ELSEVIER

Discrete Mathematics 221 (2000) 79–92

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Oracle-polynomial-time approximation of largest simplices in convex bodies ☆

Andreas Brieden[a], Peter Gritzmann[a,*,1], Victor Klee[b,1,2]

[a] Zentrum Mathematik, Technische Universität München, D-80290 Munich, Germany

[b] Department of Mathematics, University of Washington 354350, Seattle, Washington 98195-4350, USA

Received 1 April 1998; accepted 12 October 1999

Abstract

With focus on the case of variable dimension n, this paper is concerned with deterministic polynomial-time approximation of the maximum j-measure of j-simplices contained in a given n-dimensional convex body K. Under the assumption that K is accessible only by means of a weak separation oracle, upper and lower bounds on the accuracy of oracle-polynomial-time approximations are obtained. © 2000 Elsevier Science B.V. All rights reserved.

MSC: 90C30; 52B55; 68Q20; 15A15; 05B20

Keywords: Simplex; Determinant; Algorithmic theory of convex bodies; Approximation; Oracle; Polynomial time

0. Introduction

Let $\mathbb{E}^n$ denote the n-dimensional Euclidean space, $\| \ \|$ the Euclidean norm, and $\mathbb{B}^n$ the Euclidean unit ball. A *convex body* (or simply *body*) in $\mathbb{E}^n$ is an n-dimensional compact convex subset of $\mathbb{E}^n$. The set of all bodies in $\mathbb{E}^n$ is denoted by $\mathscr{K}^n$, and our focus here is on the collection $\mathscr{K} = \bigcup_{n=1}^{\infty} \mathscr{K}^n$.

For $j \in \mathbb{N}$ with $j \leqslant n$, a *j-simplex* in $\mathbb{E}^n$ is a set that is the convex hull of some $j+1$ affinely independent points of $\mathbb{E}^n$. For each $K \in \mathscr{K}$ and each $j \in \mathbb{N}$, $\sigma(K,j)$ will denote the maximum of the j-measures of the j-simplices that are contained in K. (When $j > \dim(K)$, set $\sigma(K,j) = 0$.) We are concerned with the following algorithmic

☆ Supported in part by a DAAD/NSF Travel Grant.

* Corresponding author.

E-mail addresses: brieden@mathematik.tu-muenchen.de (A. Brieden), gritzman@mathematik.tu-muenchen.de (P. Gritzmann), klee@math.washington.edu (V. Klee).

1 Supported in part by a Max Planck Research Award and a NATO Travel Grant.

2 Supported by an NSF Grant.

PII: S0012-365X(99)00387-8

task:

Given $j, n \in \mathbb{N}$ and $K \in \mathscr{K}^n$, compute $\sigma(K, j)$.

When $j = 1$ the problem is that of computing the diameter $\sigma(K, 1)$ of K, a basic problem in computational convexity; see [5,6,7,12,13]. When $j = n$ the problem subsumes, as the very special case in which $j = n \equiv 3 \pmod 4$ and K is an n-cube, the famous unsolved problem on the existence of Hadamard matrices. More generally, for each n the largest n-simplices in an n-cube correspond to the $(n+1) \times (n+1)$ real matrices that are of maximum determinant among those in which each entry is of absolute value at most 1. See [16] for details.

The intermediate values of j are related to the *weighing designs* that appear in numerous applications in chemistry, medicine and other sciences; see, e.g., [2]. In fact, the largest j-simplices with vertices in $\{0, 1\}^n$ correspond to the so-called D-optimal designs for using n weighings to weigh j objects on a spring balance; see [13] for details. Intermediate values of j are also of interest in connection with the problem of noise reduction for data sets taken from physical measurements, and these occur in settings ranging from ultramicroscopy [18] to airborne image spectrometry [4,11]. In the latter setting, each data point in n-space represents (aside from noise) a weighted average of $j + 1$ parameters associated with the imaged terrain. The underlying ideal shape of the 'data cloud' is therefore that of a j-simplex in n-space, and the problem becomes that of finding a j-simplex that in some appropriate sense best represents the data set. A reasonable first candidate for this is the largest j-simplex contained in the convex hull of the data points.

The present paper studies the problem of computing or approximating $\sigma(K, j)$ within the framework of the algorithmic theory of convex bodies developed by Grötschel et al. [15]. Bodies are assumed to be given by an *oracle* that solves a certain sort of problem and can be used as a subroutine by any algorithm. In effect, the usual binary Turing machine model is augmented by the oracle with the assumption that each call to the oracle takes only the time required to present the query to the oracle and to record the oracle's answer. This leads to the notion of an *oracle-polynomial-time* algorithm. The present paper uses a *weak separation oracle* and studies the accuracy of oracle-polynomial-time algorithms for approximating the volumes of largest simplices in bodies. (The model of computation is described in more detail in Section 1.) Naturally, bodies that are *polytopes* (with rational vertices) are dealt with much more easily than general bodies since they can be specified in a finite manner by a suitable system of linear inequalities ($\mathscr{H}$-polytope) or a finite set of points including their vertices ($\mathscr{V}$-polytope). Hence, when dealing with polytopes, the standard Turing machine model suffices.

While the problem of computing the volume of general ($\mathscr{V}$- or $\mathscr{H}$-) polytopes is #$\mathbb{P}$-hard [10], computing the volume of a single j-simplex can be accomplished by evaluating a determinant (see Proposition 1.3). Hence it is the task of *maximization* rather than that of volume computation that poses the problem here. It is of course true that if P is a polytope with m vertices, then a largest j-simplex in E can be found with the aid of $\binom{m}{j+1}$ determinant evaluations. However, that is not reassuring, for the decision version of each of the following problems is $\mathbb{NP}$-hard: finding a largest 1-simplex in an n-parallelotope [12], finding a largest $\lfloor n/2 \rfloor$-simplex in an n-simplex [14], finding a largest n-simplex in a fairly simple sort of n-dimensional $\mathscr{V}$-polytope [14].

