Geometric Methods in Combinatorial Optimization

M. Grötschel

Institut f. Ökonometrie und Operations Research
Universität Bonn
D-5300 Bonn, Germany

L. Lovász

Mathematical Institute
Eötvös L. University
Budapest, H-1088, Hungary

A. Schrijver

Instituut voor Actuariaat en Econometrie
Universiteit van Amsterdam
Jodenbreestraat 23, Amsterdam
The Netherlands

This paper is a somewhat polished-up form of the lecture notes for the instructional series of talks given by L. Lovasz. This series was based on a forthcoming book by the three authors, which discusses combinatorial applications of the ellipsoid method and other algorithms, most of which have a geometric flavor.

In this paper we take the opportunity to illuminate some of the problems one encounters when trying to develop and apply geometric algorithms, and to show some of the results which are easiest to state, without going into too many technical details. Some of these details can be found in the papers [GLS 1981 a], [GLS 1981 b], others will be elaborated in the book. In particular, we do not go into the description of the Ellipsoid Method (Shor 1970, Yudin - Nemirowskii 1976, Khachiyan 1979), since this is by now quite well known.

1. Convex sets and the Ellipsoid Method

It is a classical result that every compact convex set in $\mathbb{R}^n$ is the convex hull of its extreme points as well as the intersection of its supporting halfspaces. From an algorithmic point of view, there are two basic problems concerning a convex body K, paralleling the above two

characterizations: we may ask if a given point $y \in Q^n$ belongs to K, and also if a given halfspace $\{x \in \mathbb{R}^n : c^T x \leq d\}$ contains K. We call these the *membership* and *validity problems* respectively. It follows from the two characterizations that if we have an "oracle" which tells us the solution of, say, the membership problem, then this also determines the solution of the validity problem. But does it yield an algorithm to find this solution? The main implication of the *Ellipsoid Method* discovered by Shor (1970, 1976), Yudin and Nemirowskii (1976) and Khachiyan (1979) is that the validity and membership problems for a convex body are not only logically but algorithmically equivalent in the sense that any oracle answering one of these problems can be used to obtain a polynomial-time algorithm to answer the other one. This statement is, however, not precise and not valid without appropriate hypotheses on the way the convex body is given. Our first aim will be to describe these hypotheses and to show that in a sense they are quite natural.

Before going into these details, let us formulate two further algorithmic problems on convex bodies. The *separation problem* is a strengthening of the membership problem: it asks, for each $y \in Q^n$, to check whether $y \in K$ and if not, then to find a vector $c \in Q^n$ such that $c^T y > c^T x$ for every $x \in K$ (i.e. it asks for a separating hyperplane for each $y \in K$). The *optimization problem* asks, for each $c \in Q^n$, to find a point $x \in K$ maximizing the linear objective function $c^T x$ over K.

A few examples might illuminate the relationship between these problems.

EXAMPLES.

(1.1) Let $a_1, \ldots, a_m \in Q^n$, and $K = conv\{a_1, \ldots, a_m\}$. Then the validity and optimization problems for K are trivially solvable, the membership and separation problems are equivalent to linear programming.

(1.2) Let $a_1, \ldots, a_m \in Q^n$, $b_1, \ldots, b_m \in Q$ and $K = \{x \in \mathbb{R}^n : a_i^T x \leq b_i$ for $i = i, \ldots, m\}$. Then the membership and separation problems for K are trivial, the validity and optimization problems for K are equivalent to linear programming.

(1.3) Let $f : \mathbb{R}^n \to R$ be a convex function and $G_f = \{(x,t) : x \in \mathbb{R}^n, t \in \mathbb{R}, f(x) \leq t\}$ be the "epigraph" of f. Then the membership problem for G_f is trivial (provided we can evaluate f at any point $x \in Q^n$).. If we also have an algorithm to compute a subgradient of f, then the separation problem for f is also solvable. The validity and optimization problems for G_f include the problem of minimizing a convex function.

(1.4) Let K be a convex body described by its support function p. (The support function of K is defined as follows: for each unit vector v, $p(v)$ is the signed distance of the supporting hyperplane of K with outward normal vector v from the origin.) Then the validity problem for K is trivial, while the other three problems introduced above are not.

The optimization problem raises immediately the question: in what form do we want the answer? The maximum of $c^T x$ over K may be attained at an irrational point, and then the algorithm cannot have the exact answer as its output. Thus a more correct formulation is to ask for a point which "almost" maximizes the objective function $c^T x$. Although less apparent, more detailed analysis suggests that also for the other three problems, a "weak" formulation which allows for a small error is more correct in general. Thus we get to the following four weaker problems.

For any $x \subseteq \mathbb{R}^n$, $t \in \mathbb{R}$ satisfying $t > 0$, we define $S(x, t) = \{x \in \mathbb{R}^n : \inf\{|x-y| : y \in x\} \leq t\}$.

