Martin Grötschel
László Lovász
Alexander Schrijver

Geometric Algorithms and Combinatorial Optimization

几何算法和组合最优化 [英]

Springer-Verlag
World Publishing Corp

Martin Grötschel
László Lovász
Alexander Schrijver

Geometric Algorithms and Combinatorial Optimization

Springer-Verlag
World Publishing Corp

Martin Grötschel
Institute of Mathematics
University of Augsburg
Memminger Straße 6
D-8900 Augsburg
Fed. Rep. of Germany

László Lovász
Department of Computer Science
Eötvös Loránd University
Budapest
Múzeum krt. 6–8
Hungary H-1088

Alexander Schrijver
Department of Econometrics
Tilburg University
P.O. Box 90153
NL-5000 LE Tilburg
The Netherlands

1980 Mathematics Subject Classification (1985 Revision):
primary 05-02, 11Hxx, 52-02, 90Cxx; secondary 05Cxx, 11H06, 11H55, 11J13, 52A43, 68Q25, 90C05, 90C10, 90C25, 90C27

ISBN 3-540-13624-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-13624-X Springer-Verlag New York Berlin Heidelberg

With 23 Figures

Library of Congress Cataloging-in-Publication Data
Grötschel, Martin.
Geometric algorithms and combinatorial optimization.
(Algorithms and combinatorics; 2)
Bibliography: p. Includes indexes.
1. Combinatorial geometry. 2. Geometry of numbers. 3. Mathematical optimization. 4. Programming (Mathematics) I. Lovász, László, 1948–. II. Schrijver, A. III. Title. IV. Series. QA167.G76 1988 511'.6 87-36923
ISBN 0-387-13624-X (U.S.)

Reprinted by World Publishing Corporation, Beijing, 1990
for distribution and sale in The People's Republic of China only
ISBN 7-5062-0768-0

Preface

Historically, there is a close connection between geometry and optimization. This is illustrated by methods like the gradient method and the simplex method, which are associated with clear geometric pictures. In combinatorial optimization, however, many of the strongest and most frequently used algorithms are based on the discrete structure of the problems: the greedy algorithm, shortest path and alternating path methods, branch-and-bound, etc. In the last several years geometric methods, in particular polyhedral combinatorics, have played a more and more profound role in combinatorial optimization as well.

Our book discusses two recent geometric algorithms that have turned out to have particularly interesting consequences in combinatorial optimization, at least from a theoretical point of view. These algorithms are able to utilize the rich body of results in polyhedral combinatorics.

The first of these algorithms is the **ellipsoid method**, developed for nonlinear programming by N. Z. Shor, D. B. Yudin, and A. S. Nemirovskiĭ. It was a great surprise when L. G. Khachiyan showed that this method can be adapted to solve linear programs in polynomial time, thus solving an important open theoretical problem. While the ellipsoid method has not proved to be competitive with the simplex method in practice, it does have some features which make it particularly suited for the purposes of combinatorial optimization.

The second algorithm we discuss finds its roots in the classical "geometry of numbers", developed by Minkowski. This method has had traditionally deep applications in number theory, in particular in diophantine approximation. Methods from the geometry of numbers were introduced in integer programming by H. W. Lenstra. An important element of his technique, called **basis reduction**, goes in fact back to Hermite. An efficient version of basis reduction yields a polynomial time algorithm useful not only in combinatorial optimization, but also in fields like number theory, algebra, and cryptography.

A combination of these two methods results in a powerful tool for combinatorial optimization. It yields a theoretical framework in which the polynomial time solvability of a large number of combinatorial optimization problems can be shown quite easily. It establishes the algorithmic equivalence of problems which are "dual" in various senses.

Being this general, this method cannot be expected to give running times comparable with special-purpose algorithms. Our policy in this book is, therefore, not to attempt to obtain the best possible running times; rather, it is to derive just the polynomial time solvability of the problems as quickly and painlessly as possible. Thus, our results are best conceived as "almost pure" existence results for polynomial time algorithms for certain problems and classes of problems.

