume also that K is *well-bounded*, *i.e.*, K is circumscribed and, in addition, a positive rational number $\underline{r}$ is given such that K contains a ball (whose position may not be known) of radius $\underline{r}$. (Thus $\underline{r}$ is a lower bound for K's inradius in l_2.) Then, of course, size $(K) := n + \text{size}(\underline{r}) + \text{size}(\bar{R})$.

One important oracle for our purposes is the weak separation oracle, where "weak" refers to the fact that we have to allow for a rounding error, since only finite precision is available. Recall that, for $\varepsilon \geqslant 0$, the *outer parallel body* and the *inner parallel body* of a body K are given respectively by

$$K(\varepsilon) = K + \varepsilon\mathbb{B}_2 \quad \text{and} \quad K(-\varepsilon) = \{x \in \mathbb{R}^n : x + \varepsilon\mathbb{B}_2 \subset K\}.$$

A *weak separation oracle* for a body K in $\mathbb{R}^n$ solves the WEAK SEPARATION PROBLEM. *Given $y \in \mathbb{Q}^n$ and a positive rational ε, assert that $y \in K(\varepsilon)$, or deliver a vector $c \in \mathbb{Q}^n$ with $\|c\|_\infty = 1$ such that $c^T \leqslant x \leqslant c^T y + \varepsilon$ for all $x \in K(-\varepsilon)$.*

For the situation in which the input K is a full-dimensional $\mathscr{H}$-polytope or a full-dimensional $\mathscr{V}$-polytope, [GLS93] produces deterministic polynomial-time algorithms for well-boundedness and for solving the weak separation problem. In general, however, as mentioned above, the separation oracle functions as a "black box".

Under the assumption of infinite precision it makes sense to allow $\varepsilon = 0$ instead of $\varepsilon > 0$. In this case we say that a *strong separation oracle* solves the *strong separation problem*. Proving our upper bounds on accuracy with strong oracles yields in some sense stronger results, and this will be done in Subsections 2.C and 3.E. For the lower bounds, working with weak oracles and the attendant details of finite precision is necessary in order to obtain the sharpest results. This will be done in the case of the lower bounds for deterministic algorithms, but for simplicity of presentation we use strong instead of weak oracles in the discussion of randomized algorithms.

The origin of the algorithmic theory of convex bodies, and also one of its major algorithmic tools, is the ellipsoid algorithm of Shor [Sho77], Yudin and Nemirovskii [YN76], and Khachiyan [Kha79]. In particular, the following fundamental result can be proved with the aid of the ellipsoid algorithm (see Corollaries 4.2.7 and 4.4.7 of [GLS93]).

PROPOSITION 1.8. *There is an oracle-polynomial-time algorithm which, accepting as input $n \in \mathbb{N}$, a circumscribed body K in $\mathbb{R}^n$ given by a weak separation oracle, a rational n-vector c, and a positive rational ε, solves the* WEAK OPTIMIZATION PROBLEM, *i.e., either asserts that $K(-\varepsilon) = \varnothing$ or delivers a rational n-vector v such that $v \in K(\varepsilon)$ and $c^T x \leqslant c^T v + \varepsilon$ for all $x \in K(-\varepsilon)$. Conversely, if the body, not necessarily circumscribed, is given by a weak optimization oracle, then the weak separation problem can be solved in oracle-polynomial time.*

Any such output point v of a weak optimization oracle is called a *weak optimizer* over K of the linear functional associated with the vector c.

Besides investigating the relationships among various oracles for the same body, [GLS93] provides results about oracles associated with bodies that are formed by combining other bodies in various ways (see Section 4.7 of [GLS93]). Here is an example.

PROPOSITION 1.9. *There exists an oracle-polynomial-time algorithm which, given as input a well-bounded body K presented by a weak optimization oracle, solves the weak optimization problem for the difference body $K-K$.*

For the reader not acquainted with the oracular method, these two propositions may serve to provide some feeling for the strength of the method. Roughly speaking, the linear optimization problem is reduced to the separation problem, and since the latter can be solved in polynomial time for both $\mathcal{V}$- and $\mathcal{H}$-polytopes, any oracle-polynomial-time algorithm becomes a genuinely polynomial-time algorithm for such polytopes. Thus, in a sense, the oracle method provides a unified approach to $\mathcal{V}$-polytopes and $\mathcal{H}$-polytopes. For another illustration, consider a situation in which a polytope P is $\mathcal{H}$-presented, and we want to solve some problem for the polytope $P-P$. In general, it is not possible to produce an $\mathcal{H}$-presentation for $P-P$ in polynomial time, but a polynomial-time optimization oracle for $P-P$ is available.

Whenever a body K is considered here without specified additional information about its presentation, it is assumed that K is well-bounded, is at least 2-dimensional, and is presented by a separation or optimization oracle.

§1.*D. Accuracy.* Consider an arbitrary measurement for bodies—a function φ which, for each $n\in\mathbb{N}$ and each $K\in\mathcal{K}^n$, assigns a positive number $\varphi(K)$—and consider an algorithm A for approximating φ by a function φ_A. For a function $\underline{\lambda}:\mathbb{N}\to[0,1]$ we say that

- *the accuracy of A in approximating φ is at least $\underline{\lambda}$* if there exist two functions $\lambda_1:\mathbb{N}\to[0,\infty]$ and $\lambda_2:\mathbb{N}\to]0,\infty[$ such that $\underline{\lambda}=\lambda_1/\lambda_2$, and such that, for each $n\in\mathbb{N}$ and each $K\in\mathcal{K}^n$, it is true that

$$\lambda_1(n)\varphi_A(K)\leq\varphi(K)\leq\lambda_2(n)\varphi_A(K). \tag{1}$$

Further, for a function $\bar{\lambda}:\mathbb{N}\to[0,1]$, we say that

- *the accuracy of A in approximating φ is at most $\bar{\lambda}$* if there does not exist any function $\underline{\lambda}$ of the sort just described such that $\bar{\lambda}<\underline{\lambda}$.

Note that the latter is equivalent to the fact that, for each function $\underline{\lambda}$ with $\bar{\lambda}<\underline{\lambda}$, (1) fails for at least one $K\in\mathcal{K}^n$ for any $n\in\mathbb{N}$.

Depending on the number of oracle-calls performed in the worst case, algorithms can be divided into several different classes. With respect to any such class $\mathcal{A}$ of algorithms for approximating φ, we say that $\mathcal{A}$'s *accuracy in approximating* φ is

- *at least* $\underline{\lambda}$ if there exists $A\in\mathcal{A}$ whose accuracy in approximating φ is at least $\underline{\lambda}$,
- *at most* $\bar{\lambda}$ if each $A\in\mathcal{A}$ has accuracy in approximating φ of at most $\bar{\lambda}$.

When $\mathcal{A}$ consists of all deterministic (oracle-) polynomial-time algorithms we simply speak of *accuracy in deterministic (oracle-) polynomial-time approximation.*

For a function $f: \mathbb{N} \to [0, 1]$, we say that the accuracy is $\Omega(f(n))$ if it is at least $\underline{c} f(n)$ for some constant $\underline{c} > 0$, and the accuracy is $O(f(n))$ if it is at most $\bar{c} f(n)$ for some constant $0 < \bar{c} < \infty$, where the constants are independent of the dimension. When the accuracy is both $\Omega(f(n))$ and $O(f(n))$, we say that the accuracy is $\Theta(f(n))$. In this case our asymptotic estimate for the accuracy is optimal up to a factor independent of the dimension, and the same is true for our algorithm that is used to justify the $\Omega(f(n))$.

The above concept must be slightly modified for randomized approximation. In this case a number μ with $1/2 < \mu \leq 1$ is given, and we say that the *accuracy of A in approximating φ with probability at least μ is at least $\underline{\lambda}$* if (1) holds with probability greater than or equal to μ. The other definitions are modified analogously.

When $\mathcal{A}$ consists of all randomized (oracle-) polynomial-time algorithms which, for some $\mu \in]1/2, 1]$, approximate φ with probability at least μ, we omit explicit mention of $\mathcal{A}$ and speak simply of *accuracy in randomized (oracle-) polynomial-time approximation.* To understand the focus on the case $1/2 < \mu$, recall that there is a standard trick—choosing the median of the outputs from a polynomial number of independent runs of the algorithm—whereby any polynomial-time algorithm whose accuracy in approximating φ with probability at least μ is at least $\underline{\lambda}$ can be used as a subroutine in producing a polynomial-time algorithm whose accuracy in approximating φ with probability at least ν is at least $\underline{\lambda}$, where ν can be arbitrarily chosen from $[\mu, 1[$, *cf.* [JVV86]. Hence the restriction to $1/2 < \mu$ is quite natural.

§2. *Randomization does not help!* Extending ideas of Elekes [Ele86], Bárány and Füredi [BF87] showed that, if c is a constant independent of the dimension n, and a convex body K in Euclidean n-space is presented by means of an optimization oracle, then a superpolynomial number of calls to the oracle is required to approximate K's volume deterministically with relative error less than $(cn/\log(n))^n$. It follows easily that a superpolynomial number of calls is also required to approximate K's diameter or width deterministically with relative error less than $\sqrt{cn/\log n}$, and this statement about diameter and width holds also for the other radii considered here. (See the Euclidean part of Theorem 3.21.) Thus the results of Elekes, Bárány and Füredi tell us that deterministic algorithms are very bad in estimating these measurements for bodies in high-dimensional Euclidean spaces. In the specific form just stated, this negative conclusion concerns only the oracle model. However, the measurements are also hard to compute when K is given as the solution set of a system of linear inequalities, for then volume computation is #$\mathbb{P}$-hard [DF88, Kha88], and the computation of radii is $\mathbb{NP}$-hard even for very simple sorts of bodies [FO85, GK93]. Considering approximation instead of exact computation, $\mathbb{APX}$-completeness for small classes of polytopes can be proved, and the problems considered here turn out to be at least $\mathbb{APX}$-hard [BGK00]

in general. (See [PY91], [MPS98], and especially [Jan98] for an introduction to classes of approximation complexity for optimization problems.)

A breakthrough in the positive direction was achieved by Dyer, Frieze, and Kannan [DFK89], who gave a randomized oracle-polynomial-time algorithm that finds an approximation of the volume with arbitrarily small relative error. Their original running-time bound of $O^*(n^{23})$ was improved in a sequence of papers, culminating in an $O^*(n^5)$ bound for an algorithm of Kannan, Lovász and Simonovits [KLS98]. (The notation O^* indicates that certain factors depending on $\log n$ and on the error bound are suppressed.)

The success of randomized algorithms in volume approximation, in conjunction with the similar behaviour of volume and radii in deterministic approximation, suggests that randomization might also be useful in computing radii. It was proved in [LS92] that no oracle-polynomial-time algorithm can compute the diameter of a body with arbitrarily small relative error, but this does not exclude the possibility that randomization can help in improving the accuracy. The present analysis does exclude that possibility by combining the ideas of [LS92] with careful estimates for covering numbers of the Euclidean sphere. (An approach in terms of covering numbers could also be used in Section 3 for the deterministic case, but instead we work there with polytopal approximations of the unit ball in order to facilitate the treatment of arbitrary l_p spaces.)

In the present section, "algorithm" means "randomized algorithm" and details are simplified by considering only Euclidean spaces. For further simplification, we use exact (infinite-precision) arithmetic and assume that the bodies are presented by strong optimization oracles. This yields the strongest results for upper bounds on accuracy of approximation. To obtain the strongest results on lower bounds, it would be necessary to deal with the consequences of finite precision, much as is done in Section 3.

Though only the diameter is considered explicitly in this section, it is easy to use the material in Section 3 to derive analogous results for the other radii considered in this paper.

§2.A. *Bounds for the fractional covering number of the Euclidean sphere.* The accuracy of diameter approximation in Euclidean spaces $\mathbb{E}^n$ turns out to be closely related to the efficiency with which the Euclidean unit sphere $\mathbb{S}_2 = \{x \in \mathbb{R}^n : \|x\|_2 = 1\}$ can be covered with spherical caps. For each $v \in \mathbb{S}_2$ and $0 < s < 1$, we define the *s-cap with centre v* as the set $\{u \in \mathbb{S}_2 : v^T u \geq s\}$, hence as the set of all points of $\mathbb{S}_2$ that are separated from the origin by the hyperplane $\{x : v^T x = s\}$. (Here, s is the distance of the hyperplane from the origin.)

The smallest number of s-caps that can be used to cover the unit sphere will be denoted by $\tau(n, s)$, and called the *covering number* of the sphere by s-caps. This number is closely related to the deterministic approximation of diameters, as is explained in Section 4. However, in connection with randomized approximation we must focus instead on the *fractional covering number* of the sphere by s-caps. This number, denoted by $\tau^*(n, s)$, is just the ratio of the $(n-1)$-measure of the sphere to the $(n-1)$-measure of an s-cap. It is obvious that $\tau^*(n, s) < \tau(n, s)$.

Our bounds for randomized approximation can be expressed in terms of the function τ^* or, equivalently, in terms of $\gamma = 1/\tau^*$, so that we need some estimates of these quantities.

Let $\omega_n = \pi^{n/2}/\Gamma(1+n/2)$, the volume of the n-dimensional Euclidean unit ball. Then

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

whence, with the aid of Stirling's formula asserting for $n \geqslant 3$ that

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

we can obtain the following estimates.