Weak membership problem.

Given a convex body K, a vector $y \in Q^n$, and a rational number $\xi > 0$, conclude with one of the following:

(a) $y \in S(K, \xi)$;

(b) $y \in S(\mathbb{R}^n - K, \xi)$.

Weak validity problem.

Given a convex body K, a vector $c \in Q^n$, and rational numbers $\xi > 0$ and d, conclude with one of the following:

(a) $c^T x \leq d + \xi$ for all $x \in K$;

(b) there exists an $x \in K$ for which $c^T x \geq d - \xi$.

Weak separation problem.

Given a convex body K, a vector $y \in Q^n$, and a rational number $\xi > 0$, conclude with one of the following:

(a) asserting that $y \in S(K, \xi)$,

(b) finding a vector $c \in Q^n$ such that $|c| > 1$ and $c^T y \geq c^T x - \xi$ for all $x \in K$.

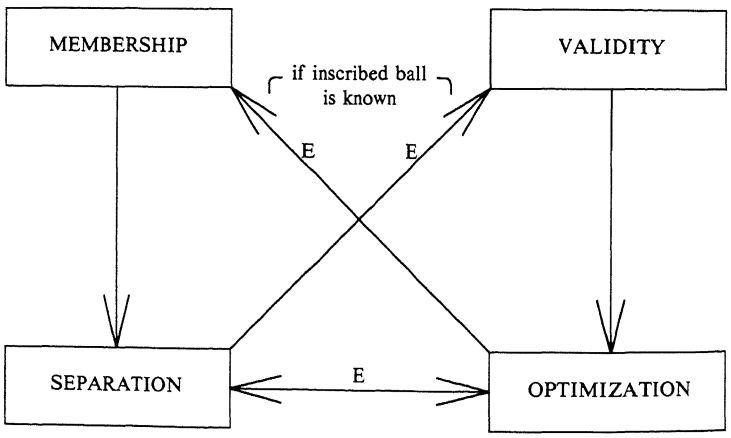
Weak optimization problem.

Given a convex body K, a vector $c \in Q^n$, and a rational number $\xi > 0$, find a vector $y \in Q^n \cap S(K, \xi)$ such that $c^T y \geq c^T x - \xi$ for all $x \in K$.

Note that the input of these problems includes the error bound ξ. Since we are interested in the running time as a function of the input length, we should point out that the input length for ξ is the number of binary digits necessary to write down the numerator and denominator of ξ. It would not make any essential difference, however, if we took $|\log_2 \xi|$ as the input length or ξ. Also note that with this definition, finding a number by binary search means as algorithm in which the number of iterations needed to determine the number with error ξ is linear in $|\log_2 \xi|$. It is interesting to remark in this respect that the Ellipsoid Method may be viewed as an n-dimensional generalization of binary search.

Finally, we briefly discuss convex bodies. To be able to apply these techniques, we need some *a priori* given information: the dimension of the space, a rational number $R > 0$ such that $K \subseteq S(0, R)$ and another rational number r such that K contains a ball with radius r. Sometimes we also need to know in advance the center of this ball with radius r.

The following chart shows the possible reductions between the four fundamental algorithmic problems concerning convex bodies, all problems in the weak sense.



Here the arrows marked by E mean reductions by the Ellipsoid Method, while the two unmarked arrows mean trivial reductions.

In combinatorial situations the convex bodies we encounter are usually polytopes, and in fact quite often they have $0-1$ vertices, or $0\ -1/2\ -1$ vertices. For such polytopes the hypotheses under which the membership-validity (or separation-optimization) equivalence holds can be weakened substantially. Most significantly, the weak and strong versions of the problems become equivalent. To state the result precisely we need the following definition.

A *rational polytope* is a triple $(P\ ;\ n\ ,\ T)$ such that $P \subseteq \mathbb{R}^n$ is a polytope such that each entry of each vertex of P is a rational number with numerator and denominator at most T.

LEMMA. If a rational polytope P is full-dimensional then $(P\ ;\ n,\ (nT^n)^{-n-1}\ ,nT)$ is a well-bounded convex body. Further, every facet of P can be described by a linear inequality whose coefficients are integers not exceeding $(nT)^n$.