Nevertheless, we could not get around quite a number of tedious technical details. We did try to outline the essential ideas in certain sections, which should give an outline of the underlying geometric and combinatorial ideas. Those sections which contain the technical details are marked by an asterisk in the list of contents. We therefore recommend, for a first reading, to skip these sections.

The central result proved and applied in this book is, roughly, the following. If K is a convex set, and if we can decide in polynomial time whether a given vector belongs to K, then we can optimize any linear objective function over K in polynomial time. This assertion is, however, not valid without a number of conditions and restrictions, and even to state these we have to go through many technical details. The most important of these is that the optimization can be carried out in an approximate sense only (as small compensation, we only need to test for membership in K in an approximate sense).

Due to the rather wide spread of topics and methods treated in this book, it seems worth while to outline its structure here.

Chapters 0 and 1 contain mathematical preliminaries. Of these, Chapter 1 discusses some non-standard material on the complexity of problems, efficiency of algorithms and the notion of oracles.

The main result, and its many versions and ramifications, are obtained by the ellipsoid method. Chapter 2 develops the framework necessary for the formulation of algorithmic problems on convex sets and the design of algorithms to solve these. A list of the main problems introduced in Chapter 2 can be found on the inner side of the back cover. Chapter 3 contains the description of (two versions of) the ellipsoid method. The statement of what exactly is achieved by this method is rather complicated, and the applications and specializations collected in Chapter 4 are, perhaps, more interesting. These range from the main result mentioned above to results about computing the diameter, width, volume, and other geometric parameters of convex sets. All these algorithms provide, however, only approximations.

Polyhedra encountered in combinatorial optimization have, typically, vertices with small integral entries and facets with small integral coefficients. For such polyhedra, the optimization problem (and many other algorithmic problems) can be solved in the exact sense, by rounding an approximate solution appropriately. While for many applications a standard rounding to some number of digits is sufficient, to obtain results in full generality we will have to use the sophisticated rounding technique of diophantine approximation. The basis reduction algorithm for lattices, which is the main ingredient of this technique, is treated in Chapter 5, along with several applications. Chapter 6 contains the main applications of diophantine approximation techniques. Besides strong versions of the main result, somewhat different combinations of the ellipsoid method with basis reduction give the strongly polynomial time solvability of several combinatorial optimization problems, and the polynomial time solvability of integer linear programming in fixed dimension, remarkable results of É. Tardos and H. W. Lenstra, respectively.

Chapters 7 to 10 contain the applications of the results obtained in the previous chapters to combinatorial optimization. Chapter 7 is an easy-to-read introduction to these applications. In Chapter 8 we give an in-depth survey of combinatorial optimization problems solvable in polynomial time with the methods of Chapter 6. Chapters 9 and 10 treat two specific areas where the ellipsoid method has resolved important algorithmic questions that so far have resisted direct combinatorial approaches: perfect graphs and submodular functions.

We are grateful to several colleagues for many discussions on the topic and text of this book, in particular to Bob Bixby, András Frank, Michael Jünger, Gerhard Reinelt, Éva Tardos, Klaus Truemper, Yoshiko Wakabayashi, and Zaw Win. We mention at this point that the technique of applying the ellipsoid method to combinatorial optimization problems was also discovered by R. M. Karp, C. H. Papadimitriou, M. W. Padberg, and M. R. Rao.

We have worked on this book over a long period at various institutions. We acknowledge, in particular, the support of the joint research project of the German Research Association (DFG) and the Hungarian Academy of Sciences (MTA), the Universities of Amsterdam, Augsburg, Bonn, Szeged, and Tilburg, Cornell University (Ithaca), Eötvös Loránd University (Budapest), and the Mathematical Centre (Amsterdam).

Our special thanks are due to Frau Theodora Konnerth for the efficient and careful typing and patient retyping of the text in TEX.

March 1987

Martin Grötschel
László Lovász
Alexander Schrijver

Table of Contents

The sections and chapters marked with * are technical. We recommend that the reader skip these on the first reading.