LEMMA 2.1.
(a) *For* $0 < s < \sqrt{2/n}$, $1/12 < \gamma(n,s) < 1/2$.
(b) *For* $\sqrt{2/n} \leqslant s < 1$,

$$\frac{1}{6s\sqrt{n}}(1-s^2)^{(n-1)/2} < \gamma(n,s) < \frac{1}{2s\sqrt{n}}(1-s^2)^{(n-1)/2}.$$

Proof. Define, for an integer $m > -2$ and non-negative h,

$$J_m^h(s) = \int_s^1 t^{-h}(1-t^2)^{m/2}\,dt,$$

and apply partial integration with $u(t) = (1-t^2)^{(m+2)/2}/(m+2)$, $v(t) = -t^{-h-1}$ to obtain

$$(m+2)J_m^h(s) = \left[\frac{-(1-t^2)^{(m+2)/2}}{t^{h+1}}\right]_s^1 - (h+1)\int_s^1 t^{-h-2}(1-t^2)^{(m+2)/2}dt$$

$$= \frac{1}{s^{h+1}}(1-s^2)^{(m+2)/2} - (h+1)J_{m+2}^{h+2}(s).$$

Since $J_{m+2}^{h+2}(s) > 0$, it follows that

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

and

$$(m+2)J_m^h(s) > \frac{1}{s^{h+1}}(1-s^2)^{(m+2)/2} - \frac{(h+1)}{(m+4)}\frac{1}{s^{h+3}}(1-s^2)^{(m+4)/2}.$$

We need this for $h = 0$:

$$\frac{1}{s}(1-s^2)^{(m+2)/2} - \frac{1}{(m+4)}\frac{1}{s^3}(1-s^2)^{(m+4)/2} < (m+2)J_m^0(s) < \frac{1}{s}(1-s^2)^{(m+2)/2}.$$

The above is true for all s. Now, for $s \geqslant \sqrt{2/(m+6)}$, we obtain

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

and hence conclude for $m = n-3$ that

$$\gamma(n,s) > \frac{n-1}{n}\sqrt{\frac{n}{2\pi}}J_{n-3}^0(s) > \frac{1}{2ns}\sqrt{\frac{n}{2\pi}}(1-s^2)^{(n-1)/2} > \frac{1}{6s\sqrt{n}}(1-s^2)^{(n-1)/2},$$

and

$$\gamma(n,s) < \frac{n-1}{n}\frac{\sqrt{n}}{2}J_{n-3}^0(s) < \frac{1}{2s\sqrt{n}}(1-s^2)^{(n-1)/2}.$$

This proves part (b) of the lemma. Part (a) is not needed here, and so its proof is omitted. □

§2.B. *Randomized algorithms for approximating radii.* We begin with a theorem that expresses the accuracy of randomized approximation in terms of the fractional covering number. The lower bound for oracle-polynomial-time algorithms is then obtained by combining this theorem with the estimates for the fractional covering number obtained in the previous subsection.

THEOREM 2.2. *For each $0 < s < 1$ there is an algorithm that, given a body $K \subset \mathbb{E}^n$, uses $4\lceil \tau^*(n,s) \rceil$ oracle calls, and produces an approximation $d_A(K)$ of $d(K)$ such that $d_A(K) \leqslant d(K)$ and* prob $(sd(K) \leqslant d_A(K)) > 6/7$.

Proof. Let $M = 2\lceil \tau^*(n,s) \rceil$, and let $u_1, \ldots, u_M$ be independently, uniformly distributed random points on the unit sphere $\mathbb{S}^{n-1}$. For $1 \leqslant i \leqslant M$, compute the maxima

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

and define $d_A(K) = \max_{1 \leqslant i \leqslant M} \omega_i$.

Since each ω_i denotes the distance between two parallel supporting hyperplanes of K, it follows that $d_A(K) \leqslant d(K)$. To prove that the probabilistic condition is satisfied, suppose that $d_A(K) < sd(K)$. Let $p, q \in K$ have $\|p-q\|_2 = d(K)$, let v be the unit vector pointing in the direction $q-p$, and let C_s denote the s-cap centred at v. Then C_s contains no u_i, because, if $u_i \in C_s$, then, by the definition of an s-cap,

$$\omega_i = \max_{x,y \in K} u_i^T(x-y) \geqslant u_i^T(q-p) = d(K)u_i^T v \geqslant sd(K),$$

and hence $d_A(K) \geq \omega_i \geq sd(K)$, contrary to the supposition. Now, the probability that no u_i belongs to C_s is

$$\left(1 - \frac{\mathrm{vol}_{n-1}(C_s)}{\mathrm{vol}_{n-1}(\mathbb{S}^{n-1})}\right)^M = \left(1 - \frac{1}{\tau^*(n,s)}\right)^M$$
$$= \left(1 - \frac{M/\tau^*(n,s)}{M}\right)^M$$
$$< e^{-M/\tau^*(n,s)} \leq e^{-2} < 1/7,$$

completing the proof. □

Theorem 2.2 could be formulated more generally: using $2\lceil v\tau^*(n,s)\rceil$ oracle calls with $v>0$ yields correct results with probability greater than $1-e^{-v}$.

THEOREM 2.3. *There is a $k_0 \in \mathbb{N}$ and an algorithm A which, given a body $K \subset \mathbb{E}^n$ and $k \in \mathbb{N}$ with $k_0 \leq k \leq 2^{n/3}$, uses fewer than k oracle calls to compute an estimate $d_A(K)$ of $d(K)$ such that $d_A(K) \leq d(K)$ and*

$$\mathrm{prob}\left(d(K) \leq \sqrt{\frac{n}{\log k}}\, d_A(K)\right) > \frac{6}{7}.$$

Proof. The theorem follows from Theorem 2.2, once we show that

$$4\lceil \tau^*(n,s')\rceil \leq k \qquad \text{for } s' = \sqrt{\frac{\log k}{n}}.$$

For $4 \leq k < 2^n$, Lemma 2.1 yields

$$4\lceil \tau^*(n,s')\rceil \leq 24\sqrt{\log k}\left(1 - \frac{\log k}{n}\right)^{(1-n)/2}$$
$$\leq 24\sqrt{\log k}(5/4e)^{(\log k)/2}$$
$$\leq 24\sqrt{\log k}(1.9)^{\log k}$$
$$\leq 24\sqrt{\log k}\, k^{0.93} \leq k,$$

where the last inequality holds for large enough k. □

§2.C. *Inapproximability results for randomized approximation.* As in the case of the lower bound, we start with a general theorem that connects the accuracy of approximation to the fractional covering numbers.

THEOREM 2.4. *Let $0 < s < 1$, and let A be an algorithm that computes, for every body $K \subset \mathbb{E}^n$, an estimate $d_A(K)$ of $d(K)$ such that* $\mathrm{prob}\,((sd(K) \leq d_A(K) \leq d(K)) \geq 3/4$. *Then A must use at least $\tau^*(n,s)/2$ oracle calls in the worst case.*

Proof. Suppose that A makes at most t oracle calls, where $t < \tau^*(n, s)/2$. Choose $s' < s$ so that $t < \tau^*(n, s')/2$. 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 $\mathbb{B}^n \cup \{(1/s')v,\ -(1/s')v\}$. The algorithm has internal coin flips, and we use the same coin flips in both copies. Let d_A and d'_A 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 $u_1, \ldots, u_t$ be the unit vectors for which the optimization oracle is called with input $\mathbb{B}^n$, let $C^1, \ldots, C^t$ be the s'-caps centred at $u_1, \ldots, u_t$, and let $Q = C^1 \cup \cdots \cup C^t$. Then

$$\text{prob}\,(v \in Q) = \frac{\text{vol}_{n-1}(Q)}{\text{vol}_{n-1}(\mathbb{S}^{n-1})} \leqslant \sum_{i=1}^{t} \frac{\text{vol}_{n-1}(C^i)}{\text{vol}_{n-1}(\mathbb{S}^{n-1})} = \frac{t}{\tau^*(n, s')} < \frac{1}{2},$$

Whenever $v \notin Q$, the two copies of the algorithm run in the same way and produce the same output. Thus $\text{prob}\,(d_A \neq d'_A) < 1/2$.

By the assumptions on the performance of A, we also know that

$$\text{prob}\,(d'_A \leqslant 2) = \text{prob}\,(d'_A \leqslant s'd(K)) \leqslant \text{prob}\,(d'_A < sd(K)) \leqslant 1/4$$

and $\text{prob}\,(2 < d_A) = \text{prob}\,(d(\mathbb{B}^n) < d_A) \leqslant 1/4$. But this implies a positive probability for joint occurrence of the three events

$$d_A \leqslant 2, \qquad 2 < d'_A, \quad \text{and} \quad d_A = d'_A,$$

leading to the contradictory conclusion that $2 < 2$. □

Note that Theorem 2.4 remains true if the bound 3/4 for the probability is replaced by an arbitrary constant μ with $1/2 < \mu < 1$, and $\tau^*(n, s)/2$ is replaced by $\tau^*(n, s)/l$, where $l < 0$ and $1 < (2\mu - 1) + (1 - 1/l) = 2\mu - 1/l$.

Combining Theorem 2.4 with a tight lower bound for the fractional covering number, we obtain the following.

THEOREM 2.5. *Suppose that λ is a real number in the interval $[\sqrt{2}, \sqrt{n/2}]$. If an algorithm A computes an approximation $d_A(K)$ of $d(K)$ for each body $K \subset \mathbb{E}^n$, and A is such that*

$$\text{prob}\left(d_A(K) \leqslant d(K) \leqslant \frac{\sqrt{n}}{\lambda} d_A(K)\right) \geqslant \frac{3}{4}$$

for each K, then A must use at least $(0.9)\lambda 2^{\lambda^2/2}$ oracle calls.

Proof. In view of Theorem 2.4, it suffices to prove that $1.8\lambda 2^{\lambda^2/2}$ is a lower bound for $\tau^*(n, \lambda/\sqrt{n})$.

Lemma 2.1 yields

$$\frac{1}{2}\tau^*\left(n, \frac{\lambda}{\sqrt{n}}\right) > \lambda\left(1 - \frac{\lambda^2}{n}\right)^{(1-n)/2} \geqslant \sqrt{1/2}\lambda e^{\lambda^2/2} \geqslant 0.9\lambda^{\lambda^2/2},$$

which finishes the proof. □

Theorem 2.5 yields the following relation between the quality of approximation and the polynomial degree of the algorithm.

COROLLARY 2.6. *Let $h \geq 1$ and let A be an oracle-polynomial-time algorithm which, for each body $K \subset \mathbb{R}^n$, uses $O(n^h)$ oracle calls to compute two values $\underline{d}_A(K)$ and $\bar{d}_A(K)$ such that*

$$\text{prob}\,(\underline{d}_A(K) \leq d(K) \leq \bar{d}_A(K)) \geq 3/4.$$

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

$$\frac{\bar{d}_A(K_0)}{\underline{d}_A(K_0)} > \sqrt{\frac{n}{2h \log n}}.$$

Proof. It follows from Theorem 2.5 that, whenever fewer than $(0.9)\lambda 2^{\lambda^2/2}$ oracle calls are made to determine two values $\underline{d}_A(K)$ and $\bar{d}_A(K)$ such that these determine with probability at least 3/4 a lower and an upper bound for the diameter, then $\bar{d}_A(K)/\underline{d}_A(K) > \sqrt{n}/\lambda$. Now the proof is finished by observing that $(0.9)\lambda 2^{\lambda^2/2} > \sqrt{h \log n}\, 2^{h \log n} \geq \sqrt{\log n}\, n^h = \Omega(n^h)$ for $\lambda = \sqrt{2h \log n}$. □

The following is just the "negative" formulation of Corollary 2.6. It shows that randomization does not help to overcome the upper bound of Bárány and Füredi [BF87] mentioned earlier.

THEOREM 2.7. *If A is an algorithm that uses a polynomial number of oracle calls to compute an approximation $d_A(K)$ 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*

$$\text{prob}\left(d_A(K_0) \leq d(K_0) \leq c \sqrt{\frac{n}{\log n}}\, d_A(K_0)\right) \leq \frac{1}{4}.$$

We remark that the arguments used in this and in the previous subsection yield the following observation. Let $K \subset \mathbb{B}$ be a convex body and set $M = \text{vol}\,(\mathbb{B})/\text{vol}\,(\mathbb{B} \setminus K)$. Then any randomized algorithm that distinguishes an isometric copy of K from $\mathbb{B}$ with probability at least 2/3 must make at least $M/3$ calls on the oracle describing K. On the other hand, we can generate $3M$ random points and check whether they belong to K; this distinguishes K from $\mathbb{B}$ with probability at least 2/3.

Theorem 2.7 shows that randomization does not help to do any better than the known bound for deterministic approximation. The good news is that asymptotically optimal randomized algorithms are available (see Theorem 2.3). However, we show in section 3.C that we can also do that well deterministically, even when using only weak oracles and taking rounding into account. Further, we obtain similarly sharp results for approximating radii in arbitrary l_p spaces.

§3. *Deterministic approximation.* In this section, "algorithm" always means "deterministic algorithm".

As was mentioned in the introduction, there are at least two different ways to approach our problems, and each has its own flavour. In Section 2, covering numbers of spheres were used for randomized approximation of radii. In the present section, we approach the deterministic approximation of radii by finding an approximation of the given l_p norm by a polytopal norm, computing the radii with respect to that norm in polynomial time, and then taking the result as an approximation of the radius with respect to the given norm.

§3.A. *Solutions with respect to polytopal norms.* We consider the inradius in detail (since it poses the most difficult problem), and then say a few words about the other radii.

Suppose that the unit ball $\mathbb{B}_\nearrow$ of a polytopal norm is $\nearrow$-presented, and we want to compute the *inradius* of a convex body K presented by a strong separation oracle. For each rational $r>0$, the existence of a point in the convex set

$$S_{K,r} = \{a \in \mathbb{R}^n : a + r\mathbb{B}_\nearrow \subset K\}$$

is equivalent to the condition that $r \leqslant r_\nearrow(K)$. Since the unit ball is $\nearrow$-presented, for each $a \in \mathbb{R}^n$ we can use the separation oracle to decide whether $a \in S_{K,r}$, and if the decision is negative we obtain a hyperplane separating K and $a + rv$ for some vertex v of $\mathbb{B}_\nearrow$. By the definition of the set $S_{K,r}$, this yields a hyperplane separating a and $S_{K,r}$. Therefore we can solve the separation problem for $S_{K,r}$ and hence, using the central cut ellipsoid method presented in [GLS93], either decide that $S_{K,r}$ is "almost empty" or obtain a point of $S_{K,r}$. A suitable binary search then yields an approximation of $r_\nearrow(K)$ with arbitrary accuracy in oracle-polynomial time. (This works even for non-symmetric polytopal norms.)

By Propositions 1.1 and 1.2, the inradius algorithm can be used to compute the *width* of K if we can solve the weak separation problem for $K-K$ in oracle-polynomial time. An algorithm solving this problem appears in [GLS93], mainly using Propositions 1.8 and 1.9. Also, we see from Proposition 1.3 that it is not necessary to apply the ellipsoid algorithm in each step, because $S_{K-K,r} \neq \emptyset$ if and only if $0 \in S_{K-K,r}$.

Turning now to details, we begin by defining, for two bodies C and K, a containment problem that is a special case of a class of containment problems introduced in [BG97].

WEAK C-CONTAINMENT PROBLEM. *Given $a \in \mathbb{Q}^n$ and a positive rational ε, assert that $a + C \subset K(\varepsilon)$, or deliver a vector $c \in \mathbb{Q}^n$ with $\|c\|_\infty = 1$ such that there exists a vector $u \in a + C$ with $c^T x \leqslant c^T u + \varepsilon$ for all $x \in K(-\varepsilon)$.*

In general, the weak C-containment problem cannot be solved in polynomial time (unless $\mathbb{P} = \text{co}\mathbb{NP}$), since it is already co$\mathbb{NP}$-complete to decide whether the standard cube is contained in a given affine image of a $\nearrow$-cross-polytope [BGKL90, FO85, GK93]. However, the problem is easy in the following special case.