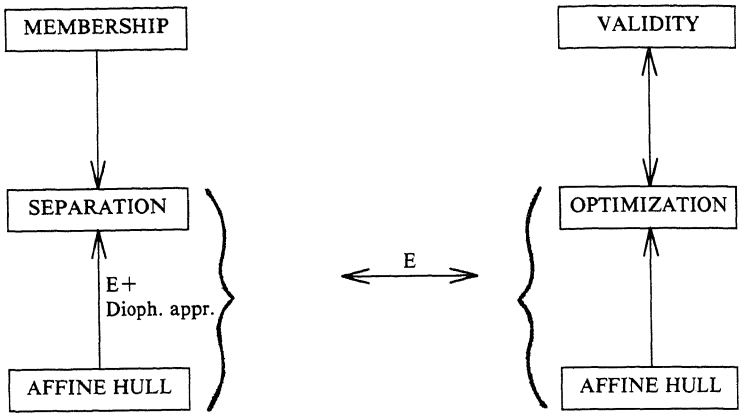
Note that full-dimensionality is not included in the definition of a rational polytope. In fact, one of the significant advantages of rational polytopes over convex bodies is that their affine hull can be determined either from an optimization oracle (Edmonds, Lovasz, Pulleyblank (1982)) or from a separation oracle. This latter is a rather complicated reduction, involving the Ellipsoid Method as well as simultaneous diophantine approximation (whose algorithmic aspects will be discussed briefly in the next section). Details of this reduction will be given in our book. Let us remark, however, that with somewhat stronger separation oracles the optimization and affine hull problems were solved by Karp and Papadimitriou (1980) and by Padberg and Rao (1981).

The following chart shows the algorithmic reducibilities between these basic problems on rational polytopes.

2. Algorithmic Problems for Lattices

Lattice geometry, also called the "geometry of numbers", is an important tool in number theory. Its role in combinatorics or discrete optimization has, however, been quite moderate compared with, say, the role of convex polytopes. This is, to a certain extent, unjustified. There are two major fields in mathematics which deal with lattice points in convex bodies: discrete optimization and the geometry of numbers. While certain ideas have been used in both fields successfully (e.g. polarity), the interfaces between these two fields have been very meager. It seems, however, that if we look at the algorithmic aspects then common problems and methods are easily found.

In this section we survey some of the simplest algorithmic problems for lattices and then describe an algorithm for finding a "simple"



basis in a lattice (A.K. Lenstra, H.W. Lenstra jr. and L. Lovasz 1982). This algorithm will have applications to simultaneous diophantine approximation as well as to integer programming in bounded dimension, where it can be used to improve the efficiency of a celebrated algorithm due to H.W. Lenstra, jr. (1981). This algorithm for simultaneous diophantine approximation can be used to show the equivalence of the separation and optimization problems for non-full-dimensional rational polytopes, as it was announced in Section 1.

Let $b_1,\dots,b_m \in \mathbb{Q}^n$. The *lattice* generated by $b_1,\dots,b_m$ is

$$L = L(b_1,\dots,b_m) = \{\sum_{i=1}^{m} \lambda_i b_i,\ \lambda_i \in \mathbb{Z}\}.$$

If $b_1,\dots,b_m$ are linearly independent then $\{b_1,\dots,b_m\}$ is called a *basis* of L. Let us recall some simple facts concerning lattices.

2.1 FACT. Every lattice has a basis. Given $a_1,\dots,a_m \in \mathbb{Q}^n$ (not necessarily linearly independent) a basis for $L(a_1,\dots,a_m)$ can be found in polynomial time.

2.2 FACT. Let L be a lattice in $\mathbb{R}^n$ and $\{b_1,\dots,b_m\}$ a basis of L. Then

$$\det L = (\det(b_i^T b_j)_{i,j=1}^{m})^{1/2}$$

is independent of the choice of the basis.

2.4 FACT. Let $b_1,\dots,b_m$, $a \in \mathbb{Q}^n$. Then $a \in L(b_1,\dots,b_m)$ can be checked in polynomial time.

Lattices play a very important role in number theory. The theory of integral points, of course, is fundamental to combinatorics, but one can find many other lattices with relevant combinatorial contents, and

these are much less studied.

EXAMPLE. Let G be a bipartite graph, and $f_1,\dots,f_M$ the incidence vectors of its perfect matchings. Then

$$L(f_1,\dots,f_M) = \mathbb{Z}^{E(G)} \cap \{\sum_{i=1}^{M} \lambda_i f_i : \lambda_i \in Q\}$$

$$= \mathbb{Z}^{E(G)} \cap \{x \in Q^{E(G)} : x(\delta(v)) = 1 \ \forall v \in V(G)\}. \quad (I)$$

This provides a good characterization of this lattice. One can also find a basis of this lattice in polynomial time. Paul Seymour raised the problem of characterizing the lattice generated by the incidence vectors of perfect matchings of a non-bipartite graph.

Let L be a lattice, and define the *greedy system* $(b_1,\dots,b_m)$ as follows:

$$|b_1| = \min\{|b| : b \in L - \{0\}\}$$

$$|b_i| = \min\{|b| : b \in L,\ b_1,\dots,b_{i-1},b \text{ are linearly independent.}\}$$

Note that since the lattice may be viewed as a matroid, the greedy system minimizes objective functions, defined on linearly independent m-subsets of L, like $|b_1| \cdots |b_m|$, $|b_1|+\dots+|b_m|$, etc. However, this matroid is infinite, and so the above described procedure cannot be implemented efficiently. Furthermore, the greedy system may not be a basis for the lattice!