The present paper asks how well $\sigma(K,j)$ can be approximated when we are restricted to polynomial-time algorithms. The problem is studied here for general bodies $K \in \mathscr{K}$ because our positive results apply to such bodies and not only to polytopes. (In a sense, the algorithmic theory of convex bodies places $\mathscr{V}$- and $\mathscr{H}$-polytopes on an equal footing.) Further, the oracle Turing machine model allows us to derive negative results showing that no oracle-polynomial-time algorithm can approximate $\sigma(K,j)$ too well for all $K \in \mathscr{K}$ and $j \in \mathbb{N}$. To make these statements precise, we must first introduce the notion of the (*asymptotic relative*) *accuracy* of approximation.

We consider the case in which the dimension n of K is part of the input, while j is related to n in some specified manner. For each non-decreasing function $\gamma : \mathbb{N} \to \mathbb{N}$ such that $\gamma(n) \leqslant n$ for all n, let the function $\sigma_\gamma : \mathscr{K} \times \mathbb{N} \to \mathbb{R}$ be defined by $\sigma_\gamma(K) = \sigma(K,\gamma(n))$. Functions γ of special interest include those for which $\gamma(n)$ or $n-\gamma(n)$ or $\lfloor n/\gamma(n) \rfloor$ is constant. The function γ is assumed to be given beforehand; it is not part of the input whose size enters into our definition of computational complexity.

Now let $\mathscr{A}_\gamma$ denote the class of oracle-polynomial-time algorithms A which, accepting as input a member K of $\mathscr{K}$, outputs an approximation $\sigma_{A,\gamma}(K)$ of $\sigma_\gamma(K)$. The *accuracy* $\alpha_{A,\gamma}$ of an algorithm $A \in \mathscr{A}_\gamma$ is a function defined on $\mathbb{N}$ and with values in $[0,1]$ such that there exist two functions $\alpha_1 : \mathbb{N} :\to [0,\infty[$ and $\alpha_2 : \mathbb{N} :\to]0,\infty[$ with $\alpha_1/\alpha_2 = \alpha_{A,\gamma}$ such that

$$\alpha_1(n)\sigma_{A,\gamma}(K) \leqslant \sigma_\gamma(K) \leqslant \alpha_2(n)\sigma_{A,\gamma}(K)$$

for each $(K,n) \in \mathscr{K} \times \mathbb{N}$. A function $\alpha_\gamma : \mathbb{N} \to [0,1]$ is called *accuracy of oracle-polynomial-time approximation of* σ_γ if

$$A \in \mathscr{A}_\gamma \Rightarrow \alpha_{A,\gamma} = O(\alpha_\gamma), \quad \text{and} \quad \text{there exists } A \in \mathscr{A}_\gamma \text{ such that } \alpha_{A,\gamma} = \Omega(\alpha_\gamma).$$

Note that this above definition extends naturally to subclasses of $\mathscr{A}_\gamma$.

The main positive result of this paper is that

$$\alpha_\gamma \geqslant \left(\frac{\log n}{n}\right)^{1/2} \quad \text{if } \gamma(n) \equiv 1, \text{ and } \alpha_\gamma \geqslant \left(\frac{c}{n}\right)^j \quad \text{if } j = \gamma(n) \geqslant 2,$$

where c is a universal constant, i.e., independent of j and n.

On the negative side we prove that there exists a universal constant ρ with $0 < \rho < 1$ such that

$$\alpha_{\beta,\gamma} \leqslant \left(j\frac{(n-j)!}{n!}\right)^{1/2} \left(\frac{\beta}{\rho^2}\log n\right)^{j/2} \qquad \text{if } j = \gamma(n) \leqslant t,$$

$$\alpha_{\beta,\gamma} \leqslant \left(\frac{j}{j-t}\frac{(n-t)!}{n!}\right)^{1/2} \left(\frac{\beta}{\rho^2}\log n\right)^{t/2} \qquad \text{if } j = \gamma(n) > t,$$

where $t = n - \log(n^\beta + 1) + 1$, and the function $\alpha_{\beta,\gamma} : \mathbb{N} \to \mathbb{R}$ is the accuracy when the algorithms are restricted to the members of $\mathscr{A}_\gamma$ that make at most n^β calls to the oracle that describes the body K of $\mathscr{K}^n$.

When $\gamma(n) \equiv 1$, a comparison of the stated lower and upper bounds shows that the accuracy is $\Theta\left(((\log n)/n)^{1/2}\right)$ in this case. In other words, the estimate of accuracy is sharp up to a multiplicative constant. This result can be found in [7,6], remains true even for randomized algorithms, and is stated here for the sake of completeness. To illustrate the gap between lower and upper bounds for other choices of γ, note that for $j = \gamma(n) \equiv const > 1$ our lower bound is $(1/n)^j$ and upper bound is $(\log n/n)^{j/2}$. At the other extreme, when $\gamma(n) \equiv n$, the lower bound is $((c/(n))^n$ and the upper bound is $\left(\psi_\beta \log n/n\right)^{(n-\beta\log n)/2}$, where ψ_β is a constant that depends only on β.

Let us remark that, for $\mathscr{V}$-polytopes (in the usual Turing machine model, see Subsection 1.1) largest n-simplices can be approximated with accuracy greater than $(d/n)^{n/2}$, where d is a universal constant, see [17].