LEMMA 3.1. *The Weak C-Containment Problem is solvable in oracle-polynomial time if the body K is circumscribed and the body C is a $\mathcal{V}$-polytope.*

Proof. Let $(n, s; v_1, \ldots, v_s)$ represent C, and let ε and a be the input of the Weak C-Containment Problem. Call the weak separation oracle for K with input ε and $a+v_i$ for $1 \leq i \leq s$, where $v_1, \ldots, v_s$ are the vertices of C. If all assertions are affirmative—*i.e.*, if $a+v_i \in K(\varepsilon)$ for all i—we obtain $a+C \subset K(\varepsilon)$ by convexity. If not, at least one call, say the first, delivers a rational n-vector c with $\|c\|_\infty = 1$ and $c^T x \leq c^T(a+v_1)+\varepsilon$ for all $x \in K(-\varepsilon)$. Since $a+v_1 \in a+C$, this yields a valid answer for the C-containment problem. □

Now we can prove the following.

LEMMA 3.2. *There exists an oracle-polynomial-time algorithm A which, for input consisting of a positive rational μ, a string $\mathbb{B}_\mathcal{V} = (n, s; v_1, \ldots, v_s)$ defining the unit ball of a polytopal norm, and a well-bounded body K, delivers a number $\tau_A(K)$ with*

$$r_A(K) \leq r_\mathcal{V}(K) < (1+\mu) r_A(K),$$

and a point $a_A(K)$ with $a_A(K) + r_A(K)\mathbb{B}_\mathcal{V} \subset K$.

Proof. First note that, in polynomial time, we can find positive rationals γ_1, γ_2 such that $\gamma_1 \mathbb{B}_2 \subset \mathbb{B}_\mathcal{V} \subset \gamma_2 \mathbb{B}_2$; see [GLS93]. Now, let the rationals $\underline{r}$ and $\bar{R}$ denote respectively a positive lower bound for K's Euclidean inradius and an upper bound for K's Euclidean circumradius, and let ρ denote a rational with $0 < \rho \leq (\mu \underline{r})/(2\gamma_2)$.

For $r > 0$, define the circumscribed convex set

$$S_{K,r} = \{a \in \mathbb{R}^n : a + r\mathbb{B}_\mathcal{V} \subset K\}.$$

By the definition, if $S_{K,r} \neq \varnothing$ then $r_\mathcal{V}(K) \geq r$. On the other hand, since, for arbitrary $x \in \mathbb{R}^n$,

$$x + \rho\gamma_1 \mathbb{B}_2 + r\mathbb{B}_\mathcal{V} \subset x + (\rho + r)\mathbb{B}_\mathcal{V},$$

$S_{K,r}(-\rho\gamma_1) = \varnothing$ yields $r_\mathcal{V}(K) < r + \rho$.

Assume for a moment that we can either find $a \in S_{K,r}$ or decide whether $S_{K,r}(-\rho\gamma_1) = \varnothing$ for arbitrary r. Define $r_l = \underline{r}/\gamma_2$ and $r_u = \bar{R}/\gamma_1$. Since $\gamma_1 \mathbb{B}_2 \subset \mathbb{B}_\mathcal{V} \subset \gamma_2 \mathbb{B}_2$, we obtain $r_l \leq r_\mathcal{V}(K) \leq r_u$. Solve the problem just mentioned with $r = \frac{1}{2}(r_l + r_u)$. If we find $a \in S_{K,r}$ we set $r_l = r$, and otherwise $r_u = r$. We repeat this until, after a polynomial number of steps, $r_u - r_l \leq \rho$; then set $r_A = r_l$ and conclude that

$$r_A(K) \leq r_\mathcal{V}(K) < r_u + \rho \leq r_l + 2\rho \leq r_A(K) + 2\rho$$

$$\leq r_A(K) + \frac{\mu \underline{r}}{\gamma_2} \leq (1+\mu) r_A(K).$$

In addition, setting $a_A(K)$ equal to the query point given to the oracle together with $r_A(K)$ yields $a_A(K) + r_A(K)\mathbb{B}_\mathcal{V} \subset K$.

But the problem of either finding a point $a \in S_{K,r}$ or asserting that $S_{K,r}(-\rho\gamma_1) \neq \varnothing$ can be solved in oracle-polynomial time with the central cut ellipsoid method (see Theorem 3.2.1 in [GLS93]), assuming that we can solve a slight modification of the weak separation problem for the set $S_{K,r}$. More exactly, while the second answer of a weak separation oracle does not change, we demand $y \in S_{K,r}$ instead of $y \in S_{K,r}(\varepsilon)$ as the first answer. Now, note that, by Lemma 3.1, the (standard) separation problem for $S_{K,r}$ (a input, $C = r\mathbb{B}_\cdot$ fixed) can be solved in polynomial time. Thus we can complete the proof by noting that the modified oracle just mentioned was derived in [BG97]. □

In particular, it follows from Propositions 1.1 and 1.2 that the width of K can be computed by dealing instead with the inradius of $K - K$, and here is the conclusion.

COROLLARY 3.3. *There exists an oracle-polynomial time algorithm A which, for input consisting of a positive rational μ, a string $\mathbb{B}_\cdot = (n, s; v_1, \ldots, v_s)$ defining the unit ball of a polytopal norm, and a well-bounded body K, delivers a number $w_A(K)$ with*

$$w_A(K) \leqslant w_{\mathbb{B}_\cdot}(K) < (1+\mu) w_A(K).$$

Furthermore, a pair of parallel hyperplanes with distance $(1+\mu)w_A(K)$ that contains K can be computed.

For a 0-symmetric body K, there is an oracle-polynomial-time algorithm that solves the weak separation problem for the polar of K (see [GLS93]). This makes it possible, using the propositions of Subsection 1.A, to reduce the problem of diameter approximation to that of inradius approximation. Simply note that the diameter is invariant under symmetrization, and that, for a centrally symmetric body K, $d(K) = 2R(K)$ and $R(K) = 1/r(K^\circ)$. Here is the specific conclusion.

PROPOSITION 3.4. *There exists an oracle-polynomial-time algorithm A which, for input consisting of a positive rational μ, a string $\mathbb{B}_\cdot = (n, s; Q, b)$ defining the unit ball of a polytopal norm, and a well-bounded body K, delivers a number $d_A(K)$ with*

$$(1-\mu) d_A(K) < d_{\mathbb{B}_\cdot}(K) \leqslant d_A(K).$$

In addition, two points x and y contained in $K(\mu)$ are computed with $\|x - y\|_{\mathbb{B}_\cdot} \geqslant d_{\mathbb{B}_\cdot}(K) - \mu$.

The circumradius is not invariant under symmetrization, but with respect to a given polytopal norm the computation of the circumradius can be approached as follows (giving a rough description in terms of exact arithmetic). Let the polytopal unit ball be $\mathcal{H}$-presented, more precisely, given by $\{x: \pm q_i^T x \leqslant 1 \text{ for } i = 1, \ldots, k\}$. Then the circumradius of K with respect to the induced norm is given as the solution of the linear program that asks for the minimum of ρ such that $\rho \pm u_i^T a \geqslant \delta_i^{\pm}$ for $i = 1, \ldots, k$, where $\delta_i^{\pm} = \max_{x \in K} \pm u_i^T x$, (*cf.* [GK93]). (Note that a is a candidate for the centre of K's

circumsphere with respect to the polytopal norm.) Since a (weak) optimization problem is at hand, the circumradius problem is reduced to a linear optimization problem, and this can be solved in polynomial-time using an ellipsoid algorithm. To be more precise, a binary search with respect to the value v of the objective function is performed, and in each step an ellipsoid algorithm determines whether the intersetion of a convex set with a proper half-space is empty or not. The half-space is determined by a separating hyperplane on which the evaluation of the objective function equals the current binary search value v. This means that we must develop a separation oracle for a convex set that depends on v. The details are omitted (they can be found in [Bri98]), but here is the conclusion.

LEMMA 3.5. *There exists an oracle-polynomial-time algorithm A which, for input consisting of a positive rational μ, a string $\mathbb{B}_{\nearrow} = (n, s; Q, b)$ defining the unit ball of a polytopal norm, and a well-bounded body K, delivers a number $R_A(K)$ with*

$$(1-\mu)R_A(K) < R_{\nearrow}(K) \leqslant R_A(K),$$

and also a point $a_A(K)$ with $a_A(K) + R_A(K)\mathbb{B}_{\nearrow} \supset K$.

Finally, we record the result for norm-maximization,.

LEMMA 3.6. *There exists an oracle-polynomial-time algorithm A which, for input consisting of a positive rational μ with $\mu < 1$, a string $\mathbb{B}_{\nearrow} = (n, s; Q, b)$ defining the unit ball $\mathbb{B}_{\nearrow}$ of a polytopal norm $\|\cdot\|_{\nearrow}$, and a well-bounded convex body K, delivers a number $N_A(K)$ with*

$$\frac{1}{1+\mu} N_A(K) \leqslant N_{\nearrow}(K) \leqslant \frac{1}{1-\mu} N_A(K),$$

and also a point $x_A(K)$ with $\|x_A(K)\|_{\nearrow} = N_A(K)$.

§3.B. *Approximation of l_p unit balls by polytopes.* Recalling our plan to deal with l_p norms by taking solutions with respect to appropriate approximating polytopal norms, we now want to construct, for each fixed $p \in [1, \infty]$, $\nearrow$- and $\nwarrow$-polytopes that approximate the l_p unit ball $\mathbb{B}_p^n$ of $\mathbb{R}^n$ and have encoding length that is bounded by a polynomial in n. In order to treat the case in which p is not an integer, an approach polar to that of Kochol [Koc94] is developed. However, the main idea is taken from his construction of the asymptotically optimal spherical codes in Euclidean space whose existence was shown by Bárány and Füredi [BF88]. When additional effort is necessary, methods of Carl and Pajor [CP88] are used.

The construction is carried out in two stages. We first consider approximations where, given a positive integer η, we are allowed to use an m-polytope with η^m facets or vertices to approximate the m-dimensional unit ball $\mathbb{B}_p^m$. (The approximation error of our specific construction depends only on η and not on the dimension m.) To obtain oracle-polynomial-time algorithms, we then choose m logarithmic in the underlying dimension n and, using the m-polytopes as substructures, we construct n-dimensional $\nearrow$- or $\nwarrow$-polytopes whose encoding

lengths are bounded by a polynomial in n and whose deviations from $\mathbb{B}_p = \mathbb{B}_p^n$ depend on n.

Approximation in m-dimensional subspaces. For the first stage of the construction, let m denote a positive integer. Note that, in the following, *e.g.*, $\mathbb{B}_p = \mathbb{B}_p^m$.

To provide easier reading of the proof, the algorithm for constructing the subspaces is split into two lemmas. In the first lemma it is assumed that all computations can be done with infinite precision. The somewhat tiresome calculations for the Turing model are given in the second lemma.

LEMMA 3.7. *For each $\beta > 1$ and $p \in [1, \infty[$, there is a positive integer $\eta = \eta(p, \beta)$ that has the following property: for each $m \in \mathbb{N}$, there exists a 0-symmetric polytope P with at most η^m facets and with*

$$\mathbb{B}_p \subset P \subset \frac{\beta}{\beta - 1} \mathbb{B}_p.$$

Proof. First note that l_1 is a polytopal norm and that its unit ball, the regular cross-polytope, has 2^m facets. Hence it suffices to consider the case in which $1 < p < \infty$. For $\beta > 1$, we define

$$C' = \mathbb{Z}^m \cap (\beta m^{1/p'}) \mathbb{B}_{p'} \setminus \{0\}, \qquad C = \{c'/\|c'\|_{p'} : c' \in C'\},$$

and claim that the polytope

$$P = \bigcap_{c \in C} \{x : c^T x \leqslant 1\}$$

has the required properties.

That $\mathbb{B}_p \subset P$ follows immediately by polarity from the fact that $C \subset \mathbb{S}_{p'}$. To establish the second inclusion, $P \subset \beta/(\beta - 1)\mathbb{B}_p$, we show that, for each $x \in \mathbb{S}_p$, there exists a $c \in C$ with $c^T x \geqslant (\beta - 1)/\beta$. Starting with $x = (\xi_1, \ldots, \xi_m)^T \in \mathbb{S}_p$, we define the index-sets

$$I_+ = \{i : \xi_i \geqslant 0\} \quad \text{and} \quad I_- = \{i : \xi_i < 0\}$$

and the vector $c' = (\gamma_1', \ldots, \gamma_m')^T$ by setting

$$\gamma_i' = \begin{cases} \lfloor \beta m^{1/p'} |\xi_i|^{p-1} \rfloor, & \text{if } i \in I_+, \\ \lceil -\beta m^{1/p'} |\xi_i|^{p-1} \rceil, & \text{if } i \in I_-. \end{cases}$$

Then $\|c'\|_{p'} \leqslant \beta m^{1/p'} \|x\|_p^{p-1} = \beta m^{1/p'}$, so that $c' \in C'$, and, in addition, using the fact that

$$\|x\|_q \leqslant \|x\|_p \leqslant m^{(q-p)/(pq)} \|x\|_q$$

for $p, q \in \mathbb{R}$ with $1 \leqslant p \leqslant q \leqslant \infty$ and $x = (\xi_1, \ldots, \xi_m)^T \in \mathbb{R}^m$ (see Proposition 1.5), we have

$$\begin{aligned} c'^T x &= \sum_{i=1}^m \xi_i \gamma_i' = \sum_{i \in I_+} \xi_i \gamma_i' + \sum_{i \in I_-} \xi_i \gamma_i' \\ &\geqslant \sum_{i \in I_+} |\xi_i| (\beta m^{1/p'} |\xi_i|^{p-1} - 1) + \sum_{i \in I_-} |\xi_i| (\beta m^{1/p'} |\xi_i|^{p-1} - 1) \\ &= \beta m^{1/p'} \|x\|_p^p - \|x\|_1 \geqslant \beta m^{1/p'} - m^{1/p'}. \end{aligned}$$

Now consider the vector $c = c'/\|c'\|_{p'}$. Obviously, $c \in C$ and, furthermore,

$$c^T x \geq \frac{\beta m^{1/p'} - m^{1/p'}}{\beta m^{1/p'}} = \frac{\beta - 1}{\beta}.$$

It remains to show that, for an appropriate constant η (independent of m), the cardinality of the set C' (and hence of C) is at most η^m. The idea is to associate, with each point c' of the integral lattice $\mathbb{Z}^m$, a cube with side length 1 and centre c'. The volume of each cube is equal to 1 and the cubes do not overlap, so that the cardinality of the set C' is equal to the sum of the volumes of the corresponding cubes. Each cube is contained in $\gamma m^{1/p'} \mathbb{B}_{p'}$ for an appropriate $\gamma > \beta$, and therefore the volume $\mathrm{vol}\,(\gamma m^{1/p'} \mathbb{B}_{p'})$ is an upper bound for $|C|$.