Chapter 0

Mathematical Preliminaries

This chapter summarizes mathematical background material from linear algebra, linear programming, and graph theory used in this book. We expect the reader to be familiar with the concepts treated here. We do not recommend to go thoroughly through all the definitions and results listed in the sequel – they are mainly meant for reference.

0.1 Linear Algebra and Linear Programming

In this section we survey notions and well-known facts from linear algebra, linear programming, polyhedral theory, and related fields that will be employed frequently in subsequent chapters. We have also included a number of useful inequalities and estimates. The material covered here is standard and can be found in several textbooks. As references for linear algebra we mention FADDEEV and FADDEEVA (1963), GANTMACHER (1959), LANCASTER and TISMENETSKY (1985), MARCUS and MINC (1964), STRANG (1980). For information on linear programming and polyhedral theory see for instance CHVÁTAL (1983), DANTZIG (1963), GASS (1984), GRÜNBAUM (1967), ROCKAFELLAR (1970), SCHRIJVER (1986), STOER and WITZGALL (1970).

Basic Notation

By $\mathbb{R}$ ($\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{C}$) we denote the set of real (rational, integral, natural, complex) numbers. The set $\mathbb{N}$ of natural numbers does not contain zero. $\mathbb{R}_+$ ($\mathbb{Q}_+$, $\mathbb{Z}_+$) denotes the nonnegative real (rational, integral) numbers. For $n \in \mathbb{N}$, the symbol $\mathbb{R}^n$ ($\mathbb{Q}^n$, $\mathbb{Z}^n$, $\mathbb{N}^n$, $\mathbb{C}^n$) denotes the set of vectors with n components (or n-tuples or n-vectors) with entries in $\mathbb{R}$ ($\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{C}$). If E and R are sets, then R^E is the set of mappings of E to R. If E is finite, it is very convenient to consider the elements of R^E as $|E|$-vectors where each component of a vector $x \in R^E$ is indexed by an element of E, i. e., $x = (x_e)_{e \in E}$. For $F \subseteq E$, the vector $\chi^F \in \mathbb{R}^E$ defined by $\chi^F_e = 1$ if $e \in F$ and $\chi^F_e = 0$ if $e \in E \setminus F$ is called the **incidence vector** of F.

Addition of vectors and multiplication of vectors with scalars are as usual. With these operations, $\mathbb{R}^n$ and $\mathbb{Q}^n$ are vector spaces over the fields $\mathbb{R}$ and $\mathbb{Q}$, respectively, while $\mathbb{Z}^n$ is a module over the ring $\mathbb{Z}$. A vector is always considered as a **column vector**, unless otherwise stated. The **superscript** "T"

denotes **transposition**. So, for $x \in \mathbb{R}^n$, x^T is a row vector, unless otherwise stated. $\mathbb{R}^n$ is endowed with a **(Euclidean) inner product** defined as follows:

$$x^T y := \sum_{i=1}^{n} x_i y_i \quad \text{for } x, y \in \mathbb{R}^n.$$

For a real number α, the symbol $\lfloor \alpha \rfloor$ denotes the largest integer not larger than α (the **floor** or **lower integer part** of α), $\lceil \alpha \rceil$ denotes the smallest integer not smaller than α (the **ceiling** or **upper integer part** of α) and $\lceil \alpha \rfloor := \lceil \alpha - \frac{1}{2} \rceil$ denotes the integer nearest to α. If $a = (a_1, \ldots, a_n)^T$ and $b = (b_1, \ldots, b_n)^T$ are vectors, we write $a \leq b$ if $a_i \leq b_i$ for $i = 1, \ldots, n$.

For two sets M and N, the expression $M \subseteq N$ means that M is a subset of N, while $M \subset N$ denotes strict containment, i. e., $M \subseteq N$ and $M \neq N$. We write $M \setminus N$ for the set-theoretical difference $\{x \in M \mid x \notin N\}$, $M \Delta N$ for the **symmetric difference** $(M \setminus N) \cup (N \setminus M)$, and 2^M for the set of all subsets of M, the so-called **power set** of M. For $M, N \subseteq \mathbb{R}^n$ and $\alpha \in \mathbb{R}$, we use the following standard terminology for set operations: $M + N := \{x + y \mid x \in M, y \in N\}$, $\alpha M := \{\alpha x \mid x \in M\}$, $-M := \{-x \mid x \in M\}$, $M - N := M + (-N)$.