Section 1 contains various preliminaries, including an outline of the underlying model of computation, some volume formulas, etc. Our lower bounds are derived in Section 2 and the upper bounds are established in Section 3.

1. Preliminaries

1.1. The model of computation

The underlying model of computation is the binary Turing machine model, augmented by certain oracles. Polytopes can be presented in a finite and (if they are rational) algorithmically suitable manner. A string $(n, s; v_1, \dots, v_s)$ with $n, s \in \mathbb{N}$ and $v_1, \dots, v_s \in \mathbb{Q}^n$ is called a *$\mathscr{V}$-polytope* in $\mathbb{E}^n$; it represents the geometric object $P = \operatorname{conv}\{v_1, \dots, v_s\}$. Similarly, an *$\mathscr{H}$-polytope* is a string $(n, s; Q, b)$ such that $n, s \in \mathbb{N}$, Q is a rational $s \times n$ matrix, and b is a rational s-vector for which the set $P = \{x \in \mathbb{E}^n \colon Qx \leqslant b\}$ is bounded and hence is a polytope; again, the string is identified with the geometric object P. The *binary size* (or simply *size*) of a $\mathscr{V}$- or an $\mathscr{H}$-polytope P is the number of binary digits needed to encode the data of the presentation; see [12,13].

A way to deal algorithmically with general bodies K has been introduced and extensively studied in [15]. 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. One sort of *a priori* information is that the body K is *circumscribed*, i.e., a rational number $\bar{R}$ is given explicitly such that $K \subset \bar{R}\mathbb{B}^n$. (Thus $\bar{R}$ is an upper bound for K's Euclidean circumradius.) The *size* of K is then defined by $\operatorname{size}(K) = n + \operatorname{size}(\bar{R})$. If in addition a positive rational number $\underline{r}$ is given such that K contains a ball (whose position may not be known) of radius $\underline{r}$, the body is *well-bounded*. (Thus $\underline{r}$ is a lower bound for K's Euclidean inradius.) Then, of course, $\operatorname{size}(K) = n + \operatorname{size}(\underline{r}) + \operatorname{size}(\bar{R})$.

The most appropriate oracle for our purpose 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 $K \subset \mathbb{E}^n$ are given, respectively, by

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

A *weak separation oracle* for a body K in $\mathbb{E}^n$ solves the following problem.

Weak separation problem. *Given $y \in \mathbb{Q}^n$, and a positive rational ε, assert that $y \in K(\varepsilon)$ or determine a vector $c \in \mathbb{Q}^n$ with $||c||_\infty = 1$ such that $c^T x \leqslant c^T y + \varepsilon$ 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, [15] produces deterministic polynomial-time algorithms for well-boundedness and for solving the weak separation problem. In general, however, a separation oracle functions as a 'black box' in the sense that we know the input and the output of the oracle but we know nothing about how the output is produced. An algorithm is called an *oracle-polynomial-time* algorithm if it is polynomial in the oracle-Turing-machine model. This means that the algorithm is polynomial in the usual sense, except that each call to the oracle is assumed to take only the time required to write the input of the call onto a tape of the Turing machine and to read the oracle's answer from a tape of the machine. In other words, we do not know or care how hard the oracle must work to produce its answer.

Throughout this paper, we assume that bodies K are well-bounded and are given by a weak separation oracle. In order to exclude the trivial case $n = 1$, we assume also that K is at least two-dimensional.

1.2. Some volume and determinant formulas

In later sections, use is made of some standard results that are stated here explicitly as a service to the reader. For a list of references to these and other related results see [14,16]. For any compact convex subset C of $\mathbb{E}^n$, $\mathrm{vol}(C)$ will always denote the volume taken in the affine hull $\mathrm{aff}(C)$ of C; in other words, when C is j-dimensional, $\mathrm{vol}(C)$ denotes the j-measure of C.

Proposition 1.1. *If v is a vertex of a j-simplex S, F is a $(j-1)$-face of S that misses v, and δ is the distance from v to $\mathrm{aff}(F)$, then $\mathrm{vol}(S) = (\delta/j)\mathrm{vol}(F)$.*

Proposition 1.2. *The largest j-simplices in $\mathbb{B}^n$ are precisely the regular j-simplices whose vertices all belong to the boundary of a j-dimensional central section of $\mathbb{B}^n$. The volume of each such j-simplex is equal to $(j+1)^{(j+1)/2}/(j!j^{j/2})$.*

Proposition 1.3. *If S_j is a j-simplex in $\mathbb{E}^n$ with $0 \in \operatorname{aff}(S_j)$, and A is the $(j+1)\times n$ matrix whose rows list the vertices of S_j, then*

$$(j!)^2\operatorname{vol}^2(S_j) = \det(J + AA^{\mathrm{T}}),$$

where J is the $(j+1)\times(j+1)$ matrix whose entries are all 1. If 0 is a vertex of S_j, then

$$(j!)^2\operatorname{vol}^2(S_j) = \det(A_0A_0^{\mathrm{T}}),$$

where A_0 is the matrix obtained from A by discarding the 0-row. In particular,

$$n!\,\operatorname{vol}(S_n) = |\det A_0|.$$

In addition to the volume formulas we need two facts about determinants. The first is obvious, while the second is intuitively clear and not hard to prove; see, e.g., [19, 5.2.2(9)].

Proposition 1.4. *If M is a $j\times j$ matrix and N is an $n\times j$ matrix, then*

$$\det(MN^{\mathrm{T}}NM^{\mathrm{T}}) = \det(MM^{\mathrm{T}})\det(N^{\mathrm{T}}N).$$

Proposition 1.5. *Let Z be a positive definite $n\times n$ matrix with eigenvalues $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ and corresponding orthonormal eigenvectors $v_1,\ldots,v_n$. Let W be an $n\times j$ matrix with $W^{\mathrm{T}}W = I_j$, where I_j is the $j\times j$ identity matrix. Then*

$$\det(W^{\mathrm{T}}ZW) \leqslant \prod_{i=1}^{j} \lambda_i$$

with equality for $W = (v_1,\ldots,v_j)$.