Since

$$\begin{aligned} \|c' + (\pm\tfrac{1}{2}, \ldots, \pm\tfrac{1}{2})^T\|_{p'} &\leq \|c'\|_{p'} + \|(\pm\tfrac{1}{2}, \ldots, \pm\tfrac{1}{2})^T\|_{p'} \\ &\leq \beta m^{1/p'} + \tfrac{1}{2} m^{1/p'} = (\beta + \tfrac{1}{2}) m^{1/p'} \end{aligned}$$

for each $c' \in C'$, it will suffice to set $\gamma = \beta + 1/2$. Using Proposition 1.6, we see that

$$|C| = |C'| \leq \mathrm{vol}\,(\gamma m^{1/p'} \mathbb{B}_{p'}) = \gamma^m m^{m/p'} \,\mathrm{vol}\,(\mathbb{B}_{p'}) = (2\gamma)^m m^{m/p'} \frac{(\Gamma(1 + 1/p))^m}{\Gamma(1 + m/p)}.$$

At this point, we use the following quantitative version of Stirling's formula:

$$\sqrt{2\pi} y^{y+1/2} e^{-y} < \Gamma(1 + y) < \sqrt{2\pi} y^{y+1/2} e^{-y + 1/(12y)} \qquad \text{for } y > 0.$$

This yields the followng inequalities:

$$\Gamma\left(1 + \frac{m}{p'}\right) > \sqrt{2\pi} \left(\frac{m}{p'}\right)^{m/p' + 1/2} e^{-m/p'},$$

and

$$\left(\Gamma\left(1 + \frac{1}{p'}\right)\right)^m < (2\pi)^{m/2} \left(\frac{1}{p'}\right)^{m/p' + m/2} e^{-m/p' + mp'/12}.$$

Hence

$$\begin{aligned} |C| &< \frac{(2\gamma)^m (2\pi/p')^{m/2} e^{mp'/12}}{\sqrt{2\pi m/p'}} < (2\gamma)^m \left(\frac{2\pi}{p'}\right)^{(m-1)/2} e^{mp'/12} \\ &\leq (\max\{1, \sqrt{(2\pi)/p'}\} 2\gamma e^{p'/12})^m, \end{aligned}$$

and setting $\eta = \lceil \max\{1, \sqrt{(2\pi)/p'}\} 2(\beta + 1/2) e^{p'/12} \rceil$ finishes the proof. □

To obtain a (rational) $\mathcal{H}$-polytope we have to modify the construction, due to the restriction to finite precision in the Turing model.

LEMMA 3.8. *For each choice of rationals $\beta, \nu > 1$, and $p \in [1, \infty[$, there is a positive integer $\eta = \eta(p, \beta, \nu)$ that has the following property: for each $m \in \mathbb{N}$ there exists a 0-symmetric (rational) $\mathcal{H}$-polytope P with at most η^m facets and with*

$$\mathbb{B}_p \subset P \subset \nu \frac{\beta}{\beta - 1} \mathbb{B}_p.$$

Proof. Of course, the idea of the construction is the same as in Lemma 3.7, but minor modifications are needed whenever the restriction to finite precision becomes active. To model this, let ε be a positive rational number and k a positive integer with $2^{-k} \leq \varepsilon$. This means that rounding down or up to the kth digit behind the binary point of a number μ leads to an error less than ε. We denote the rational numbers obtained from this rounding process by μ^- and μ^+ respectively, so that

$$\mu - \varepsilon \leq \mu^- \leq \mu^+ \leq \mu + \varepsilon.$$

Now, if given $\nu > 1$, determine ε with $(1 + m\varepsilon)^{1/p'} + \varepsilon \leq \nu$, and choose a number k (which indicates the finite precision of the Turing machine) with $2^{-k} \leq \varepsilon$. Recalling the sets

$$C' = \mathbb{Z}^m \cap (\beta m^{1/p'}) B_{p'} \setminus \{0\}$$

and

$$C = \{c'/\|c'\|_{p'} : c' \in C'\}$$

of the proof of Lemma 3.7, we define their rounded versions (indicated by $\tilde{}$) by setting

$$\tilde{C}' = \mathbb{Z}^m \cap \left\{ \tilde{c}' = (\tilde{\gamma}'_1, \ldots, \tilde{\gamma}'_m)^T : \sum_{i=1}^m (|\tilde{\gamma}'_i|^{p'})^+ \leq ((\beta^{p'})^- + 2\varepsilon)m \right\} \setminus \{0\}$$

and

$$\tilde{C} = \{\tilde{c}'/\psi(\tilde{c}') : \tilde{c}' \in \tilde{C}'\}, \qquad \text{where } \psi(\tilde{c}') = \left(\left(\sum_{i=1}^m (|\tilde{\gamma}'_i|^{p'})^+ \right)^{1/p'} \right)^+.$$

Note that $C' \subset \tilde{C}'$, because, for each $c' = (\gamma'_1, \ldots, \gamma'_m)^T \in C'$, we have

$$\sum_{i=1}^m (|\gamma'_i|^{p'})^+ \leq \sum_{i=1}^m (|\gamma'_i|^{p'} + \varepsilon) \leq (\beta^{p'} + \varepsilon)m \leq ((\beta^{p'})^- + 2\varepsilon)m,$$

and hence $c' \in \tilde{C}'$. From the fact that $C' \subset \tilde{C}'$ it follows that

$$\operatorname{conv} C \subset \operatorname{conv} \{\tilde{c}'/\|\tilde{c}'\|_{p'} : \tilde{c}' \in \tilde{C}'\}.$$

Now, setting $P = \bigcap_{\tilde{c} \in \tilde{C}} \{x : \tilde{c}^T x \leq 1\}$, we claim that $\mathbb{B}_p \subset P \subset (\nu\beta/(\beta - 1))\mathbb{B}_p$. For the first inclusion, just note that, since $\psi(\tilde{c}') \geq \|\tilde{c}'\|_{p'}$, $\tilde{C} \subset \mathbb{B}_{p'}$. For the second, we show that $((\beta - 1)/\beta)\mathbb{B}_{p'} \subset \nu \operatorname{conv} \tilde{C}$. Using Lemma 3.7, we know that $((\beta - 1)/\beta)\mathbb{B}_{p'} \subset \operatorname{conv} C$, and hence it suffices to show that

$$\operatorname{conv} \{\tilde{c}'/\|\tilde{c}'\|_{p'} : \tilde{c}' \in \tilde{C}'\} \subset \nu \operatorname{conv} \{\tilde{c}'/\psi(\tilde{c}') : \tilde{c}' \in \tilde{C}'\} = \nu \operatorname{conv} \tilde{C},$$

because we have already seen that conv C is contained in the set on the left. Since all components of $\tilde{c}'$ are integers, we obtain

$$\frac{\psi(\tilde{c}')}{\|\tilde{c}'\|_{p'}} = \frac{((\sum_{o=1}^{m}(|\tilde{\gamma}_i'|^{p'})^+)^{1/p'})^+}{(\sum_{i=1}^{m}|\tilde{\gamma}_i'|^{p'})^{1/p'}} \leqslant \frac{((\sum_{i=1}^{m}(|\tilde{\gamma}_i'|^{p'}+\varepsilon))^{1/p'})^+}{(\sum_{i=1}^{m}|\tilde{\gamma}_i'|^{p'})^{1/p'}}$$

$$\leqslant \frac{(\sum_{i=1}^{m}(|\tilde{\gamma}_i'|^{p'}+\varepsilon))^{1/p'}+\varepsilon}{(\sum_{i=1}^{m}|\tilde{\gamma}_i'|^{p'})^{1/p'}} \leqslant \left(\frac{\sum_{i=1}^{m}(|\tilde{\gamma}_i'|^{p'}+\varepsilon)}{\sum_{i=1}^{m}|\tilde{\gamma}_i'|^{p'}}\right)^{1/p'}+\varepsilon$$

$$\leqslant (1+m\varepsilon)^{1/p'}+\varepsilon \leqslant \nu,$$

whence the desired conclusion follows.

It remains to show that $|\tilde{C}| \leqslant \eta^m$. Recalling the corresponding part in the proof of Lemma 3.7, it suffices to show that we can determine a number $\tilde{\gamma}$, independent of m, such that $\tilde{C}' \subset \tilde{\gamma} m^{1/p'} \mathbb{B}_{p'}$. For this, take an arbitrary $\tilde{c}' \in \tilde{C}'$. Then

$$\|\tilde{c}'\|_{p'}^{p'} = \sum_{i=1}^{m}|\tilde{\gamma}_i'|p' \leqslant \sum_{i=1}^{m}(|\tilde{\gamma}_i'|^{p'})^+ \leqslant ((\beta^{p'})^- + 2\varepsilon)m \leqslant ((\beta^{p'})^- + 2\nu)m,$$

and we can continue as in the proof of Lemma 3.7. □

Polynomial-size approximation. Now let us show how the construction in m-dimensional subspaces of $\mathbb{R}^n$ can be used to produce full-dimensional polytopes.

LEMMA 3.9. *For each rational $\beta > 1$ and rational $p \in [1, \infty]$, there are positive numbers $\gamma = \gamma(\beta, p)$ and $\eta = \eta(\beta, p)$ for which the following is true: for each n, $h \in \mathbb{N}$ with $2n \leqslant h < n\eta^n$, there exists a 0-symmetric $\mathscr{H}$-polytope $\mathbb{B}_{\mathscr{H}}$ with at most h facets such that*

$$\mathbb{B}_p \subset \mathbb{B}_{\mathscr{H}} \subset \left(\frac{\gamma\eta}{\log(h/n)}\right)^{1/p} \mathbb{B}_p,$$

and there exists a 0-symmetric $\mathscr{V}$-polytope $\mathbb{B}_{\mathscr{V}}$ with at most h vertices such that

$$\left(\frac{\log(h/n)}{\gamma n}\right)^{1/p'} \mathbb{B}_p \subset \mathbb{B}_{\mathscr{V}} \subset \mathbb{B}_p.$$

Proof. Since the two conclusions are equivalent under polarity, attention may be confined to the search for $\mathbb{B}_{\mathscr{H}}$. The case $p = \infty$ is trivial, and so we assume that $1 \leqslant p < \infty$. By Lemma 3.8, there exist, for each $\beta > 1$, a number $\eta(\beta, p)$ such that, for each $m \in \mathbb{N}$, we can construct a 0-symmetric m-dimensional $\mathscr{H}$-polytope $\mathbb{B}_{\mathscr{H}}^m$ with at most η^m facets and with

$$\mathbb{B}_p^m \subset \mathbb{B}_{\mathscr{H}}^m \subset \frac{\beta}{\beta-1}\mathbb{B}_p^m.$$

(Note that the parameter ν in Lemma 3.8 was introduced only for technical reasons, to facilitate the deduction of that lemma from Lemma 3.7. Hence Lemma 3.8 could be reformulated without ν.)

When $2n \leq h \leq \eta^2 n$, the desired n-dimensional $\mathcal{H}$-polytope $\mathbb{B}_{\mathcal{H}}$ is obtained by setting $\mathbb{B}_{\mathcal{H}} = \mathbb{B}_\infty^n$, and recalling that $\|x\|_p = n^{1/p}$ for each vertex x of $\mathbb{B}_\infty^n$. Now suppose, on the other hand, that $\eta^2 n < h$, and define

$$m = \left\lfloor \log_\eta \frac{h}{\eta} \right\rfloor \quad \text{and} \quad s = \left\lceil \frac{n}{m} \right\rceil.$$

Since $h < n\eta^n$ we have $m < n$, and interpret $\mathbb{R}^n$ as $\mathbb{R}^m \times \cdots \times \mathbb{R}^m \times \mathbb{R}^{\tilde{m}}$ with $n - (s-1)m = \tilde{m} \leq m$ and s a positive integer. Then apply Lemma 3.7 in each of the $s-1$ copies $S_1, \ldots, S_{s-1}$ of $\mathbb{R}^m$ and in the copy S_s of $\mathbb{R}^{\tilde{m}}$. For $1 \leq j \leq s$, let C_j denote the set of outer normals defining the $\mathcal{H}$-polytope approximating $\mathbb{B}_p^m$ or $\mathbb{B}_p^{\tilde{m}}$, and let $\hat{c}_j$ denote the canonical embedding of S_j into $\mathbb{R}^n$. Then setting

$$P = \bigcap_{j=1}^{s} \bigcap_{c \in C_j} \{x : \hat{c}_j(c)^T x \leq 1\}$$

guarantees that, for each $x \in P$, $\|x^{P_j}\|_p \leq \beta/(\beta-1)$, where x^{P_j} denotes the projection of x into S_j. Hence, using $m \geq 2$,

$$\begin{aligned}
\|x\|_p^p &= \sum_{j=1}^{s} \|x^{P_j}\|_p^p \leq s \max_{1 \leq j \leq s} \|x^{P_j}\|_p^p \leq \left(\frac{n}{m} + 1\right)\left(\frac{\beta}{\beta-1}\right)^p \\
&\leq \left(1 + \frac{n}{\log_\eta (h/n) - 1}\right)\left(\frac{\beta}{\beta-1}\right)^p \\
&\leq 3 \frac{n}{\log_\eta (h/n)}\left(\frac{\beta}{\beta-1}\right)^p \\
&= \frac{3}{\log_\eta 2} \frac{n}{\log (h/n)}\left(\frac{\beta}{\beta-1}\right)^p,
\end{aligned}$$

and setting

$$\gamma = \frac{3}{\log_\eta 2}\left(\frac{\beta}{\beta-1}\right)^p$$

yields

$$\mathbb{B}_{\mathcal{H}} \subset \left(\gamma \frac{n}{\log (h/n)}\right)^{1/p} \mathbb{B}_p.$$

As before, the inclusion $\mathbb{B}_p \subset \mathbb{B}_{\mathcal{H}}$ follows from a polarity argument, and so we can finish the proof by showing that the number f of facets is at most h. In fact, since $n, m \geq 2$, we see that

$$f \leq s\eta^m \leq \left(\frac{n}{m} + 1\right)\frac{h}{n} = \frac{h}{m} + \frac{h}{n} \leq h. \qquad \square$$

Improving the performance by using Hadamard matrices. In attempting to improve Lemma 3.9, we encounter an interesting phenomenon that is caused

by our restriction on the encoding size of the polytope approximating the unit ball. It can be explained as follows.