For any set R, $R^{m \times n}$ denotes the set of $m \times n$-**matrices** with entries in R. For a matrix $A \in R^{m \times n}$, we usually assume that the row index set of A is $\{1, \ldots, m\}$ and that the column index set is $\{1, \ldots, n\}$. Unless specified otherwise, the elements or entries of $A \in R^{m \times n}$ are denoted by a_{ij}, $1 \leq i \leq m$, $1 \leq j \leq n$; we write $A = (a_{ij})$. Vectors with n components are also considered as $n \times 1$-matrices.

If I is a subset of the row index set M of a matrix A and J a subset of the column index set N of A, then A_{IJ} denotes the submatrix of A induced by those rows and columns of A whose indices belong to I and J, respectively. Instead of A_{MJ} (A_{IN} resp.) we frequently write $A_{.J}$ ($A_{I.}$ resp.). A submatrix A of the form A_{II} is called a **principal submatrix** of A. If $K = \{1, \ldots, k\}$ then A_{KK} is called the k-th **leading principal submatrix** of A. $A_{i.}$ is the i-th row of A (so it is a row vector), and $A_{.j}$ is the j-th column of A.

Whenever we do not explicitly state whether a number, vector, or matrix is integral, rational, or complex it is implicitly assumed to be real. Moreover, we often do not specify the dimensions of vectors and matrices explicitly. When operating with them, we always assume that their dimensions are compatible.

The **identity matrix** is denoted by I or, if we want to stress its dimension, by I_n. The symbol 0 stands for any appropriately sized matrix which has all entries equal to zero, and similarly for any zero vector. The symbol $\mathbb{1}$ denotes a vector which has all components equal to one. The j**-th unit vector** in $\mathbb{R}^n$, whose j-th component is one while all other components are zero, is denoted by e_j. If $x = (x_1, \ldots, x_n)^T$ is a vector then the $n \times n$-matrix with the entries $x_1, \ldots, x_n$ on the main diagonal and zeros outside the main diagonal is denoted by diag(x). If $A \in R^{m \times p}$ and $B \in R^{m \times q}$ then (A, B) (or just $(A\ B)$ if this does not lead to confusion) denotes the matrix in $R^{m \times (p+q)}$ whose first p columns are the columns of A and whose other q columns are those of B.

The **determinant** of an $n \times n$-matrix A is denoted by det(A). The **trace** of an $n \times n$-matrix A, denoted by tr(A), is the sum of the elements of the main diagonal of the matrix A.

When using functions like det, tr, or diag we often omit the brackets if there is no danger of confusion, i. e., we frequently write det A instead of det(A) etc.

The inverse matrix of an $n \times n$-matrix A is denoted by A^{-1}. If a matrix has an inverse matrix then it is called **nonsingular**, and otherwise **singular**. An $n \times n$-matrix A is nonsigular if and only if det $A \neq 0$.

Hulls, Independence, Dimension

A vector $x \in \mathbb{R}^n$ is called a **linear combination** of the vectors $x_1, x_2, \ldots, x_k \in \mathbb{R}^n$ if, for some $\lambda \in \mathbb{R}^k$,

$$x = \sum_{i=1}^{k} \lambda_i x_i .$$

If, in addition,

$$\left.\begin{array}{l} \lambda \geq 0 \\ \qquad \lambda^T \mathbb{1} = 1 \\ \lambda \geq 0, \quad \lambda^T \mathbb{1} = 1 \end{array}\right\} \text{ we call } x \text{ a } \left\{\begin{array}{c} \textbf{conic} \\ \textbf{affine} \\ \textbf{convex} \end{array}\right\} \textbf{ combination}$$