2. The lower bounds

The basic idea of our approximation algorithm is very simple: Given $K \in \mathscr{K}^n$ and $2 \leqslant j \leqslant n$, a lower bound for $\sigma(K,j)$ is provided by the volume of any j-simplex contained in K, and an upper bound for $\sigma(K,j)$ is provided by $\sigma(E,j)$ for any body E that contains K.

For computational convenience, E should belong to a class of bodies in which largest j-simplices can be computed in polynomial time. Surprisingly, we do not know of any class of 'nice' polytopes for which this is true, and the $\mathbb{NP}$-hardness results quoted in the introduction cast doubt on the existence of such a class. Even finding a largest j-simplex in a unit n-cube $[0,1]^n$ can be a daunting task. For $1 \leqslant j \leqslant 5$, it has been solved for all n [16,21,22], but beyond that the picture is spotty. In particular, for the case in which $k \in \{0,3,4\}$ and $n \equiv k \pmod 4$, there are infinitely many n for which $\sigma([0,1]^n, n)$ is known precisely, but also infinitely many n for which it is not known [16,20]. And when $n \equiv 2 \pmod 4$, the precise value of $\sigma([0,1]^n, n)$ has been determined only for $n \in \{2,6,10\}$ [9,16].

Fortunately, largest j-simplices in ellipsoids can be computed (with high enough accuracy) in polynomial time; in fact, we present a modification of the *shallow-cut ellipsoid algorithm* of [15,25,26] that determines, roughly speaking, a pair of j-simplices T and U such that T is a largest j-simplex in an ellipsoid that contains K and U is a homothetic copy of T (scaled by a factor $\mathrm{O}(1/n)$) that is contained in K.

2.1. Largest j-simplices in ellipsoids

An n-dimensional ellipsoid E can always be presented by a positive definite $n \times n$ matrix Z and an n-vector q such that $E_{Z,q} = q + Q\mathbb{B}^n$, where $Q^{\mathrm{T}}Q = Z$. Let $\lambda_1, \ldots, \lambda_n$ denote Z's eigenvalues in descending order $\lambda_1 \geqslant \cdots \geqslant \lambda_n$, and let $v_1, \ldots, v_n$ be associated orthonormal eigenvectors. Of course, the axes of $E_{Z,q}$ are determined by the eigenvectors and the length of each axis is twice the square root of the corresponding eigenvalue. We will now show that each largest j-simplex contained in E is the image of a largest j-simplex contained in $\mathrm{lin}\{v_1, \ldots, v_j\} \cap \mathbb{B}^n$ under the affine transformation $x \mapsto q + Qx$. Note that this is clear for $j = 1$ and n.

Lemma 2.1. *Let $E_{Z,q}$ be an n-dimensional ellipsoid. Then each largest j-simplex contained in $E_{Z,q}$ is the image of a largest j-simplex contained in $\mathrm{lin}\{v_1, \ldots, v_j\} \cap \mathbb{B}^n$ under the affine transformation $x \mapsto q + Qx$, and its volume is equal to*

$$\frac{(j+1)^{(j+1)/2}}{j!\,j^{j/2}} \prod_{i=1}^{j} \sqrt{\lambda_i}.$$

Proof. Without loss of generality, we may assume that $q = 0$. Let $S = \mathrm{conv}\{x_0, \ldots, x_j\}$ be a j-simplex contained in $\mathbb{B}^n$ and let $QS = \mathrm{conv}\{y_0, \ldots, y_j\}$ be its image contained in $Q\mathbb{B}^n$. Let $w_1, \ldots, w_j \in \mathbb{E}^n$ with $S - x_0 \subset \mathrm{lin}\{w_1, \ldots, w_j\}$ and $W^{\mathrm{T}}W = I_j$, where $W = (w_1, \ldots, w_j)$. We define

$$A_0 = \begin{pmatrix} (x_1 - x_0)^{\mathrm{T}} \\ \vdots \\ (x_j - x_0)^{\mathrm{T}} \end{pmatrix}, \qquad B_0 = \begin{pmatrix} (y_1 - y_0)^{\mathrm{T}} \\ \vdots \\ (y_j - y_0)^{\mathrm{T}} \end{pmatrix}$$

and choose M such that $A_0 = MW^{\mathrm{T}}$. Using Propositions 1.3–1.5 (with $QW = N$) we obtain

$$\begin{aligned}
\mathrm{vol}^2(QS) &= \mathrm{vol}^2(QS - y_0) = \mathrm{vol}^2(\mathrm{conv}\{0, y_1 - y_0, \ldots, y_j - y_0\}) \\
&= \frac{1}{(j!)^2}\det(B_0B_0^{\mathrm{T}}) = \frac{1}{(j!)^2}\det((A_0Q^{\mathrm{T}})(QA_0^{\mathrm{T}})) \\
&= \frac{1}{(j!)^2}\det((MW^{\mathrm{T}}Q^{\mathrm{T}})(QWM^{\mathrm{T}})) = \frac{1}{(j!)^2}\det(M(W^{\mathrm{T}}Q^{\mathrm{T}}QW)M^{\mathrm{T}}) \\
&= \frac{1}{(j!)^2}\det(W^{\mathrm{T}}ZW)\det(MM^{\mathrm{T}}) = \frac{1}{(j!)^2}\det(W^{\mathrm{T}}ZW)\det(MW^{\mathrm{T}}WM^{\mathrm{T}})
\end{aligned}$$