Suppose that, working in the n-dimensional l_p space $\mathbb{R}_p^n$, we may choose between $n^{1/p'}\mathbb{B}_1$ and $\mathbb{B}_\infty$ for outer approximation of $\mathbb{B}_p$ by an n-polytope P that has small circumradius $R_p(P)$. Since $R_p(n^{1/p'}\mathbb{B}_1) = n^{1/p'}$ and $R_p(\mathbb{B}_\infty) = n^{1/p}$, taking $\mathbb{B}_\infty$ is better when $p > 2$ and worse when $p < 2$. However, if we want to use the containing polytope as the basis of an oracle-polynomial-time approximation algorithm for the circumradius of a body in $\mathbb{R}_p^n$, we are always forced to choose $\mathbb{B}_\infty$ because $\mathbb{B}_1$ has 2^n facets.

Even though the set $n^{1/p'}\mathbb{B}_1$ itself cannot serve as the desired polytope, $\mathbb{B}_1$ will serve as a guide for our (suboptimal) procedure, which is that of producing a 0-symmetric n-dimensional $\mathscr{H}$-polytope P such that $\mathbb{B}_p \subset P$, each facet normal of P is also a facet normal of $\mathbb{B}_1$, and the total number of facets of P is not too large. Certain invertible linear transformations play a role in the construction of P, and these mappings are defined with the aid of Hadamard matrices (hereafter, *H-matrices*). To provide a better understanding of the method, we start with the simple case of the unit cube $\mathbb{B}_\infty$. In the dual situation the idea is to transform $\mathbb{B}_1$ by using H-matrices, a technique used by Carl and Pajor to show that, when $2 \leq p < \infty$, their estimates in [CP88] for $\mathscr{H}$-approximation of the l_p unit ball with respect to the volume are asymptotically optimal when the number of allowable vertices is linear in the dimension.

An *H-matrix of order n* is an $n \times n$ matrix whose entries are all -1 or 1 and whose rows (and columns) are pairwise orthogonal. The integer n will be called an *H-number* when such a matrix exists. It is well known that, aside from 1 and 2, each H-number is divisible by 4. A long-standing conjecture is that every multiple of 4 is an H-number, but this is still open for infinitely many such multiples. (See [SY92] for a survey of the problem.) However, from our algorithmic viewpoint this difficulty can be handled by approximating $\mathbb{R}^n$ by a relatively small collection of mutually orthogonal subspaces, in each of which H-matrices are given explicitly.

That each power of 2 is an H-number is a consequence of the following well-known recursive construction:

$$H_{2^0} = (1) \quad \text{and} \quad H_{2^{k+1}} = \begin{pmatrix} H_{2^k} & H_{2^k} \\ H_{2^k} & -H_{2^k} \end{pmatrix}, \qquad k \in \mathbb{N} \cup \{0\}.$$

Our algorithms will use these H-matrices, which were first described by Sylvester [Syl67]. The next lemma shows that the sort of mapping we need can be performed by any H-matrix.

LEMMA 3.10. *If there exists an $n \times n$ H-matrix H, then, for each $p \in [1, 2]$, there exists a 0-symmetric n-polytope P with $2n$ facets such that*

$$\mathbb{B}_p \subset P \subset n^{1/2}\mathbb{B}_p,$$

and, for each $p \in [2, \infty]$, there exists a 0-symmetric n-polytope Q with $2n$ vertices such that

$$n^{-1/2}\mathbb{B}_p \subset Q \subset \mathbb{B}_p.$$

Proof. Because of polarity, it suffices to consider the first statement. With

$$\mathbb{B}_\infty = \bigcap_{1 \leq i \leq n} \{x : \pm e_i^T x \leq 1\},$$

consider the polytope

$$P = n^{-1/p} H \mathbb{B}_\infty = \bigcap_{1 \leq i \leq n} \{x : \pm n^{-1/p'} (He_i)^T x \leq 1\}.$$

Since $\|n^{-1/p'} He_i\|_{p'} = 1$, $\mathbb{B}_p \subset P$. Furthermore, for each $x \in P$, there exists a point $y \in \mathbb{B}_\infty$ with $x = n^{-1/p} Hy$, and we conclude that

$$\|x\|_p = n^{-1/p} \|Hy\|_p \leq n^{-1/2} \|Hy\|_2 \leq \|y\|_2 \leq n^{1/2}. \qquad \square$$

Now we use orthogonal subspaces to obtain sufficient approximations even in dimensions for which no H-matrix is known or existent.

LEMMA 3.11. *For each $p \in [1, \infty]$, there is a number $\gamma = \gamma(p)$ that has the following property: if $p \in [1, 2]$, then there exists a 0-symmetric n-polytope P with $2n$ facets such that*

$$\mathbb{B}_p \subset P \subset \gamma n^{1/2} \mathbb{B}_p,$$

and, if $p \in [2, \infty]$, then there exists a 0-symmetric n-polytope Q with $2n$ vertices such that

$$\gamma^{-1} n^{-1/2} \mathbb{B}_p \subset Q \subset \mathbb{B}_p.$$

Proof. Let $l = \lfloor \log n \rfloor$, and let $d = (\delta_0, \ldots, \delta_l)^T$ denote the $\{0, 1\}^{l+1}$-vector uniquely determined by $n = \sum_{k=0}^{l} \delta_k 2^k$. Whenever $\delta_k = 1$, we use the $2^k \times 2^k$ Sylvester matrix to construct a 2^k-polytope P^{2^k} with 2^{k+1} facets and $\mathbb{B}_p^{2^k} \subset P^{2^k} \subset (2^k)^{1/2} \mathbb{B}_p^{2^k}$.

Now, using the same embedding technique and notation as in the proof of Lemma 3.9, we obtain pairwise orthogonal subspaces $S_0, \ldots, S_l$ with $\dim(S_k) = \delta_k 2^k$, and an n-polytope P that contains $\mathbb{B}_p$ and has $\sum_{k=0}^{l} \delta_k 2^{k+1} = 2n$ facets. Furthermore, it is true for each $x \in P$ that

$$\|x\|_p^p = \sum_{\substack{k=0 \\ k:\delta_k = 1}}^{l} \|x^{P_k}\|_p^p \leq \sum_{k=0}^{l} (2^{p/2})^k = \frac{2^{p(l+1)/2} - 1}{2^{p/2} - 1} < \frac{2^{p/2}}{2^{p/2} - 1} n^{p/2},$$

and hence that $\|x\|_p \leq \gamma \sqrt{n}$, where the multiplier $\gamma = 2^{1/2} / (2^{p/2} - 1)^{1/p}$ is independent of n. $\square$

Although this simple construction is optimal for $1 < p \leq 2$ when we are restricted to a linear number of facets, it seems obvious (and turns out to be true) that allowing a polynomial of higher degree should lead to a better approximation. Again it seems natural to transform "simple" polytopes in such a way that all outer normals are chosen from the set of outer normals of $\mathbb{B}_1$. However, controlling this behaviour turns out to be difficult, and hence our actual approach is based on the more manageable idea of choosing outer normals that are, in a sense, the outer normals of certain lower-dimensional cross-polytopes.

LEMMA 3.12. *For each $\beta > 1$ and $p \in [1, 2]$, there is a number $\eta = \eta(\beta, p)$ that has the following property: for all $m \in \mathbb{N}$, $k \in \mathbb{N} \cup \{0\}$, there exists a 0-symmetric $(2^k m)$-polytope P with at most $2^k \eta^m$ facets such that $\mathbb{B}_p \subset P \subset (\beta/(\beta-1)) 2^{k/2} m^{1/p - 1/2} \mathbb{B}_p$.*

Proof. First we define a generalization of the Sylvester matrices by setting

$$H_{2^0} = I \quad \text{and} \quad H_{2^{k+1}} = \begin{pmatrix} H_{2^k} & H_{2^k} \\ H_{2^k} & -H_{2^k} \end{pmatrix}, \qquad k \in \mathbb{N} \cup \{0\},$$

where I denotes the $m \times m$ identity matrix. Then H_{2^k} is a $2^k m \times 2^k m$-matrix whose eigenvalues are $\pm\sqrt{2^k}$, and it is obvious that $H_{2^k} = H_{2^k}^T$ and $H_{2^k}^{-1} = 2^{-k} H_{2^k}$.

Now, given m, p and β as input, use Lemma 3.7 to construct an m-dimensional polytope P with at most η^m facets and $\mathbb{B}_p^m \subset P^m \subset (\beta/(\beta-1)) \mathbb{B}_p^m$. Let $\tilde{P}$ denote the $(2^k m)$-polytope obtained by applying the construction method of Lemma 3.9 (using 2^k orthogonal subspaces), and let C be the set of its normalized outer normals, *i.e.*, $\tilde{P} = \bigcap_{c \in C} \{x : c^T x \leq 1\}$. It follows that $|C| \leq 2^k \eta^m$ and

$$P := 2^{-k/p} H \tilde{P} = \bigcap_{c \in C} \{x : 2^{-k/p'} (Hc)^T x \leq 1\},$$

where $H = H_{2^k}$. By the construction we obtain $\|2^{-k/p'} Hc\|_{p'} = 1$, whence $\mathbb{B}_p \subset P$.

Furthermore, for each $x \in P$ there exists a unique point $y \in \tilde{P}$ with $x = 2^{-k/p} Hy$, and we continue with

$$\begin{aligned} \|x\|_p &= 2^{-k/p} \|Hy\|_p \leq 2^{-k/p} (2^k m)^{1/p - 1/2} \|H\|_2 \|y\|_2 \\ &= m^{1/p - 1/2} \|y\|_2 \leq m^{1/p - 1/2} \left(\sum_{i=1}^{2^k} \left(\frac{\beta}{\beta - 1} \right)^2 \right)^{1/2} \\ &\leq m^{1/p - 1/2} \frac{\beta}{\beta - 1} 2^{k/2}. \end{aligned}$$

□

As before, we can extend this result to arbitrary dimensions.

LEMMA 3.13. *For each $\beta > 1$ and $p \in [1, \infty]$, there are positive numbers $\gamma = \gamma(\beta, p)$ and $\eta = \eta(\beta, p)$ such that the following holds for all n, $h \in \mathbb{N}$ with $2n \leq h < n\eta^n$: if $p \in [1, 2]$, then there exists a 0-symmetric $\mathscr{H}$-polytope $\mathbb{B}_\mathscr{H}$ with at most h facets such that*

$$\mathbb{B}_p \subset \mathbb{B}_\mathscr{H} \subset \frac{\gamma n^{1/2}}{(\log(h/n))^{1/p'}} \mathbb{B}_p,$$

and if $p \in [2, \infty]$ there exists a 0-symmetric polytope $\mathbb{B}_\mathscr{V}$ with at most h vertices such that

$$\frac{(\log(h/n))^{1/p}}{\gamma n^{1/2}} \mathbb{B}_p \subset \mathbb{B}_\mathscr{V} \subset \mathbb{B}_p.$$

Proof. Again it suffices, because of polarity, to consider the case when $p \in [1, 2]$. Rather than explicitly producing the $\mathscr{H}$-polytope $\mathbb{B}_\mathscr{H}$ as described,

we merely show the existence of a (not necessarily rational) polytope (called P) of the desired sort. To produce $\mathbb{B}_{p'}$ then requires a rounding argument that is left to the reader. This argument slightly increases the value of the constants γ and η, but does not affect their existence or their independence of the dimension.

If $h \leq \eta^2 n$, where η is defined as in Lemma 3.7, then Lemma 3.11 can be applied here. Therefore it remains only to study the case in which $h > \eta^2 n$, and we choose (given β, p and n) m as in the proof of Lemma 3.9. Now define $l = \lfloor \log n/m \rfloor$, and compute $(\delta_0, \ldots, \delta_l)^T \in \{0,1\}^{l+1}$ and $\tilde{m} \in \mathbb{N}$, with $0 \leq \tilde{m} < m$ and $n = \sum_{k=0}^{l} \delta_k m 2^k + \tilde{m}$. If $\delta_k = 1$, we apply Lemma 3.12 and obtain a $(2^k m)$-polytope $P^{2^k m}$ with at most $2^k \eta^m$ facets and with

$$\mathbb{B}_p^{2^k m} \subset P^{2^k m} \subset \frac{\beta}{\beta - 1} 2^{k/2} m^{1/p - 1/2} \mathbb{B}_p^{2^k m}.$$

In addition, if $\tilde{m} \neq 0$, then we apply Lemma 3.7 in dimension $\tilde{m}$, and denote by $x^{P^{\tilde{m}}}$ that part of an n-vector x lying in the $\tilde{m}$-dimensional subspace (set $\|x^{P^{\tilde{m}}}\|_p = 0$ if $\tilde{m} = 0$). Using the same embedding as before, we obtain an n-polytope $P \supset \mathbb{B}_p$ with at most

$$\sum_{k=0}^{l} \eta^m 2^k + \eta^{\tilde{m}} \leq \eta^m 2^{l+1} \leq 2 \frac{h}{n} \frac{n}{m} \leq h$$

facets. We conclude, for any $x \in P$, that

$$\begin{aligned} \|x\|_p^p &= \sum_{\substack{k=0 \\ k:\delta_k = 1}}^{l} \|x^{P_k}\|_p^p + \|x^{P^{\tilde{m}}}\|_p^p \\ &\leq \left(\frac{\beta}{\beta - 1}\right)^p (m^{1/p - 1/2})^p \left(\sum_{k=0}^{l} (2^{p/2})^k + 1 \right) \\ &\leq \left(\frac{\beta}{\beta - 1}\right)^p (m^{1/p - 1/2})^p \frac{2^{p/2}}{2^{p/2} + 1} 2^{pl/2} \\ &\leq \left(\frac{\beta}{\beta - 1}\right)^p (m^{1/p - 1/2})^p \frac{2^{p/2}}{2^{p/2} - 1} \left(\frac{n}{m}\right)^{p/2}. \end{aligned}$$

Hence

$$\|x\|_p \leq \gamma \frac{n^{1/2}}{(\log (h/n))^{1/p'}},$$

where γ can obviously be chosen independently of n and h. □

Although Lemma 3.13 improves Lemma 3.11 by gaining a logarithmic factor, we conjecture that this result is still not optimal.

To end this section, we summarize its results that are used in what follows.

THEOREM 3.14. *For each rational $p \in [1, \infty]$ there is a polynomial-time algorithm which, given n as input, delivers a 0-symmetric n-dimensional p-polytope $\mathbb{B}_{p'}$ and a 0-symmetric n-dimensional p-polytope $\mathbb{B}_p$, such that the*

conditions listed in Table 2 are satisfied for constants γ_i that depend on p but not on the dimension n.

Table 2. Polynomial-time approximation of l_p unit balls by $\mathcal{P}$- and $\mathcal{K}$-polytopes.