of the vectors $x_1, x_2, \ldots, x_k$. These combinations are called **proper** if neither $\lambda = 0$ nor $\lambda = e_j$ for some $j \in \{1, 2, \ldots, k\}$. For a nonempty subset $S \subseteq \mathbb{R}^n$, we denote by

$$\left.\begin{array}{l} \text{lin}(S) \\ \text{cone}(S) \\ \text{aff}(S) \\ \text{conv}(S) \end{array}\right\} \text{ the } \left\{\begin{array}{c} \textbf{linear} \\ \textbf{conic} \\ \textbf{affine} \\ \textbf{convex} \end{array}\right\} \textbf{ hull} \text{ of the elements of } S,$$

that is, the set of all vectors that are linear (conic, affine, convex) combinations of finitely many vectors of S. For the empty set, we define lin($\emptyset$) := cone($\emptyset$) := $\{0\}$ and aff($\emptyset$) := conv($\emptyset$) := $\emptyset$.

A subset $S \subseteq \mathbb{R}^n$ is called

$$\left\{\begin{array}{l} \text{a } \textbf{linear subspace} \\ \text{a } \textbf{cone} \\ \text{an } \textbf{affine subspace} \\ \text{a } \textbf{convex set} \end{array}\right\} \text{ if } \left\{\begin{array}{l} S = \text{lin}(S) \\ S = \text{cone}(S) \\ S = \text{aff}(S) \\ S = \text{conv}(S) \end{array}\right\}.$$

A subset $S \subseteq \mathbb{R}^n$ is called **linearly (affinely) independent** if none of its members is a proper linear (affine) combination of elements of S; otherwise S is called **linearly (affinely) dependent**. It is well-known that a linearly (affinely) independent subset of $\mathbb{R}^n$ contains at most n elements ($n + 1$ elements). For any set $S \subseteq \mathbb{R}^n$, the **rank** of S (**affine rank** of S) denoted by rank(S) (arank(S)), is the cardinality of the largest linearly (affinely) independent subset of S. For any subset $S \subseteq \mathbb{R}^n$, the **dimension** of S, denoted by dim(S), is the cardinality of a largest affinely independent subset of S minus one, i. e., dim(S) = arank(S) − 1. A set $S \subseteq \mathbb{R}^n$ with dim(S) = n is called **full-dimensional**.

The **rank of a matrix** A (notation: rank(A)), is the rank of the set of its column vectors. This is known to be equal to the rank of the set of its row vectors. An $m \times n$-matrix A is said to have **full row rank (full column rank)** if rank $A = m$ (rank $A = n$).

Eigenvalues, Positive Definite Matrices

If A is an $n \times n$-matrix, then every complex number λ with the property that there is a nonzero vector $u \in \mathbb{C}^n$ such that $Au = \lambda u$ is called an **eigenvalue** of A. The vector u is called an **eigenvector** of A associated with λ. The function $f(\lambda) := \det(\lambda I_n - A)$ is a polynomial of degree n, called the **characteristic polynomial** of A. Thus the equation

$$\det(\lambda I_n - A) = 0$$

has n (complex) roots (multiple roots counted with their multiplicity). These roots are the (not necessarily distinct) n eigenvalues of A.

We will often consider **symmetric matrices** (i. e., $n \times n$-matrices $A = (a_{ij})$ with $a_{ij} = a_{ji}$, $1 \le i \le j \le n$). It is easy to see that all eigenvalues of real symmetric matrices are real numbers.

There are useful relations between the eigenvalues $\lambda_1, \ldots, \lambda_n$ of a matrix A, its determinant and its trace, namely

(0.1.1) $$\det A = \prod_{i=1}^{n} \lambda_i,$$

(0.1.2) $$\operatorname{tr} A = \sum_{i=1}^{n} \lambda_i.$$

An $n \times n$-matrix A is called **positive definite (positive semidefinite)** if A is symmetric and if $x^T A x > 0$ for all $x \in \mathbb{R}^n \setminus \{0\}$ ($x^T A x \ge 0$ for all $x \in \mathbb{R}^n$). If A is positive definite then A is nonsingular and its inverse is also positive definite. In fact, for a symmetric $n \times n$-matrix A the following conditions are equivalent:

(0.1.3)
- (i) A is positive definite.
- (ii) A^{-1} is positive definite.
- (iii) All eigenvalues of A are positive real numbers.
- (iv) $A = B^T B$ for some nonsingular matrix B.
- (v) $\det A_k > 0$ for $k = 1, \ldots, n$, where A_k is the k-th leading principal submatrix of A.