$$= \det(W^{\mathrm{T}}ZW)\frac{1}{(j!)^2}\det(A_0A_0^{\mathrm{T}}) = \det(W^{\mathrm{T}}ZW)\mathrm{vol}(S)$$

$$\leqslant \mathrm{vol}(S)\prod_{i=1}^{j}\lambda_i,$$

with equality in the last step for $W = (v_1,\dots,v_j)$. Now, by Proposition 1.2, S is a largest j-simplex in $\mathbb{B}^n$ if and only if S is regular and its vertices all belong to the boundary of a central j-section of $\mathbb{B}^n$. But this is achieved only if $x_0 \in \mathrm{lin}\{v_1,\dots,v_j\}$, whence $S \subset \mathrm{lin}\{v_1,\dots,v_j\}$. The rest of the assertion then follows from Proposition 1.2. □

We note in passing that if K is an n-dimensional ellipsoid, Lemma 2.1 implies that for each j, every largest j-simplex in K contains the center of K. If $j=1$ or n, this conclusion holds for an arbitrary centrally symmetric K. (Use Proposition 1.1 when $j=n$.) However, Asa Packer has pointed out that for each (j,n) with $1<j<n$ there is an n-dimensional affine cross-polytope in which no largest j-simplex contains the center.

2.2. A modified shallow-cut ellipsoid algorithm

For easy reading we apply the following notational convention: j-simplices contained in $\mathbb{B}^n$ are denoted by S, their images under the affine map $x \mapsto q+Qx$ are denoted by T, and homothetic images of T are denoted by U.

The ellipsoid algorithm will produce a homothetic copy of a j-simplex 'close' to a largest j-Simplex in $E=E_{Z,q}$ that is contained in K. For this we have to solve the following problem in each step of the algorithm. (Recall that $E(\varepsilon)$ is an outer parallel body of E.)

Simplex Problem. *Given $j,n \in \mathbb{N}$ with $j \leqslant n$, a well-bounded body K in $\mathbb{E}^n$ given by a weak separation oracle, an ellipsoid $E=E_{Z,q}$, and positive rationals μ, ν and ε, do one of the following*:

- produce a j-simplex

  $$T = \mathrm{conv}\{y_0,\dots,y_j\} \subset E(\varepsilon)$$

  for which

  $$(1+\mu)\mathrm{vol}(T) \geqslant \sigma(E,j)$$

  and assert that the j-simplex

  $$U = q + \frac{1}{\nu+1}\frac{1}{n+1}\mathrm{conv}\{y_0-q,\dots,y_j-q\}$$

  is contained in K; or

- produce a nonzero vector $c \in \mathbb{Q}^n$ such that

$$c^{\mathrm{T}}x \leqslant c^{\mathrm{T}}q + \frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}$$

for all $x \in K$.

A vector c with the stated property is called a *shallow-cut* for K, and an algorithm that solves the simplex problem is here called a *simplex oracle*. For geometric understanding, note that

$$\max_{x \in E_{Z,q}} c^{\mathrm{T}}x = c^{\mathrm{T}}q + \sqrt{c^{\mathrm{T}}Zc}.$$

Before constructing a simplex oracle, we should remark that Lemma 2.1 shows only how to construct T using infinite precision real arithmetic. In general, neither the construction of S nor the computation of Q can be done exactly in finite precision. (In fact, regular n-simplices with rational vertices do not exist in all dimensions; see [23,24].) However, [5] shows that standard rounding techniques can be used to carry out all the relevant computations in finite precision of polynomially bounded length.

Lemma 2.2. *There is a polynomial-time algorithm which, accepting as input positive integers j, n with $j \leqslant n$, an ellipsoid $E = E_{Z,q}$ in $\mathbb{E}^n$, and positive rationals μ and ε, produces a j-simplex T with*

$$T \subset E(\varepsilon) \quad \text{and} \quad (1+\mu)\mathrm{vol}(T) \geqslant \sigma(E, j).$$

The following result yields the desired simplex oracle.

Theorem 2.3. *The simplex problem can be solved in oracle-polynomial time.*

Proof. Let $(K, j, n, E, \mu, v, \varepsilon')$ be an instance of the simplex problem with $E = E_{Z,q}$ and $Z = Q^T Q$. We choose a positive rational ε with

$$\varepsilon \leqslant \min\{\varepsilon', v, \underline{\lambda}_n/((v+1)(n+2)^2)\},$$

where $\underline{\lambda}_n$ denotes a positive lower bound for the smallest eigenvalue λ_n of Z, and apply Lemma 2.2 to $(j, n, E, \mu, \varepsilon)$ so as to produce a j-simplex

$$T = \mathrm{conv}\{y_0, \ldots, y_j\} \subset E(\varepsilon) \subset E(\varepsilon').$$

Note that $\underline{\lambda}_n$ can be determined in polynomial time using binary search on the parameter τ, using the fact that $Z - \tau I_n$ is positive definite if and only if the determinants of its principal submatrices are all positive.