$\mathbb{B}_p^n \subset \mathbb{B}_{\mathcal{P}} \subset \gamma_1 n^{1/2} \mathbb{B}_p^n$,	if $p = 1$,
$\mathbb{B}_p^n \subset \mathbb{B}_{\mathcal{K}} \subset \gamma_2 \frac{n^{1/2}}{(\log n)^{1/p'}} \mathbb{B}_p^n$,	if $1 < p \leq 2$,
$\mathbb{B}_p^n \subset \mathbb{B}_{\mathcal{P}} \subset \gamma_3 \left(\frac{n}{\log n}\right)^{1/p} \mathbb{B}_p^n$,	if $2 < p < \infty$,
$B_p^n = \mathbb{B}_{\mathcal{K}}$,	if $p = \infty$,
$\mathbb{B}_{\mathcal{P}} = B_p^n$,	if $p = 1$,
$\frac{1}{\gamma^3}\left(\frac{\log n}{n}\right)^{1/p'} \mathbb{B}_p^n \subset \mathbb{B}_{\mathcal{P}} \subset \mathbb{B}_p^n$,	if $1 < p \leq 2$,
$\frac{1}{\gamma^2} \frac{(\log n)^{1/p}}{n^{1/2}} \mathbb{B}_p^n \subset \mathbb{B}_{\mathcal{P}} \subset \mathbb{B}_p^n$,	if $2 < p < \infty$,
$\frac{1}{\gamma_1} \frac{1}{n^{1/2}} \mathbb{B}_p^n \subset \mathbb{B}_{\mathcal{P}} \subset \mathbb{B}_p^n$,	if $p = \infty$.

Proof. The results follow from Lemmas 3.9 and 3.13, if we choose polytopes whose size can be bounded by a polynomial in n. Note that the determination of the sets containing the, say, vertices of the $\mathcal{P}$-polytope, can be done in polynomial time. □

§3.C. *Deterministic algorithms for approximating radii.* Now we combine the results obtained in Subsections 3.A and 3.B.

First note that, if $\tau_1 \leq 1 \leq \tau_2$, then from $\tau_1 \mathbb{B}_p \subset \mathbb{B}_{\mathcal{P}} \subset \mathbb{B}_p$ it follows that $\tau_1 \tau_{\mathcal{P}}(K) \leq r_p(K) \leq r_{\mathcal{V}}(K)$, and from $\mathbb{B}_p \subset \mathbb{B}_{\mathcal{K}} \subset \tau_2 \mathbb{B}_p$ it follows that

$$R_{\mathcal{P}}(K) \leq R_p(K) \leq \tau_2 R_{\mathcal{K}}(K) \quad \text{and} \quad N_{\mathcal{K}}(K) \leq N_p(K) \leq \tau_2 N_{\mathcal{K}}(K).$$

Then it is easy to prove

THEOREM 3.15. *For each rational $p \in [1, \infty]$, the lower bounds for the accuracy of oracle-polynomial-time approximation are as indicated in Table 3.*

Table 3. Lower bounds for accuracy of deterministic oracle-polynomial-time approximation of radii.

p	1	$1 < p \leq 2$	$2 \leq p < \infty$	∞
r_p, w_p	$\mathbb{DOP}$	$\Omega\left(\left(\frac{\log n}{n}\right)^{1/p'}\right)$	$\Omega\left(\frac{(\log n)^{1/p}}{n^{1/2}}\right)$	$\Omega\left(\frac{1}{n^{1/2}}\right)$
R_p, d_p, N_p	$\Omega\left(\frac{1}{n^{1/2}}\right)$	$\Omega\left(\frac{(\log n)^{1/p'}}{n^{1/2}}\right)$	$\Omega\left(\left(\frac{\log n}{n}\right)^{1/p}\right)$	$\mathbb{DOP}$

Proof. Briefly, given n as input, we approximate the l_p unit ball by an appropriate polytope, using the results of Subsection 3.B. For this we choose,

depending on the measurement in question, either an outer approximation $\mathbb{B}_{\nearrow}$ of $\mathbb{B}_p$ with a polynomial number of facets or an inner approximation $\mathbb{B}_{\searrow}$ of $\mathbb{B}_p$ with a polynomial number of vertices, *i.e.*, we obtain either $\tau_1\mathbb{B}_p \subset \mathbb{B}_{\searrow} \subset \mathbb{B}_p$ or $\mathbb{B}_p \subset \mathbb{B}_{\nearrow} \subset \tau_2\mathbb{B}_p$, where the exact values for τ_1 and τ_2 (depending on n and the degree of the polynomial bounding the complexity of the algorithm) can be found in Lemmas 3.9 and 3.13. Then we solve the polytopal problem with the algorithms of Subsection 3.A (after choosing an error parameter $\mu > 1$), and take this solution as an approximation for the original problem. This yields the following estimates of accuracy for oracle-polynomial-time approximation algorithms.

Inradius:

$$\tau_1 r_A(K) \leq \tau_1 r_{\searrow}(K) \leq r_p(K) \leq r_{\searrow}(K) < (1+\mu) r_A(K).$$

Width:

$$\begin{aligned}\tau_1 w_A(K) &\leq \tau_1 w_{\searrow}(K) = \tfrac{1}{2}\tau_1 w_{\searrow}(K-K) = \tfrac{1}{2}\tau_1 r_{\searrow}(K-K)\\ &\leq \tfrac{1}{2} r_p(K-K) = \tfrac{1}{2} w_p(K-K)\\ &= w_p(K) \leq \tfrac{1}{2} r_{\searrow}(K-K) = \tfrac{1}{2} w_{\searrow}(K-K)\\ &= w_{\nearrow}(K) < (1+\mu) w_A(K).\end{aligned}$$

Circumradius:

$$(1-\mu) R_A(K) < R_{\nearrow}(K) \leq R_p(K) \leq \tau_2 R_{\nearrow}(K) \leq \tau_2 R_A(K).$$

Diameter:

$$\begin{aligned}(1-\mu) d_A(K) < d_{\nearrow}(K) &= \tfrac{1}{2} d_{\nearrow}(K-K) = \tfrac{1}{2} R_{\nearrow}(K-K)\\ &\leq \tfrac{1}{2} R_p(K-K) = \tfrac{1}{2} d_p(K-K) = d_p(K)\\ &\leq \tfrac{1}{2}\tau_2 R_{\nearrow}(K-K) = \tau_2 d_{\nearrow}(K)\\ &\leq \tau_2 d_A(K).\end{aligned}$$

Norm-maximization:

$$\frac{1}{1+\mu} N_A(K) \leq N_{\nearrow}(K) \leq N_p(K) \leq \tau_2 N_{\searrow}(K) \leq \frac{1}{1-\mu}\tau_2 N_A(K).$$

Since $\mu > 1$ can be chosen arbitrarily, we obtain the desired results using the values computed for the polytopal norms as approximations for the values with respect to the l_p norm. □

For bodies that are $\mathcal{V}$-presented or $\mathcal{H}$-presented polytopes, the lower bounds in Theorem 3.15 hold for ordinary polynomial-time computation, and the two occurrences of $\mathbb{DOP}$ can be replaced by $\mathbb{P}$. This follows from the fact that for such bodies the weak separation problem can be solved strongly (*i.e.*, setting $\varepsilon = 0$). (In other words, a genuinely polynomial-time oracle is available.) These lower bounds apply to both types of presentation, which is of interest in the case of pairs (measurement, type of presentation) for which the problem of exact computation is $\mathbb{NP}$-hard. See [GK93] for the classification.

as to $\mathbb{NP}$-hardness or ordinary polynomial-time solvability, of radius computation.

It should be mentioned once more that the general idea of approximating bodies by polytopes is an old one, and that for each *fixed* dimension, rather sharp results are available (see especially [Gru93] for the investigation of the asymptotic behaviour in fixed dimension with respect to the number of vertices or facets). Also, it is noted in [Dud94] that the inradius of a convex body can be approximated by replacing the body step by step with an approximating $\mathscr{H}$-polytope whose inradius can be computed with arbitrary accuracy; however, complexity aspects are not considered there.

§3.D. *Entropy numbers, Rademacher type, and volume ratios.* This subsection is devoted to the proof of Proposition 1.7, which is used in Subsection 3.E to derive upper bounds for the accuracy of deterministic approximation of radii in l_p-spaces.

After defining dyadic entropy and Rademacher type, we state two results (Propositions 3.16 and 3.17) involving these notions and then show how they can be used to prove Proposition 1.7. Finally, we prove Propositions 3.16 and 3.17.

Entropy Numbers. When $\mathbb{B}_E$ and $\mathbb{B}_F$ are the unit balls of Banach spaces E and F, $k\in\mathbb{N}$ and $u: E\to F$ is a linear operator, the kth *entropy number* $\mathrm{ent}_k(u)$ of u is the infimum of all $\varepsilon>0$ such that the image $u(\mathbb{B}_E)$ can be covered by k translates of the ε-ball $\varepsilon\mathbb{B}_F$. The *dyadic* entropy numbers $\varepsilon_k(u)$ are defined by $\varepsilon_k(u)=\mathrm{ent}_{2^{k-1}}(u)$. It follows from these definitions that $\mathrm{vol}(u\mathbb{B}_E))/\mathrm{vol}(\mathbb{B}_F)\leqslant 2^{k-1}\varepsilon_k^n(u)$, where $n=\dim(F)$. Thus upper bounds on (dyadic) entropy numbers can be used to provide upper bounds on volume ratios.

To obtain good upper bounds on entropy numbers requires finding sparse coverings of bodies by small balls. Such covering problems are well-known for their difficulty, and it is a common experience that, in all but the most tractable situations, random methods may provide the best approach. Thus it is not surprising that the next definition involves an averaging procedure. This procedure will be involved, through the use of a theorem on F-valued random variables, in establishing bounds on entropy numbers.

(RADEMACHER-) TYPE g. For $g\in[1,2]$, a Banach space F is said to be *of (Rademacher-) type g* if there is a constant C such that

$$\left(\frac{1}{2^l}\sum_{\lambda_i=\pm 1}\left\|\sum_{i=1}^{l}\lambda_i x_i\right\|^2\right)^{1/2}=\left(\int_0^1\left\|\sum_{i=1}^{l}r_i(t)x_i\right\|^2 dt\right)^{1/2}\leqslant C\left(\sum_{i=1}^{l}\|x_i\|^g\right)^{1/g}$$

for each finite sequence $x_1,\ldots,x_l$ of points of F, where r_i denotes the Rademacher function defined by $r_i(t)=\mathrm{sign}\,(\sin 2^i\pi t)$ for $t\in[0,1]$ and $i\in\mathbb{N}$. The *type g constant* of F is defined as the infimum of such constants C, and is denoted by $\tau_g(F)$. (The terminology *space of type p* is standard in discussing entropy numbers, but to avoid confusion with l_p spaces we speak in the definition of *spaces of type g*.)

In the above definition, "constant" means independent of the choice of l and of the vectors $x_1, \ldots, x_l$, but it permits dependence on the dimension of the space. For a geometric interpretation, note that in Euclidean space the inequality becomes, with $C = 1$, the equality known as the *parallelotope equality*.

The above definition does not restrict a Banach space to be of unique type; indeed, for each $(p, g) \in [1, \infty] \times [1, 2]$ the Banach space l_p^n is of type g. See [TJ88, MS86] for details, including the corresponding type constants that are in general dependent on the dimension of the space. For our purpose it suffices to deal with the case $g = \min\{p, 2\}$.

PROPOSITION 3.16. *The n-dimensional space l_p^n is of type $g = \min\{p, 2\}$, with associated type g constants $\tau_p(l_p^n) \leq 3$ if $1 \leq p \leq 2$, $\tau_2(l_p^n) \leq 3\sqrt{2}(\Gamma((1+p)/2)/\Gamma(\frac{1}{2}))^{1/p}$ if $2 < p < \infty$, and $\tau_2(l_\infty^n) \leq 3\sqrt{e}\sqrt{1+\ln n}$.*

The next result is a version of part of Proposition 1 in a paper of Carl [Car85] that turns out to be appropriate for our purposes. A proof (along the lines of the original) is presented later in order to make sure that the result serves our needs.

PROPOSITION 3.17. *If $h, k \in \mathbb{N}$ with $20 \log((h/k)+1) \leq k \leq h$, and u is a linear operator from l_1^h to a Banach space F of type g, then*

$$\varepsilon_k(u) \leq 4 \cdot 20^{1-1/g} \tau_g(F) \left(\frac{\log((h/k)+1)}{k} \right)^{1-1/g} \|u\|,$$

where $\|u\| = \sup_{x \in \mathbb{B}_1^h} \|u(x)\|_F$.

Here, for convenient reference, is a restatement and proof of Proposition 1.7. As was mentioned in Subsection 1.B, the purpose of this result is to elucidate the dependence on the ambient dimension of certain "constants" in results of [Car85] and [CP88].

PROPOSITION 3.18. *For each $p \in [1, \infty]$, for each choice of $h, n \in \mathbb{N}$ with $20 \log((h/n)+1) \leq n \leq h$, and for each 0-symmetric n-polytope $P \subset \mathbb{B}_p^n$ with at most 2h vertices, it is true that*

$$\left(\frac{\mathrm{vol}(P)}{\mathrm{vol}(\mathbb{B}_p^n)} \right)^{1/n} \leq 24 \cdot 20^{1-1/p} \left(\frac{\log((h/n)+1)}{n} \right)^{1-1/p} \quad \text{for } 1 \leq p \leq 2,$$

$$\left(\frac{\mathrm{vol}(P)}{\mathrm{vol}(\mathbb{B}_p^n)} \right)^{1/n} \leq 24 \cdot 40^{1/2} \left(\Gamma\left(\frac{1+p}{2} \right) / \Gamma\left(\frac{1}{2} \right) \right)^{1/p} \left(\frac{\log((h/n)+1)}{n} \right)^{1/2}$$

$$\text{for } 2 < p < \infty,$$

$$\left(\frac{\mathrm{vol}(P)}{\mathrm{vol}(\mathbb{B}_\infty^n)} \right)^{1/n} \leq 24 \cdot (20e)^{1/2} (1+\ln n)^{1/2} \left(\frac{\log((h/n)+1)}{n} \right)^{1/2}.$$

Proof. Let $\pm x_1, \ldots, \pm x_h$ denote the vertices of the polytope P. In Proposition 3.17, choose $F = l_p^n$, $k = n$, and define a linear operator u from $E = l_1^h$

to l_p^n by $\pm e_i \mapsto \pm x_i$ for $1 \leq i \leq h$. Obviously, $u(\mathbb{B}_1^h) = P$ and hence, using $\|u\|_p \leq 1$ and Propositions 3.16 and 3.17, the result follows from the types and type g-constants of the l_p^n spaces. □

It remains to prove Propositions 3.16 and 3.17. For the former, we use inequalities due to Khintchine [Khi23] and Kahane [Kah68]. See also [Pie80] and [LT79] for more information on the constants.