2.4 FACT. To find a greedy system for a lattice $L(a_1,\dots,a_k)$ is NP-hard.

2.5 FACT. To find $\min\{\|b\|_\infty : b = \in L - \{0\}\}$ is NP-had (Lagarias-Van Emde-Boas).

It is not known whether the problem of finding $\min\{|b| : b \in L - \{0\}\}$ is NP-hard, but we feel that quite likely it is. This lends more value to good bounds on this minimum. The following is a classical one.

2.6 THEOREM (Minkowski). Every lattice L in R^n has a basis $b_1,\dots,b_n$ such that

$$|b_1| \cdot \dots \cdot |b_n| \le \frac{2^n}{\nu_n} \cdot \det L,$$

where $\nu_n = \pi^{n/2}/\Gamma(\frac{n}{2}+1)$ is the volume of the unit ball in $\mathbb{R}^n$.

2.7 COROLLARY. Every lattice L in $\mathbb{R}^n$ contains a vector $b \neq 0$ with

$$|b| \le 2(\frac{\det L}{\nu_n})^{1/n}.$$

(For sharper results, see e.g. Lekkerkerker (1969).)

We now come to the main algorithm of this section. It will yield a basis of any given lattice which is "close" to the greedy basis in the sense that its vectors are at most 2^n times as long as the corresponding vectors of the greedy basis. To describe this algorithm we need some preparation.

Let $b_1,\dots,b_n$ be linearly independent vectors in $\mathbb{R}^n$. The *Gram–Schmidt orthogonalization* $(b_1^*,\dots,b_n^*)$ of the ordered basis $(b_1,\dots,b_n)$ is defined recurrently by

$$b_{i+2}^* = b_{i+1} - \sum_{j=1}^{i} \frac{b_{i+1}^T b_j^*}{|b_j^*|^2}\, b_j^* \quad (i = 0,1,\dots,n-1).$$

The notion of the Gram-Schmidt orthogonalization can be used to derive a lower bound on the shortest vector of a lattice.

2.8 LEMMA. If $b_1,\dots,b_n$ is a basis of the lattice L and $b_1^*,\dots,b_n^*$ is its Gram-Schmidt orthogonalization, then for every $b \in L$, $b \neq 0$,

$$|b| \geq \min(|b_1^*|, \dots, |b_n^*|).$$

(Note that $|b_1| \cdots |b_n| \geq |b_1^*| \cdots |b_n^*| = \det L$).

Let $b_1,\dots,b_n$ be a basis of the lattice L, and $b_1^*,\dots,b_n^*$ its Gram-Schmidt orthogonalization. Write

$$b_i = \sum_{j=1}^{i} \mu_{i,j} b_j^*. \quad (i = n,\dots,n).$$

We say that $(b_1,\dots,b_n)$ is *reduced* if

$$(a)\ |\mu_{ij}| \leq \frac{1}{2} \text{ for } 1 \leq j < i \leq n, \text{ and}$$

$$(b)\ |b_{i+1}^* + \mu_{i+1,i} b_i^*|^2 \geq \frac{3}{4} |b_i^*|^2 \text{ for } 1 \leq i \leq n-1.$$

(This mysterious condition (b) means geometrically that the sequence $(|b_1^*|^2, \dots, |b_n^*|^2)$ does not decrease "too much" lexicographically if b_i and b_{i+1} are interchanged.)

2.9 THEOREM. Let L be a lattice and $(b_1,\dots,b_n)$ a reduced basis of L. Then the following hold:

$$(a)\ |b_1| \leq 2^{\frac{n-1}{2}} \min\{|x| : x \in L,\ x \neq 0\}$$

$$(b)\ |b_1| \leq 2^{\frac{n-1}{4}} \sqrt[n]{\det L}$$

$$(c)\ |b_1| \cdots |b_n| \leq 2^{\frac{n(n-1)}{4}} \det L.$$

2.10 THEOREM. Let $a_1,\dots,a_n \in Q^n$ be linearly independent. Then we can find in polynomial time a reduced basis of the lattice $L(a_1,\dots,a_n)$.

The algorithm in Theorem 2.10 is quite straightforward from the definition of reducedness: if (a) is violated the subtract $(\mu_{ij})b_j$ from b_i (where (μ) is the integer nearest to μ), while if (b) is violated then interchange b_i and b_{i+1}. It takes a little effort to show that the running time of this algorithm is polynomial, in particular to show that the numbers involved do not grow too large.

Let us formulate some of the applications of this algorithm. First we quote a classical result due to Dirichlet.