Now, we call the weak separation oracle for K, using the given ε and using, for the y to be presented to the oracle, the $2(j+1) \times n$ choices given by

$$y = q + \frac{1}{v+1}\,\frac{1}{n+1}(y_k - q) \pm n\varepsilon e_l$$

for $k=0,\dots,j$ and $l=1,\dots,n$. (Here e_l is the lth standard unit vector.) If all assertions are affirmative, i.e., if

$$q+\frac{1}{v+1}\frac{1}{n+1}(y_k-q)\pm n\varepsilon e_l\in K(\varepsilon)$$

for all $k=0,\dots,j$ and $l=1,\dots,n$, we conclude from $U(\varepsilon)\subset K(\varepsilon)$ that

$$U=q+\frac{1}{v+1}\,\frac{1}{n+1}\operatorname{conv}\{y_0-q,\dots,y_j-q\}\subset K.$$

Otherwise, we obtain a vector $c\in\mathbb{Q}^d$ with $||c||_\infty=1$ and such that (without loss of generality)

$$c^{\mathrm{T}}x\leqslant c^{\mathrm{T}}q+\frac{1}{v+1}\,\frac{1}{n+1}c^{\mathrm{T}}(y_0-q)+n\varepsilon c^{\mathrm{T}}e_1+\varepsilon$$

for all $x\in K$. Note that since K is well bounded we may assume, without loss of generality, that the inequality holds for all $x\in K$ rather than merely for $x\in K(-\varepsilon)$, cf. [15, Remark 3.2.34]. To derive the shallow-cut we must show that the inequality

$$c^{\mathrm{T}}x\leqslant c^{\mathrm{T}}q+\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}$$

holds for all $x\in K$. In fact, since

$$\max\{c^{\mathrm{T}}x\colon x\in q+Q\mathbb{B}^n\}=c^{\mathrm{T}}q+\sqrt{c^{\mathrm{T}}Zc}$$

and $y_0\in E(\varepsilon)$, we see that for all $x\in K$,

$$\begin{aligned}
c^{\mathrm{T}}x &\leqslant c^{\mathrm{T}}q+\frac{1}{v+1}\,\frac{1}{n+1}c^{\mathrm{T}}(y_0-q)+n\varepsilon c^{\mathrm{T}}e_1+\varepsilon\\
&\leqslant c^{\mathrm{T}}q+\frac{1}{v+1}\,\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}+(n+2)\varepsilon\\
&= c^{\mathrm{T}}q+\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}-\frac{v}{v+1}\,\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}+(n+2)\varepsilon\\
&\leqslant c^{\mathrm{T}}q+\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}-\frac{v}{v+1}\,\frac{1}{n+1}\lambda_n||c||_2+(n+2)\varepsilon\\
&\leqslant c^{\mathrm{T}}q+\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}-\frac{v}{v+1}\,\frac{1}{n+1}\underline{\lambda}_n||c||_\infty+(n+2)\varepsilon\\
&\leqslant c^{\mathrm{T}}q+\frac{1}{n+1}\sqrt{c^{\mathrm{T}}Zc}. \qquad \square
\end{aligned}$$

Now we come to the main result of this section.

Theorem 2.4. *There is an oracle-polynomial-time algorithm which, accepting as input positive integers j,n with $j\leqslant n$, positive rationals μ and v, and a well-bounded body $K\in\mathscr{K}^n$ given by a weak separation oracle, produces a j-simplex U contained in K with*

$$\operatorname{vol}(U)\leqslant\sigma(K,j)\leqslant(1+\mu)(1+v)^j(n+1)^j\operatorname{vol}(U).$$

Proof. First we apply [15, Theorem 3.3.3] with the following notion of 'toughness': an ellipsoid E that contains K is called 'tough' if a current candidate j-simplex U is contained in K. It follows that there is an oracle-polynomial-time algorithm that accepts as input positive integers j,n with $j\leqslant n$, a positive rational η, and a well-bounded body K given by a simplex oracle, and that either concludes with the first outcome (E,U) of the simplex problem or produces an ellipsoid E with $K\subset E$ and $\mathrm{vol}(E)\leqslant\eta$. Of course, when the above algorithm is applied with $\eta=(r/n)^n$, where r denotes the given lower bound for K's inradius, then the second answer is impossible. Hence, after a polynomial number of steps, we obtain a j-simplex U that is contained in K and is a homothetic copy of a j-simplex T with $T\subset E(\varepsilon)$ and $(1+\mu)\mathrm{vol}(T)\geqslant\sigma(E,j)$ with scaling-factor $1/((v+1)(n+1))$. We conclude by noting that

$$\begin{aligned}\mathrm{vol}(U) &\leqslant \sigma(K,j)\leqslant\sigma(E,j)\leqslant(1+\mu)\mathrm{vol}(T)\\ &= (1+\mu)(v+1)^j(n+1)^j\mathrm{vol}(U). \qquad\square\end{aligned}$$

As an immediate consequence of Theorem 2.4, we obtain the desired lower bounds for the accuracy that can be achieved when σ_γ is approximated by means of an oracle-polynomial-time algorithm.

Corollary 2.5. The accuracy in oracle-polynomial-time approximation of largest $\gamma(n)$-simplices in bodies is

$$\alpha_\gamma\geqslant\left(\frac{\log n}{n}\right)^{1/2}\quad\text{if }\gamma(n)\equiv 1,\quad\text{and}\quad\alpha_\gamma\geqslant\left(\frac{c}{n}\right)^{j}\quad\text{if } j=\gamma(n)\geqslant 2,$$

where c is a universal constant.

Proof. The case $\gamma\equiv 1$ is contained in [7,6]. For $\gamma\neq 1$ the result follows from Theorem 2.4 in conjunction with Proposition 1.3. $\square$

Corollary 2.6. The accuracy in oracle-polynomial-time approximation of largest $\gamma(n)$-simplices in centrally-symmetric bodies is

$$\alpha_\gamma\geqslant\left(\frac{\log n}{n}\right)^{1/2}\quad\text{if }\gamma(n)\equiv 1,\quad\text{and}\quad\alpha_\gamma\geqslant\left(\frac{c}{n}\right)^{j/2}\quad\text{if } j=\gamma(n)\geqslant 2.$$

Proof. Just note that for centrally-symmetric bodies the shallow-cut ellipsoid algorithm can be improved by using parallel cuts yielding a scaling factor of $(c/n)^{1/2}$, see [15]. $\square$

3. An upper bound

We will now derive the upper bound for α_γ that is stated in the introduction.