KHINTCHINE'S INEQUALITY. For each $s \in]0, \infty[$, $n \in \mathbb{N}$, and $x \in \mathbb{R}^n$, it is true that

$$\frac{1}{2^n} \sum_{e \in \{-1,1\}^n} |x^T e|^s \leq c_s^s \|x\|_2^s,$$

where $c_s = 1$ for $0 < s \leq 2$, and $c_s = \sqrt{2}(\Gamma((1+s)/2)/\Gamma(1/2))^{1/s}$ otherwise.

KAHANE'S INEQUALITY. For each $s \in]1, \infty[$, let $K_s = ((2s-1)/(s-1))^{s-1}$. Then, for each finite sequence $x_1, \ldots, x_l$ of points in an arbitrary Banach space,

$$\int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\| dt \leq \left(\int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\|^s dt \right)^{1/s} \leq K_s \int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\| dt.$$

Proof of Proposition 3.16. For any $x_1, \ldots, x_l \in \mathbb{R}^n$, with $x_i = (\xi_{i1}, \ldots, \xi_{in})^T$ for $1 \leq i \leq l$, we obtain, using Kahane's inequality twice and Khintchine's once,

$$\begin{aligned}
\left(\int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\|_p^2 dt \right)^{1/2} &\leq K_2 \int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\|_p dt \\
&\leq K_2 \left(\int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\|_p^p dt \right)^{1/p} = K_2 \left(\int_0^1 \sum_{j=1}^n \left| \sum_{i=1}^l r_i(t) \xi_{ij} \right|^p dt \right)^{1/p} \\
&= K_2 \left(\sum_{j=1}^n \int_0^1 \left| \sum_{i=1}^l r_i(t) \xi_{ij} \right|^p dt \right)^{1/p} \leq K_2 \left(\sum_{j=1}^n c_p^p \left(\sum_{i=1}^l |\xi_{ij}|^2 \right)^{p/2} \right)^{1/p}.
\end{aligned}$$

This holds for arbitrary $1 \leq p < \infty$. Now, if $1 \leq p \leq 2$, we use $\|y\|_2 \leq \|y\|_p$ for an arbitrary l-vector y, and obtain

$$\left(\int_0^1 \left\| \sum_{i=1}^l r_i(t) x_i \right\|_p^2 dt \right)^{1/2} \leq K_2 c_p \left(\sum_{j=1}^n \sum_{i=1}^l |\xi_{ij}|^p \right)^{1/p} = K_2 c_p \left(\sum_{i=1}^l \|x_i\|_p^p \right)^{1/p}.$$

If $2 \leq p < \infty$ we obtain, using the triangle inequality in $l^2_{p/2}$,

$$\left(\int_0^1 \left\|\sum_{i=1}^{l} r_i(t)x_i\right\|_p^2 dt\right) \leq K_2 c_p \left(\left(\sum_{j=1}^{n}\left(\sum_{i=1}^{l}|\xi_{ij}|^2\right)^{p/2}\right)^{2/p}\right)^{1/2}$$

$$\leq K_2 c_p \left(\sum_{i=1}^{l}\left(\sum_{j=1}^{n}|\xi_{ij}|^p\right)^{2/p}\right)^{1/2}$$

$$= K_2 c_p \left(\sum_{i=1}^{l}\|x_i\|_p^2\right)^{1/2}.$$

The last case that is interesting for our purpose is the upper bound for $\tau_2(l_\infty^n)$. For each $\tilde{p} \in [2, \infty[$ we obtain

$$\left(\int_0^1 \left\|\sum_{i=1}^{l} r_i(t)x_i\right\|_\infty^2 dt\right)^{1/2} \leq \left(\int_0^1 \left\|\sum_{i=1}^{l} r_i(t)x_i\right\|_{\tilde{p}}^2 dt\right)^{1/2}$$

$$\leq K_2 c_{\tilde{p}} \left(\sum_{i=1}^{l}\|x_i\|_{\tilde{p}}^2\right)^{1/2}$$

$$\leq K_2 c_{\tilde{p}} n^{1/\tilde{p}} \left(\sum_{i=1}^{l}\|x_i\|_\infty^2\right)^{1/2}.$$

Now consider the term $K_2 c_{\tilde{p}} n^{1/\tilde{p}}$. With $c_{\tilde{p}} \leq \sqrt{(\tilde{p}/2)+1}$ it is sufficient for our purpose to consider the function $f: [1, \infty[\to \mathbb{R}$ given by $\tilde{p} \mapsto \tilde{p}^{1/2} n^{1/\tilde{p}}$. Its derivative is $f':]1, \infty[\to \mathbb{R}$, $\tilde{p} \mapsto \tilde{p}^{-1/2} n^{1/\tilde{p}}(1/2 - (\ln n)/\tilde{p})$, whence $\tilde{p}^* = 2 \ln n$ is a global minimizer with $f(\tilde{p}^*) = \sqrt{2e}\sqrt{\ln n}$. □

The type of a Banach space X plays an important role in estimating the expectation E of the norm of the sum of independent X-valued random variables. To prove Proposition 3.17, we need the following result of Hoffmann–Jørgensen and Pisier [HJ74, HJP76].

PROPOSITION 3.19. *If $l \in \mathbb{N}$, $g \in [1, 2]$, and F is a Banach space of type g, then*

$$E\left\|\sum_{i=1}^{l}(X_i - EX_i)\right\|^g \leq 4^g \tau_g^g(F) \sum_{i=1}^{l} E\|X_i\|^g$$

for all independent F-valued random variables $X_1, \ldots, X_m$ with finite gth moment.

Proof of Proposition 3.17. Define $y_i = u(e_i)$ for $1 \leq i \leq h$, and $V = \{\pm y_1, \ldots, \pm y_h\}$, and choose any $y \in u(\mathbb{B}_1^h)$. Since $u(\mathbb{B}_1^h) = \operatorname{conv} V$, there exist $\lambda_1^+, \lambda_1^-, \ldots, \lambda_h^+, \lambda_h^- \geq 0$ such that $\sum_{i=1}^h (\lambda_i^+ + \lambda_i^-) = 1$ and $y = \sum_{i=1}^h (\lambda_i^+ - \lambda_i^-) y_i$. This implies that the F-valued random variable Z that attains y_i (resp. $-y_i$) with probability λ_i^+ (λ_i^-) has expectation $EZ = y$, and by its definition $\|Z\| \leq \|u\|$.

Now for $20\log((h/k)+1)\leqslant k\leqslant h$ let

$$\tilde{k}=\left\lceil\frac{k}{20\log((h/k)+1)}\right\rceil,$$

and consider $\tilde{k}$ independent F-valued random variables $Z_1,\dots,Z_{\tilde{k}}$ of the sort Z described above. Using Proposition 3.19, we obtain

$$E\left\|\sum_{i=1}^{\tilde{k}}Z_i-\tilde{k}y\right\|^g=E\left\|\sum_{i=1}^{\tilde{k}}(Z_i-EZ_i)\right\|^g$$

$$\leqslant 4^g\tau_g^g(F)\sum_{i=1}^{\tilde{k}}E\|Z_i\|^g\leqslant 4^g\tau_g^g(F)\tilde{k}\|u\|^g.$$

Thus there exist $\tilde{y}_1,\dots,\tilde{y}_{\tilde{k}}\in V$ such that $\|\sum_{i=1}^{\tilde{k}}\tilde{y}_i-\tilde{k}y\|^g\leqslant 4^g\tau_g^g(F)\tilde{k}\|u\|^g$, or, equivalently, $\|1/\tilde{k}\sum_{i=1}^{\tilde{k}}\tilde{y}_i-y\|\leqslant 4\tau_g(F)\tilde{k}^{-1+1/g}\|u\|$. Hence the point y lies in a ball with radius $s=4\tau_g(F)\tilde{k}^{-1+1/g}\|u\|$ and centre $1/\tilde{k}\sum_{i=1}^{\tilde{k}}\tilde{y}_i$. There are at most $t=\binom{2h+\tilde{k}-1}{\tilde{k}}$ such centres, because t is an upper bound for the cardinality of the set $\{1/\tilde{k}\sum_{i=1}^{\tilde{k}}\tilde{y}_i\colon \tilde{y}_i\in V\}$.

Hence t balls with radius s suffice to cover $u(\mathbb{B}_1^h)$, and it follows that $\mathrm{ent}_t(u)\leqslant s$.

Using the quantitative version of Stirling's formula already stated in Subsection 3.B, we now conclude that

$$t=\binom{2h+\tilde{k}-1}{\tilde{k}}\leqslant\frac{1}{4}\left(e^2\left(1+\frac{2h-1}{\tilde{k}}\right)\right)^{\tilde{k}}.$$

It follows by the choice of $\tilde{k}$ that

$$\log t\leqslant k-1,\qquad \text{hence } t\leqslant 2^{k-1},\ \text{whence } \varepsilon_k(u)\leqslant s.\qquad\square$$

§3.E. *Inapproximability results for deterministic approximation.* The underlying idea for the inapproximability results is that any oracle-polynomial-time algorithm for, say, approximating the inradius cannot decide, given the unit ball presented by an appropriate oracle as input, whether the input body is the unit ball itself or the convex hull of a polynomial number of vertices inscribed in the unit sphere (*cf.* [BF87] in the l_2 case). Hence an upper bound for the inradii of $\mathscr{P}$-polytopes of polynomial size contained in the l_p unit balls yields an upper bound for the accuracy in oracle-polynomial time approximation of the inradius.

To illustrate how the accuracy of an algorithm is determined by its capability of distinguishing between bodies, assume that $A\in\mathscr{A}$ is an algorithm approximating a measurement φ by a function φ_A, and that there exist, for each $n\in\mathbb{N}$, bodies K_1^n and K_2^n such that A outputs $\varphi_A(K_1^n)=\varphi_A(K_2^n)$. Now, let the accuracy of A be λ_1/λ_2, where the functions λ_1 and λ_2 are as in the definition of accuracy, and consider an arbitrary n.

By the definition of accuracy, the number $\varphi_A(K_i^n)$ delivered by the algorithm must be such that $\lambda_1(n)\varphi_A(K_i^n)\leqslant\varphi(K_i^n)\leqslant\lambda_2(n)\varphi_A(K_i^n)$ for $i=1,2$. Hence

$$\frac{\lambda_1(n)}{\lambda_2(n)}=\frac{\lambda_1(n)\varphi_A(K_1^n)}{\lambda_2(n)\varphi_A(K_2^n)}\leqslant\frac{\varphi(K_1^n)}{\varphi(K_2^n)}.$$

This implies that the accuracy of A in approximating φ is bounded above by the function $\bar{\lambda}$ defined by

$$\bar{\lambda}(n) = \frac{\min\{\varphi(K_1^n), \varphi(K_2^n)\}}{\max\{\varphi(K_1^n), \varphi(K_2^n)\}}.$$

Now assume that our algorithm for, say, approximating the inradius can, under the additional assumption of infinite precision, use a strong optimization oracle for a body K that is known to be contained in the unit ball. Assume further that in fact this oracle describes $\mathbb{B}_p$, not known *a priori* to the algorithm. Any oracle-polynomial-time algorithm can use only a polynomial number of oracle calls to gain information toward the determination of $\varphi(\mathbb{B}_p)$, and since the oracle describes the unit ball we obtain a polynomial number of points that are contained in the unit sphere. Then the algorithm can only assert for K that $K_1 = P \subset K \subset \mathbb{B}_p = K_2$, where P is a polytope inscribed in the unit ball with a polynomial number of vertices, because the answer to each oracle-call made by the algorithm is valid for any such K.

Following this argumentation, it remains to find estimates for the inradius of polytopes P contained in the unit ball $\mathbb{B}_p$ and having a polynomial number of vertices. Since $\text{vol}(P)/\text{vol}(\mathbb{B}_p) \leq \alpha^n$ implies $r_p(P) \leq \alpha$, Proposition 1.7 yields the required result.

PROPOSITION 3.20. *For each $p \in [1, \infty]$, there exists a constant $\rho = \rho(p)$ that has the following property: for each choice of n, $h \in \mathbb{N}$ with $20 \log h \leq n \leq h$ and for each 0-symmetric n-polytope $P \subset \mathbb{B}_p^n$ with at most $2h$ vertices, it is true that*

$$r_p(P) \leq \rho\left(\frac{\log((h/n)+1)}{n}\right)^{1-1/\min\{p,2\}}.$$

Now we can state the main result of this section.

THEOREM 3.2.1. *For $1 \leq p \leq \infty$, the upper bounds for the accuracy of oracle-polynomial-time approximation are as indicated in Table 4.*

Table 4. Upper accuracy bounds for deterministic oracle-polynomial-time approximation of radii- and norm-maximization

p	1	$1 < p \leq 2$	$2 \leq p < \infty$	∞
r_p, w_p	DOP	$O\left(\left(\frac{\log n}{n}\right)^{1/p'}\right)$	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$
R_p, d_p, N_p	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$	$O\left(\left(\frac{\log n}{n}\right)^{1/2}\right)$	$O\left(\left(\frac{\log n}{n}\right)^{1/p}\right)$	DOP

Proof. The inradius result follows from combining the above argumentation with Proposition 3.20. For width, circumradius and diameter note that, by the propositions in Subsection 1.A, "negative" results for the inradius yield analogous results for the other radii. For norm-maximization, just recall that, for 0-symmetric bodies, $N_p(K) = R_p(K)$. □

A comparison of Theorems 3.15 and 3.21 shows that, for oracle-polynomial-time algorithms that approximate certain radii with respect to the l_p norm, $((\log n)/n)^{1/p'}$ is the optimal order of approximation of inradius and width when $p \leq 2$, and $((\log n)/n)^{1/p}$ is the optimal order of approximation for circumradius, diameter and norm-maximization when $p \geq 2$. In the remaining cases, there is still a gap between the lower and upper bounds for the optimal order of approximation. The ratio of the upper to the lower bound is $(\log n)^{|1/2 - 1/p|}$.

§4. *Randomized versus deterministic approximation—a comparison.* In closing, we want to compare the upper and lower bounds for both randomized and deterministic approximation of diameter in Euclidean spaces (in the following denoted by d). For this purpose, we restate the results for the deterministic case in a slightly different form, and we assume that infinite precision is available in both cases. In particular, we assume that the bodies are presented by strong optimization oracles. The proofs are omitted, but can be found in [BGK+98] or derived from the results in Section 3.

It follows from the theorem of Jung and the results of Section 3 that analogous results (with slightly different constants) hold for the Euclidean circumradius, inradius and width of K, and for the maximum of the l_2 norm over K.

The following result extends that of Theorem 3.21 for $p = 2$ by describing a trade-off between the number of vectors that determine a covering of the sphere and the relative error.