2.11 THEOREM (Dirichlet). Let $\alpha_1, \dots, \alpha_n \in R^n$ and $\xi > 0$. Then there exist integers $p_1,\dots,p_n$ and q such that

$$|q\alpha_i - p_i| \le \xi \quad (i = 1,\dots,n)$$
$$0 < q \le \xi^{-n}.$$

Algorithmically, the following weaker result holds.

2.12 THEOREM. Let $\alpha_1, \dots, \alpha_n \in Q^n$ and $\xi \in Q$, $\xi > 0$. Then we can find in polynomial time integers $p_1,\dots,p_n$ and q such that

$$|q\alpha_i - p_i| \le \xi \quad (i = 1,\dots,n)$$
$$0 < q \le 2^{n^2}\xi^{-n}.$$

It is not known whether $p_1,\dots,p_n$ and q as in Dirichlet's theorem can be found in polynomial time.

A very nice combination of the Ellipsoid Method and basis reduction can be used to prove the following result of H.W. Lenstra, jr. (1981).

2.13 THEOREM (H.W. Lenstra). Let n be fixed. Given a convex body (K, n, r, R), by a separation oracle, we can decide in polynomial time if K contains an integral point, and find this point if it exists.

We sketch this algorithm. In its first phase we run an Ellipsoid Method to find a (rational) point in K. But in fact we use a version of the Ellipsoid Method, due to Yudin and Nemirowskii (1976) which finds a point x which is not only in K but "deep in K" in the following sense. The algorithm also yields an ellipsoid E with centre x including K (as all ellipsoid methods do) with the additional property that the ellipsoid E', homothetical with E with ratio $n^{-3/2}$ and with centre x, is contained in K. We do not go into the details of this version of the Ellipsoid Method, which we call the Shallow Cut Ellipsoid Method; but we remark that this application of it has also been found by Goffin

(1982).

We now apply a linear transformation L such that $\det L = 1$ and the ellipsoid E is mapped onto a ball $S(a, R)$. Then K is mapped onto a convex body LK which is nice in the sense that

$$S(a, n^{-3/2}R) \subseteq LK \subseteq S(a, R)$$

where $a = Lx$. Our task is equivalent to finding a point of the lattice LZ^n in the convex body LK. Unfortunately, the lattice LZ^n, or at least its basis $Le_1, \ldots, Le_n$, may be terrible. But, fortunately, we can apply the basis reduction algorithm and find in LZ^n a new basis $(b_1, \ldots, b_n)$ which has the properties stated in Theorem 2.9. Let β be the linear transformation which maps $(b_1, \ldots, b_n)$ onto $(e_1, \ldots, e_n)$, then βL is a linear transformation which maps Z^n onto itself (i.e. it is a linear transformation with integral entries and determinant 1). Of course, βLK is not as nice as LK. But let E_1 denote the ellipsoid with center $\beta\alpha$ whose axes are parallel to the coordinate axes and have length $\frac{n2}{|b_1|\frac{n(n-1)}{4}}, \ldots, \frac{n2}{|b_n|\frac{n(n-1)}{4}}$, respectively. Further, let E_1' denote the ellipsoid concentrical and homothetical with E_1 with ratio $2^{-\frac{n(n-1)}{4}} n^{-3}$ and with centre βa. Then

$$E_1' \subseteq \beta LK \subseteq E_1.$$

The crucial property of E_1 is that its axes are parallel to the coordinate axes. If all the axes of E_1' are longer than $\sqrt{n}$ then trivially, E_1' and hence $L\beta K$ contains an integer point (and this point can be found easily). If not, then at least one of the coordinates varies at most $2 \cdot 2^{\frac{n(n-1)}{4}} \cdot n^{7/2}$ and so our problem can be split into this number of lower dimensional problems. Thus we are done by induction.

Note that all but the last sentence can be carried out in time polynomial even for varying n. Thus in fact we have proved the following.

2.14 THEOREM. Given a convex body $(K; n, r.R)$ by a separation oracle, we can achieve in polynomial time one of the following:

(a) find an integral point in K;

(b) find an affine transformation x keeping $\mathbb{Z}^n$ invariant such that the first coordinate of any point in LK is less than $n^{7/2}2^{\frac{n(n-1)}{4}}$ in absolute value.

3. Combinatorial applications

In this section we survey some of the applications of the ellipsoid method to combinatorial problems. First we discuss some selected combinatorial problems. The following results are due to Ford and Fulkerson (1962), Edmonds (1967, 1973), Lucchesi and Younger (1978) and Edmonds and Johnson (1973).