Suppose that the *a priori* information asserts that a member K of $\mathscr{K}^n$ contains $\mathbb{B}^n$. Suppose further that we call the separation oracle with points outside $\mathbb{B}^n$ and we always get a separating hyperplane. Then, after n^β calls to the oracle, no algorithm (that cannot access additional information) can distinguish K from $\mathbb{B}^n$ or from the resulting $\mathscr{H}$-polytope P with at most n^β facets. Hence it remains to derive a lower bound for the volume of a largest j-simplex in P. The argument for this is based on the fact (used iteratively) that P contains a vertex 'far away' from the origin [1,3,8].

The first proposition is a restatement of a result of [8].

Proposition 3.1. *There exists a positive constant $\rho < 1$ such that for all $k, \kappa \in \mathbb{N}$ with $\log(\kappa+1) \leqslant k \leqslant \kappa$, every k-dimensional 0-symmetric polytope that contains $\mathbb{B}^k$ and has at most κ facets has a vertex v with*

$$||v|| \geqslant \rho\left(\frac{k}{\log(\kappa/k+1)}\right)^{1/2}.$$

The next lemma provides a tool for the iterative construction of a large j-simplex.

Lemma 3.2. *Let $j', n', \kappa \in \mathbb{N}$ with $j' \leqslant n'$, and let P be a 0-symmetric n'-polytope in $\mathbb{E}^{n'}$ with at most κ facets. Further, let $v \in P \setminus \{0\}$, let V denote the linear subspace of $E^{n'}$ perpendicular to v, and let $P' = P \cap V$. Then P' has at most κ facets and*

$$\sigma(P, j') \geqslant ||v|| \cdot \begin{cases} 2 & \text{for } j' = 1, \\ \sigma(P'; j'-1)/j' & \text{for } j' \geqslant 2. \end{cases}$$

Proof. The assertion is a direct consequence of Proposition 1.1. □

Lemma 3.3. *There exists a positive constant $\rho < 1$ such that the following holds. Let $j, n, \beta \in \mathbb{N}$ with $j \leqslant n$, $n, \beta \geqslant 2$, and $\log(n^\beta + 1) \leqslant n$, and let P be a 0-symmetric n-polytope that contains $\mathbb{B}^n$ and has at most n^β facets. Then P contains a j-simplex S with*

$$\mathrm{vol}(S) \geqslant \begin{cases} \frac{2}{3}\rho^j \left(\frac{1}{j}\frac{n!}{(n-j)!}\right)^{1/2} (\beta \log n)^{-j/2} \sigma(\mathbb{B}^n, j) & \text{if } j \leqslant t, \\ \frac{1}{3}\rho^t \left(\frac{j-t}{j}\frac{n!}{(n-t)!}\right)^{1/2} (\beta \log n)^{-t/2} \sigma(\mathbb{B}^n, j) & \text{if } j > t, \end{cases}$$

where $t = n - \log(n^\beta + 1) + 1$.

Proof. Let j, n, β, P satisfy the assumptions. First note that for $n, \beta \geqslant 2$ and $l \in \mathbb{N}$ with $2 \leqslant l \leqslant n$,

$$\log\left(\frac{n^\beta}{l} + 1\right) \leqslant \beta \log n \quad \text{whence} \quad \frac{l}{\log(n^\beta/l+1)} \geqslant \frac{l}{\beta \log n}.$$

Now, using the inequalities

$$\frac{\sqrt{j}}{j!} \leqslant \sigma(\mathbb{B}^n, j) \leqslant \frac{\sqrt{e(j+1)}}{j!} \leqslant 3\frac{\sqrt{j}}{j!}$$

and combining Proposition 3.1 and Lemma 3.2 iteratively, we obtain for $j \leqslant t$

$$\begin{aligned}\sigma(P,j) &\geqslant 2\prod_{s=1}^{j}\rho\left(\frac{n-s+1}{\beta\log n}\right)^{1/2}\frac{1}{j-s+1}\\ &\geqslant \frac{2}{3}\left(\frac{1}{j}\frac{n!}{(n-j)!}\right)^{1/2}\rho^{j}(\beta\log n)^{-j/2}\sigma(\mathbb{B}^n,j).\end{aligned}$$

For $j > t$ we obtain similarly

$$\begin{aligned}\sigma(P,j) &\geqslant \sigma(\hat{P},j-t)\prod_{s=1}^{t}\rho\left(\frac{n-s+1}{\beta\log n}\right)^{1/2}\frac{1}{j-s+1}\\ &\geqslant \sigma(\mathbb{B}^n,j-t)\left(\frac{n!}{(n-t)!}\right)^{1/2}\rho^{t}(\beta\log n)^{-t/2}\frac{(j-t)!}{j!}\\ &\geqslant \frac{1}{3}\left(\frac{j-t}{j}\frac{n!}{(n-t)!}\right)^{1/2}\rho^{t}(\beta\log n)^{-t/2}\sigma(\mathbb{B}^n,j),\end{aligned}$$

where $\hat{P}$ denotes the intersection of P with the appropriate $(n-t)$-dimensional subspace that is constructed in the iterative application of Lemma 3.2. □

Now, we are ready to prove the desired upper bounds for the accuracy of polynomial-time approximations of σ_γ by means of algorithms that are restricted to those members of $\mathscr{A}_\gamma$ that make at most n^β calls to the oracle describing the body K of $\mathscr{K}^n$.