THEOREM 4.1. *For each $0 < s < 1$, there is a deterministic algorithm A which, for every body $K \subset \mathbb{E}^n$, uses $\tau(n, s)$ oracle calls to compute a value $d_A(K)$ such that*

$$sd(K) \leq d_A(K) \leq d(K).$$

Using the deterministic algorithm for the construction of a covering of the sphere, we conclude

THEOREM 4.2. *For each $0 < s < 1/2$, there is a deterministic algorithm A that finds, for every body $K \subset \mathbb{R}^n$, a value $d_A(K)$ with $sd(K) \leq d_A(K) \leq d(K)$. This A does by using $O((1/s^2)e^{12s^2n})$ oracle calls whose input is determined in $O((n^2/s^2)e^{12s^2n})$ operations.*

As a corollary, we obtain

COROLLARY 4.3. *For any constant $h > 1$, there is a deterministic polynomial-time algorithm A that finds, for every body $K \subset \mathbb{R}^n$, a value $d_A(K)$ with*

$$\sqrt{\frac{(h-1)\log n}{20n}}\, d(K) \leq d_A(K) \leq d(K).$$

This A does by using $O(n^h)$ oracle calls whose input is determined in $O(n^{h+2})$ operations.

Proof. Regarding Theorem 4.2, it suffices to observe that, for $s = \sqrt{(h-1)\log n/(20n)}$,

$$\frac{1}{s^2} e^{12s^2 n} \leqslant \frac{20n}{(h-1)\log n} e^{0.6(h-1)\log n} \leqslant \frac{20n}{(h-1)\log n} n^{0.9(h-1)} = O(n^h). \qquad \square$$

On the other side, we have the following from Section 3.E, as well as from [BGK+98].

THEOREM 4.4. *If $0 < s < 1$, and A is a deterministic algorithm that computes, for every body $K \subset \mathbb{R}^n$, an estimate $d_A(K)$ of $d(K)$ such that*

$$sd(K) < d_A(K) \leqslant d(K),$$

then A must use at least $\tau(n,s)/2$ oracle calls in the worst case.

Bounding $\tau(n,s)/2$ from below for $s = \sqrt{(2h\log n)/n}$, we obtain

COROLLARY 4.5. *If $h \geqslant 1$ is a constant and A is a deterministic algorithm that computes, for every body $K \subset \mathbb{R}^n$, an estimate $d_A(K)$ of $d(K)$ such that*

$$\sqrt{2h\log n/n}\, d(K) < d_A(K) \leqslant d(K),$$

then using $O(n^h)$ oracle calls does not suffice in the worst case.

In order to compare these results with randomized approximation, we express the accuracy of diameter algorithms in terms of the required number of calls to the optimization oracle.

- Corollary 4.3 yields a deterministic algorithnm that uses $O(n^h)$ oracle-calls and approximates the diameter with accuracy at least $\sqrt{(h-1)/20}\sqrt{(\log n)/n}$. The input for the oracle-calls is determined by $O(n^{h+2})$ operations.
- Corollary 4.5 states that approximating the diameter with accuracy at least $\sqrt{2h}\sqrt{(\log n)/n}$ cannot be done with $O(n^h)$ oracle calls.
- Theorem 2.3 yields a randomized algorithm that uses $O(n^h)$ oracle-calls and whose accuracy in approximating the diameter with probability at least $6/7$ is at least $\sqrt{h}\sqrt{(\log n)/n}$.
- Corollary 2.6 states that if an algorithm uses only $O(n^h)$ oracle calls, then the probability is less than $3/4$ that it approximates the diameter with accuracy at least $\sqrt{2h}\sqrt{(\log n)/n}$.

Note that, although randomization does not yield an improvement in the asymptotic accuracy, it might be possible to decrease the degree of the involved polynomial. In particular the deterministic algorithm presented here requires $O(n^h)$ oracle calls, where $h > 1$. On the other side, we conclude the following, from Theorem 2.3 and Jung's theorem, for convex bodies presented by weak optimization oracles:

COROLLARY 4.6. *Even if restricted to a linear number of oracle calls, the accuracy for randomized oracle-polynomial-time approximation of the Euclidean*

diameter and circumradius is

$$\Theta\left(\sqrt{\frac{\log n}{n}}\right).$$

However, more generally, without considering the degree of the polynomial involved, the theorems mentioned above can be summarized as follows.

THEOREM 4.7. *The accuracy for both randomized and deterministic oracle-polynomial-time approximation of the Euclidean diameter, width, circumradius, inradius and the norm-maximum is*

$$\Theta\left(\sqrt{\frac{\log n}{n}}\right).$$

Finally, we want to give a short informal explanation of why randomization helps for volume computation but does not help (except in reducing the degree of the polynomial) in approximating the diameter. For this, recall one of the basic ideas that are used in a couple of randomized volume algorithms, *cf.* [DFK89]. For a body that is contained in the unit ball, the volume is asymptotically equal to the ratio of the number of sample points contained in it to the total number of sample points, where the samples are chosen uniformly at random from the unit ball. Each oracle call determines whether a given point is contained in the convex body, and hence, no matter what the oracle's answer, the answer provides additional information about the volume. However, for a typical 0-symmetric body K, a single point at maximum distance from the origin is needed to determine the diameter, and with high probability many useless oracle calls are necessary to detect this point or even to distinguish K from the largest 0-symmetric ball contained in K.

References

[BF87] I. Bárány and Z. Füredi. Computing the volume is difficult. *Discrete Comput. Geom.*, 2 (1987), 319–326.

[BF88] I. Bárány and Z. Füredi. Approximation of the sphere by polytopes having few vertices. *Proc. Amer. Math. Soc.*, 102 (1988), 651–659.

[BG97] A. Brieden and P. Gritzmann. On Helly's theorem: algorithms and extensions. *Discrete Comput. Geom.*, 17 (1997), 393–410.

[BGK+98] A. Brieden, P. Gritzmann, R. Kannan, V. Klee, L. Lovász and M. Simonovits. Approximation of radii and norm-maxima: Randomization doesn't help. *Proc. 39th Sympos. FOCS, IEEE* (1998), 244–251.

[BGK99] A. Brieden, P. Gritzmann and V. Klee. Inapproximability of some geometric and quadratic optimization problems. *Approximation and Complexity in Numerical Optimization* (ed. P. M. Pardalos). Kluwer (Boston, 2000), 96–115.

[BGKL90] H. L. Bodlaender, P. Gritzmann, V. Klee and J. van Leeuwen. Computational complexity of norm-maximization. *Combinatorica*, 10 (1990), 203–225.

[BP90] K. Ball and A. Pajor. Convex bodies with few faces. *Proc. Amer. Math. Soc.*, 110 (1990), 225–231.

[Bri98] A. Brieden. *Deterministic Approximation Algorithms in Computational Convexity*, PhD thesis (Tech. Univ. Munich, 1998).

[Car85] B. Carl. Inequalities of Bernstein–Jackson-type and the degree of compactness of operators in Banach spaces. *Ann. l'Inst. Fourier*, 35 (1985), 79–118.

[CP88] B. Carl and A. Pajor. Gelfand numbers of operators with values in a Hilbert space. *Invent. Math.*, 94 (1988), 479–504.

[DF88] M. Dyer and A. Frieze. On the complexity of computing the volume of a polytope. *SIAM J. Comput.*, 17 (1988), 967–974.

[DFK89] M. Dyer, A. Frieze and R. Kannan. A random polynomial time algorithm for approximating the volume of convex bodies. *Proc. 21st ACM Sympos. Theory Comput.* (1989), 375–381.

[DGK63] L. Danzer, B. Grünbaum and V. Klee. Helly's theorem and its relatives. *Proc. Sympos. Pure Math.*, 7 (1963), 101–180.

[Dud94] S. I. Dudov. An inner bound of a convex set by a norm body. *Comput. Math. Math. Physics*, 36 (1994), 683–688.

[Ele86] G. Elekes. A geometric inequality and the complexity of computing volume. *Discrete Comput. Geom.*, 1 (1986), 289–292.

[FO85] R. M. Freund and J. B. Orlin. On the complexity of four polyhedral set containment problems. *Math. Programming*, 33 (1985), 139–145.

[Gil77] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM J. Comput.*, 6 (1977), 675–695.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and Intractability. A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979).

[GK92] P. Gritzmann and V. Klee. Inner and outer j-radii of convex bodies in finite-dimensional normed spaces. *Discrete Comput. Geom.*, 7 (1992), 255–280.

[GK93] P. Gritzmann and V. Klee. Computational complexity of inner and outer j-radii of polytopes in finite-dimensional normed spaces. *Math. Programming*, 59 (1993), 163–213.

[GK94] P. Gritzmann and V. Klee. On the complexity of some basic problems in computational convexity: I. Containment problems. *Discrete Math.*, 136 (1994), 129–174.

[GLS93] M. Grötschel, L. Lovász and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization* (Springer, Berlin, 1988, 1993).

[GMR94] Y. Gordon, M. Meyer and S. Reisner. Volume approximation of convex bodies—a constructive method. *Studia Math.*, 111 (1994) 81–95.

[GMR95] Y. Gordon, M. Meyer and S. Reisner. Constructing a polytope to approximate a convex body. *Geom. Dedicata*, 57 (1995), 217–222.

[Gru93] P. M. Gruber. Aspects of approximation of convex bodies. *Handbook of Convex Geometry*. P. M. Gruber and J. M. Wills, eds. (Elsevier, Amsterdam, 1993), 319–345.

[HJ74] J. Hoffmann-Jørgensen. Sums of independent Banach space valued random variables. *Studia Math.*, 52 (1974), 159–186.

[HJP76] J. Hoffman-Jørgensen and G. Pisier. The law of large numbers and the central limit theorem in Banach spaces. *Ann. Probab.*, 4 (1976), 587–599.

[Jan98] T. Jansen. Introduction to the theory of complexity and approximation algorithms. In Mayr *et al.* [MPS98], 5–28.

[Jun01] H. W. E. Jung. Über den kleinsten Kreis, der eine ebene Figur einschließt. *J. Reine Angew. Math.*, 130 (1901), 310–313.

[JVV86] M. R. Jerrum, L. G. Valiant and V. V. Vazirani. Random generation of combinatorial structures from a uniform distribution. *Theoret. Comput. Sci.*, 43 (1986), 169–188.

[Kah68] J.-P. Kahane. *Some Random Series of Functions* (Heath, Cambridge, 1968; 2nd edition, Cambridge University Press, 1985).

[Kha79] L. G. Khachiyan. Polynomial algorithms in linear programming. *Dokl. Akad. Nauk SSSR*, 244 (1979), 1093–1096. (Russian); English translation: *Doklady Mathematics*, 20 (1979), 191–194.

[Kha88] L. G. Khachiyan. On the complexity of computing the volume of a polytope. *Izv. Akad. Nauk SSSR, Engineering Cybernetics*, 3 (1988), 216–217.

[Khi23] A. Khintchine. Über dyadische Brüche. *Math. Z.*, 18 (1923), 109–116.

[KLS98] R. Kannan, L. Lovász and M. Simonovits. Random walks and an $O^*(n^5)$ volume algorithm for convex bodies. *Random Structures Algorithms*, 11 (1998), 1–50.

[Koc94] M. Kochol. Constructive approximation of a ball by polytopes. *Math. Slovaca*, 44 (1994), 99–105.

[LS92] L. Lovász and M. Simonovits. On the randomized complexity of volume and diameter. *Proc. 33rd Sympos. FOCS, IEEE* (1992), 482–491.

[LT79] J. Lindenstrauss and L. Tzafriri. *Classical Banach Spaces II* (Springer, Berlin, 1979).

[MPS98] E. W. Mayr, H. J. Prömel and A. Steger (eds.). *Lectures on Proof Verification and Approxiomation Algorithms*. Lecture Notes in Computer Science, no. 1367 (Springer, 1998).

[MS86] V. D. Milman and G. Schechtman. *Asymptotic Theory of Finite Dimensional Normed Spaces*. Lecture Notes in Mathematics, vol. 1200 (Springer, 1986).

[Pie80] A. Pietsch. *Operator Ideals* (North-Holland, Amsterdam, 1980).

[Pis88] G. Pisier. *The Volume of Convex Bodies and Banach Space Geometry* (Cambridge University Press, 1988).

[PY91] C. H. Papadimitriou and M. Yannakakis. Optimization, approximation, and complexity classes. *J. Comput. System Sci.*, 43 (1991), 425–440.

[Sho77] N. Z. Shor. Cut-off method with space extension in convex programming problems. *Kibernetika*, 1977 (1977), no. 1, 94–95; English translation: *Cybernetics*, 13 (1977), 94–96.

[Ste22] P. Steinhagen. Über die größte Kugel in einer konvexen Punktmenge. *Abh. Math. Sem. Univ. Hamburg* (1922), 15–22.

[SY92] J. R. Seberry and M. Yamada. Hadamard matrices, sequences, and block designs. *Contemporary Design Theory—A Collection of Surveys* (North Holland, New York, 1992), 431–560.

[Syl67] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile work, and the theory of numbers. *Philos. Magazine*, 34 (1867), 461–475.

[TJ88] N. Tomczak-Jaegermann. *Banach–Mazur Distances and Finite-Dimensional Operator Ideals* (Longman Scientific & Technical, 1988).

[Vaa79] J. D. Vaaler. A geometric inequality with applications to linear forms. *Pacific J. Math.*, 83 (1979), 543–553.

[YN76] B. D. Yudin and A. S. Nemirovskii. Informational complexity and efficient methods for the solution of convex extremal problems. *Ekonomika i Mat. Metody*, 12 (1976), 357–369; English translation: *Matekon*, 13, 25–45.

Dr. Andreas Brieden,
Zentrum Mathematik,
Technische Universität München,
D-80290 Munich,
Germany
E-mail: brieden@mathematik.tu-muenchen.de

Professor Peter Gritzmann,
Zentrum Mathematik,
Technische Universität München,
D-80290 Munich,
Germany
E-mail: gritzman@mathematik.tu-muenchen.de

Professor Ravindran Kannan,
Department of Computer Science,
Yale University,
New Haven, CT 06520,
U.S.A.
E-mail: kannan@cs.yale.edu

Professor Victor Klee,
Department of Mathematics,
University of Washington,
Box 354350,
Seattle, WA 98195-4350,
U.S.A.
E-mail: klee@math.washington.edu

Dr. László Lovász,
Microsoft Research,
One Microsoft Way,
Redmond, WA 98053,
U.S.A.
E-mail: lovasz@microsoft.com

Dr. Miklós Simonovits,
Alfréd Rényi Institute of Mathematics,
Reáltanoda u. 13-15,
H-1053, Budapest,
Hungary
E-mail: miki@math-inst.hu

52B55: *CONVEX AND DISCRETE GEOMETRY; Polytopes and polyhedra; Computational aspects related to convexity.*

Received on the 17th of October, 2000.