Let G be a digraph and $s, t \in V(G)$. An $(s, t)-cut$ is the set of edges connecting a set $V \subseteq V(G) - t, s \in X$ to $V(G) - X$. A *cut rooted at s* is the set of edges connecting a set $X \subset V(G), s \in X$ to $V(G) - X$. *A directed cut* is the set of edges connecting a set $X \subset V(G)$, $X \neq \emptyset$ to $V(G) - X$, provided no edge connects $V(G) - X$ to X.

Let $T \subseteq V(G)$, $|T|$ even. Then a $T-cut$ is the set of edges of G connecting a set $V \subseteq V(G)$ with $|X \cap T|$ odd to $V(G) - X$.

A number of important graph-theoretic problems can be formulated as problems of packing and covering of various kinds of cuts. We formulate some of these, using polyhedral language. Let the *conical hull* of a set $S \subseteq \mathbb{R}^n$ be defined as the set

$$conv(S) + \mathbb{R}^n_+.$$

3.1 THEOREM

(a) The conical hull of (incidence vectors of) $(s-t)$-cuts is given by the inequalities

$$x \geq 0$$

$$x(P) \geq 1 \text{ for all } (s,t)-\text{paths } P.$$

(b) The conical hull of (s,t)-paths is given by the inequalities

$$x \geq 0$$

$$x(C) \geq 1 \text{ for all } (s,t)-\text{cuts } C.$$

3.2 THEOREM

(a) The conical hull of cuts rooted at r is given by the inequalities

$$x \geq 0$$

$$x(B) \geq 1 \text{ for all branchings}$$

(b) The conical hull of all branchings rooted at S is given by the inequalities

$$x \geq 0$$

$$x(C) \geq 1 \text{ for all cuts } C \text{ rooted at } s.$$

3.3 THEOREM

(a) The conical hull of all diconnecting sets is given by the inequalities

$$x \geq 0$$

$$x(C) \geq 1 \text{ for all directed cuts } C.$$

(b) The conical hull of all directed cuts is given by the inequalities

$$x \geq 0$$

$$x(D) \geq 1 \text{ for all diconnecting sets } D.$$

What lends combinatorial significance to these polyhedral results is that optimal dual solutions to linear optimization problems for them are integral and hence have combinatorial meaning.

3.4 THEOREM. The systems of inequalities in 3.1 - 3.3 (a) are totally dual integral, i.e. for any linear objective function with integral coefficients, the dual linear program has an integral solution.

It was shown by A. Schrijver (1980) that this does not remain valid for the system of inequalities in Theorem 3.3 (b).

3.5 THEOREM

(a) The conical hull of all T-joins is given by the inequalities

$$x \geq 0,$$

$$x(C) \geq 1 \text{ for all } T-\text{cuts } C.$$

(b) The conical hull of all T-cuts is given by the inequalities

$$x \geq 0$$

$$x(J) \geq 1 \text{ for all } T-\text{joins } J.$$

3.6 THEOREM. The system of linear inequalities in Theorem 3.5 (a) is totally dual half-integer.

A great many combinatorial optimization problems can be formulated as linear objective optimization problems over one of the above polyhedra: maximum flow, minimum cost flow, maximum weight

matching, minimum weight perfect matching, maximum and minimum weight branching, shortest odd st-path, shortest odd/even cycle, minimum feedback set in planar graphs, etc.

The following chart summarizes the algorithmic reductions among these problems. E means reduction by ellipsoid method, D means equivalence by LP duality, G means reduction by a greedy algorithm, and the unmarked arrows mean reductions by usually simple ad hoc tricks. The most involved is the reduction of minimum T-cuts to minimum cuts, which was recently discovered by Padberg and Rao (1982), and which is based on the Gomory-Hu flow-equivalent tree. The white box on the bottom means the "trivial problem".

Another class of combinatorial optimization problems to which the Ellipsoid Method can be applied successfully concerns matroids and submodular setfunctions. In contrast with the previous group of problems, where direct algorithms were known, here quite often the only known polynomial-time algorithm to solve them is the Ellipsoid Method.

Let us start with a quick survey of some polyhedral results on matroids. They are due to Edmonds (1970).

Let (S, r) be a matroid. Then the *matroid polyhedron* associated with (S, r) is the convex hull of independent sets in (S, r).