Theorem 3.4. *There exists a positive constant $\rho < 1$ such that for each $\beta \in \mathbb{N}\setminus\{1\}$*

$$\alpha_{\beta,\gamma} \leqslant \left(j\frac{(n-j)!}{n!}\right)^{1/2}\left(\frac{\beta}{\rho^2}\log n\right)^{j/2} \qquad \text{if } j=\gamma(n)\leqslant t,$$

$$\alpha_{\beta,\gamma} \leqslant \left(\frac{j}{j-t}\frac{(n-t)!}{n!}\right)^{1/2}\left(\frac{\beta}{\rho^2}\log n\right)^{t/2} \qquad \text{if } j=\gamma(n) > t,$$

where $t = n - \log(n^\beta + 1) + 1$.

Proof. Any oracle-polynomial-time algorithm that is restricted to making at most n^β calls to the oracle describing a given n-dimensional body K cannot distinguish between $\mathbb{B}^n$ and a polytope P^n having at most n^β facets. Corollary 3.3 then yields the stated result. □

References

[1] K. Ball, A. Pajor, Convex Bodies with few faces, Proc. Amer. Math. Soc. 104 (1990) 225–231.
[2] K.S. Banerjee, Weighing Designs for Chemistry, Medicine, Economics, Operations research, Statistics, Marcel Dekker, New York, 1975.
[3] I. Bárány, Z. Füredi, Computing the volume is difficult, Discrete Comput. Geom. 2 (1987) 319–326.

[4] J.W. Boardman, A.F.H. Goetz, Sedimentary facies analysis using imaging spectrometry: a geophysical inverse problem, Proceedings of the Third AVIRIS Workshop, Pasadena, CA, Jet Propulsion Laboratory, 1991, JPL Publication 91-28, pp. 4–13.
[5] A. Brieden, Approximation algorithms in computational convexity, Ph.D. Thesis, Technische Universität München, Munich, Germany, 1998.
[6] A. Brieden, P. Gritzmann, R. Kannan, V. Klee, L. Lovász, and M. Simonovits. Deterministic and randomized polynomial-time approximation of radii. to be submitted.
[7] A. Brieden, P. Gritzmann, R. Kannan, V. Klee, L. Lovász, and M. Simonovits. Approximation of radii and norm-maxima: Randomization doesn't help. in: Proc. 39th IEEE FOCS, pages 244–251, 1998.
[8] B. Carl, A. Pajor, Gelfand numbers of operators with values in a Hilbert space, Invent. Math. 94 (1988) 479–504.
[9] J.H.E. Cohn, Determinants with elements ± 1, II, Bull. London Math. Soc. 21 (1989) 36–42.
[10] M. Dyer, A. Frieze, On the complexity of computing the volume of a polytope, SIAM J. Comput. 17 (1988) 967–974.
[11] A.F.H. Goetz, Imaging spectrometry for earth remote sensing, in: F. Toselli, J. Bodechtel (Eds.), Imaging Spectroscopy: Fundamentals and Prospective Applications, Brussels, 1992, pp. 1–19.
[12] P. Gritzmann, V. Klee, Computational complexity of inner and outer j-radii of polytopes in finite-dimensional normed spaces, Math. Programming 59 (1993) 163–213.
[13] P. Gritzmann, V. Klee, On the complexity of some basic problems in computational convexity: I. containment problems, Discrete Math. 136 (1994) 129–174, Reprinted in: W. Deuber, H.J. Proemel, B. Voigt (Eds.), Trends in Discrete Mathematics, North-Holland, Amsterdam, 1995.
[14] P. Gritzmann, V. Klee, D. Larman, Largest j-simplices in n-polytopes, Discrete Comput. Geom. 34 (1995) 477–515.
[15] M. Grötschel, L. Lovász, A. Schrijver, Geometric Algorithms and Combinatorial Optimization, Springer, Berlin, 1988, 2nd Edition, 1993.
[16] M. Hudelson, V. Klee, D. Larman, Largest j-simplices in d-cubes: Some relatives of the Hadamard maximum determinant problem, Linear Algebra Appl. 241–243 (1996) 519–598.
[17] L.G. Khachiyan. On the complexity of approximating extremal determinants in matrices. J. Complexity, 11:138–153, 1995.
[18] C. Kisielowski, P. Schwander, F.H. Baumann, M. Seibt, Y. Kim, A. Ourmazd, An approach to quantitative high-resolution transmission electron microscopy of crystalline materials, Ultramicroscopy 58 (1995) 131–155.
[19] H. Lütkepohl, Handbook of Matrices, Wiley, New York, 1996.
[20] M.G. Neubauer, A.J. Radcliffe, The maximum determinant of $(\pm)$ matrices, Linear Algebra Appl. 257 (1997) 289–306.
[21] M.G. Neubauer, W. Watkins, J. Zeitlin, Maximal j-simplices in the real d-dimensional cube, J. Combin. Theory A 80 (1997) 1–12.
[22] M.G. Neubauer, W. Watkins, and J. Zeitlin. D-optimal weighing designs for four and five objects. Electronic Journal of Linear Algebra, 4:48–73, 1998.
[23] M.J. Pelling, Regular simplices with rational vertices, Bull. London Math. Soc. 9 (1977) 199–200.
[24] I.J. Schoenberg, Regular simplices and quadratic forms, J. London Math. Soc. 12 (1937) 48–55.
[25] N.Z. Shor. Cut-off method with space extension in convex programming problems. Kibernetika, 1977(1):94–95, 1977. English translation: Cybernetics 13 (1977), 94–96.
[26] B.D. Yudin, A.S. Nemirovskii, Informational complexity and efficient methods for the solution of convex extremal problems, Ekonomika i Matematicheskie Metody 12 (1976) 357–369. (English translation: Matekon 13 (2) 3–25, 1977.)