It is well known that for any positive definite matrix A, there is exactly one matrix among the matrices B satisfying (0.1.3) (iv) that is itself positive definite. This matrix is called the **(square) root** of A and is denoted by $A^{1/2}$.

Positive semidefinite matrices can be characterized in a similar way, namely, for a symmetric $n \times n$-matrix A the following conditions are equivalent:

(0.1.4)
- (i) A is positive semidefinite.
- (ii) All eigenvalues of A are nonnegative real numbers.
- (iii) $A = B^T B$ for some matrix B.
- (iv) $\det A_{II} \ge 0$ for all principal submatrices A_{II} of A.
- (v) There is a positive definite principal submatrix A_{II} of A with $|I| = \operatorname{rank} A$.

Vector Norms, Balls

A function $N : \mathbb{R}^n \to \mathbb{R}$ is called a **norm** if the following three conditions are satisfied:

(0.1.5) (i) $N(x) \geq 0$ for $x \in \mathbb{R}^n$, $N(x) = 0$ if and only if $x = 0$,
(ii) $N(\alpha x) = |\alpha| N(x)$ for all $x \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$,
(iii) $N(x+y) \leq N(x) + N(y)$ for all $x, y \in \mathbb{R}^n$ (**triangle inequality**).

Every norm N on $\mathbb{R}^n$ induces a **distance** d_N defined by

$$d_N(x, y) := N(x-y) \quad \text{for } x, y \in \mathbb{R}^n.$$

For our purposes four norms will be especially important:

$$\|x\| := \sqrt{x^T x} = \Big(\sum_{i=1}^n x_i^2\Big)^{1/2} \quad \text{(the } l_2\text{- or \textbf{Euclidean norm})}.$$

(This norm induces the **Euclidean distance** $d(x,y) = \|x-y\|$. Usually, the Euclidean norm is denoted by $\|\cdot\|_2$. But we use it so often that we write simply $\|\cdot\|$.)

$$\|x\|_1 := \sum_{i=1}^n |x_i| \qquad \text{(the } l_1\text{- or \textbf{1-norm})},$$

$$\|x\|_\infty := \max_{1 \leq i \leq n} |x_i| \qquad \text{(the } l_\infty\text{- or \textbf{maximum norm})},$$

$$\|x\|_A := \sqrt{x^T A^{-1} x},$$

where A is a positive definite $n \times n$-matrix. Recall that A induces an inner product $x^T A^{-1} y$ on $\mathbb{R}^n$. Norms of type $\|\cdot\|_A$ are sometimes called **general Euclidean** or **ellipsoidal norms**. We always consider the space $\mathbb{R}^n$ as a Euclidean space endowed with the Euclidean norm $\|\cdot\|$, unless otherwise specified. So all notions related to distances and the like are defined via the Euclidean norm.

For all $x \in \mathbb{R}^n$, the following relations hold between the norms introduced above:

(0.1.6) $$\|x\| \leq \|x\|_1 \leq \sqrt{n}\|x\|,$$

(0.1.7) $$\|x\|_\infty \leq \|x\| \leq \sqrt{n}\|x\|_\infty,$$

(0.1.8) $$\|x\|_\infty \leq \|x\|_1 \leq n\|x\|_\infty .$$

If A is a positive definite $n \times n$-matrix with smallest eigenvalue λ and largest eigenvalue Λ then

(0.1.9) $$\sqrt{\lambda}\|x\| \leq \|x\|_{A^{-1}} \leq \sqrt{\Lambda}\|x\| \quad \text{for all } x \in \mathbb{R}^n.$$