3.7 THEOREM. The matroid polyhedron associated with (S, r) is given by the linear inequalities

$$x \geq 0$$
$$x(T) \leq r(T) \quad (T \subseteq S).$$

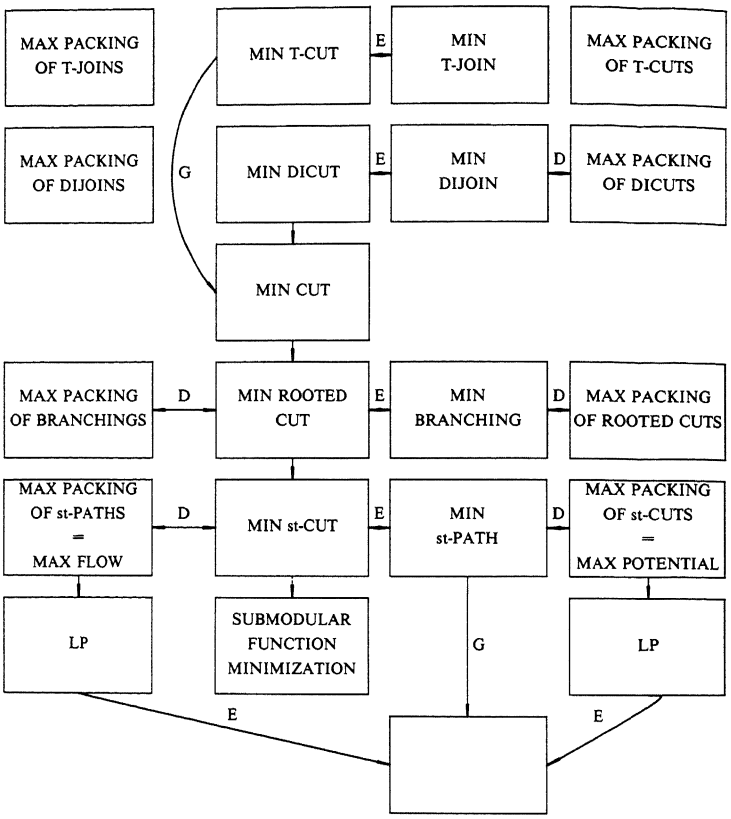
3.8 THEOREM. Let (S, r_1) and (S, r_2) be two matroids on the same underlying set S. Then the convex hull of common independent sets is given by the inequalities

$$x \geq 0$$
$$x(T) \leq \min(r_2(T), r_2(T)) \quad (T \subseteq X),$$

i.e. it is the intersection of the matroix polyhedra associated with the given matroids.

3.9 THEOREM. The systems of linear inequalities in Theorems 3.7 and 3.8 are total dual integral.

Let f be an integral valued submodular function on S. Then



the polymatroid defined by f is the polyhedron defined by the inequalities

$$x(T) \leq f(T) \quad (T \subseteq S).$$

3.10 THEOREM. Every polymatroid has integral vertices and the system of inequalities defining it is total dual integral.

3.11 THEOREM. The intersection of two polymatroids has integral vertices, and the union of the systems of linear inequalities defining these two polymatroids is total dual integral.

The most important algorithmic problem concerning a submodular setfunction is to find its minimum. This can be solved by the Ellipsoid Method; to find a combinatorial algorithm is an outstanding open problem.

Let f be a set function on S with $f(\emptyset) = 0$. Let $x \in R_+^S$. Write

$$x = \sum_{i=1}^{k} \lambda_i a_i, \qquad (*)$$

where $\lambda_i > 0$ and $a_1 \geq \ldots \geq a_k$ are (0-1) vectors. Define

$$\hat{f}(x) = \sum_{i=1}^{k} \lambda_i f(a_i).$$

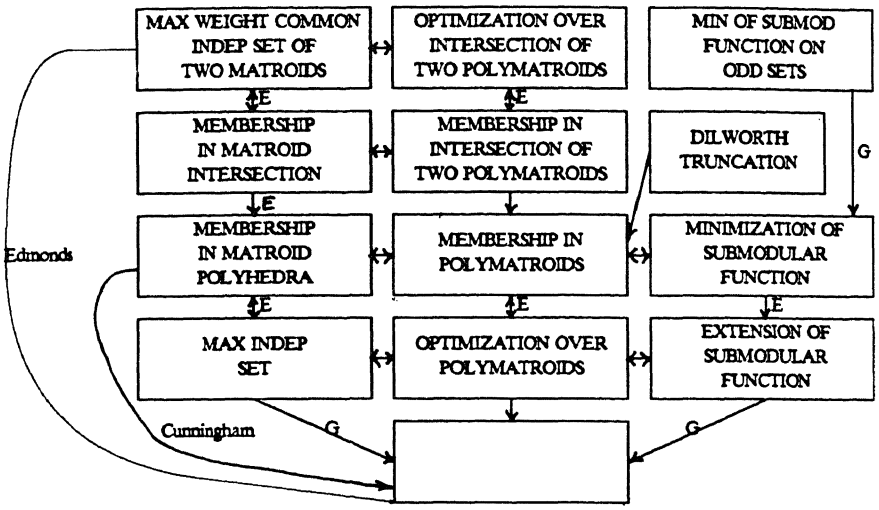
(The representation (*) is essentially unique, and hence f is well defined.)

3.12 LEMMA. $\hat{f}$ is convex iff f is submodular.

3.13 LEMMA. $\min\{f(T) : T \subseteq S\} = \min\{\hat{f}(x) : 0 \leq x \leq 1\}$.

Based on these lemmas, the minimization of a submodular setfunction is reduced to the minimization of a convex function over the unit cube, where the convex function can be evaluated at any given rational point in polynomial time. (We assume that the submodular function is given by an oracle which evaluates it at any given subset.) But the minimum of a convex function over such a nice domain can be found in polynomial time using the Ellipsoid Method (Yudin and Nemirowskii (1976)).

We can draw again a reducibility chart of these optimization problems.



References

[1959] E.W. Dijkstra, A note on two problems in connection with graphs, *Numer. Math.* 1 (1959), 269-271.

[1967] J. Edmonds, Optimum branchings, *J. Res. Nat. Bur. Standards Sect. B* 71 (1967), 233-240.

[1970] J. Edmonds, Submodular functions, matroids and certain polyhedra, in: Combinatorial Structures and their Applications, *Proc. Intern. Conf.* Calgary, Alb., 1969 (R. Guy, H. Hanani, N. Sauer and J. Schönheim eds.), Gordon and Breach, New York, 1970, 69-87.

[1973] J. Edmonds, Edge-disjoint branchings, in: Combinatorial algorithms, *Courant Comp. Sci. Symp.*, Monterey, Ca., 1972 (R. Rustin, ed.), Acad. Press, New York, 1973, 91-96.

[1979] J. Edmonds, Matroid intersection, *Annals of Discrete Math.* 4 (1979), 39-49.

[1973] J. Edmonds and E.L. Johnson, Matching, Euler tours and the Chinese postman, *Math. Programming* 5 (1973), 88-124.

[1982] J. Edmonds, L. Lovász and W. Pulleyblank, Brick decompositions and the matching rank of graphs, *Combinatorica* 2 (1982) 247-274.

[1962] L.R. Ford and D.R. Fulkerson, *Flows in networks*, Princeton Univ. Press, Princeton, N.J., 1962.

[1970] D.R. Fulkerson, Blocking polyhedra, in: *Graph Theory and its Applications, Proc. adv. Seminar*, Madison, Wis., 1969 (B. Harris, ed.), Acad. Press, New York, 1970, 93-112.

[1974] D.R. Fulkerson, Packing rooted directed cuts in a weighted directed graph, *Math. Programming* 6 (1974), 1-13.

[1982] J.-L. Goffin, Variable metric methods, part II: An implementable algorithm, or the Ellipsoid Method, preprint, McGill University, Montreal 82-27.

[1981] M. Grötschel, L. Lovász and A. Schrijver, The ellipsoid method and its consequences in combinatorial optimization, *Combinatorica* 1 (1981), 196-197.

[1981] M. Grötschel, L. Lovász and A. Schrijver, Polynomial algorithms for perfect graphs, Report No. 81176-OR, Universität Bonn, 1981.

[1981] I. Holyer, The NP-completeness of edge-colouring, *SIAM J. Comp.*, 10 (1981) 718-721.

[1980] R.M. Karp and C. Papadimitriou, On linear characterizations of combinatorial optimization problems, *Proc. 21st Ann. Symp. on Found. Comp. Sci.*, IEEE (1980) 1-9.

[1979] L.G. Khachiyan, A polynomial algorithm in linear programing, *Doklady Akademii Nauk SSSR* 244 (1979), 1093-1096 (English translation: Soviet Math. Dokl. 20, 191-194).

[1969] C.G. Lekkerkerker, Geometry of numbers, Wolters-Noordhoff, Groningen, North Holland, Amsterdam, 1969.

[1982] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Math. Annalen* 261 (1982) 515-534.

[1981] H.W. Lenstra, jr., Integer programming with a fixed number of variables, *Math. Oper. Res.* (to appear).

[1978] C.L. Lucchesi and D.H Younger, A minimax relation for directed graphs, *J. London Math. Soc.* (2) 17 (1978), 369-374.

[1982] M.W. Padberg and M.R. Rao, Minimum cut-sets and b-matchings, *Math. of Oper. Res.* 7 (1982) 67-80.

[1981] M.W. Padberg and M.R. Rao, The russian method for linear inequalities and linear optimization.

[1980] A. Schrijver, A counterexample to a conjecture of Edmonds and Giles, *Discrete Math.* 32 (1980), 213-214.

[1970] N.Z. Shor, Convergence rate of the gradient descent method with dilatation of the space, *Kibernetika 2* (1970), 80-85 (English translation: Cybernetics 6 (1970, 102-108).

[1976] D.B. Yudin and A.S. Nemirowskii, Informational complexity and effective methods of solution for convex extremal problems, *Ekonomika i Mat. Metody* 12 (1976), 357-369 (English translation: Matekon: Transl. of Russian and East European Math. Economics 13 (1976), 24-25).