On the Ellipsoid Method

Emil Klafszky
Dept. of Building Management
Techn. Univ. Budapest
1111. Budapest
Müegyetem rkp. 3.
HUNGARY

Tamás Terlaky
Dept. of O.R.
Eötvös University
1088.Budapest
Muzeum krt.6-8.
HUNGARY

Abstract

A complete version of an ellipsoid method for solving linear programming problems is presented in this paper. Simple, easy to understand elementary proofs are given for key theorems.

A new constant is used for measuring the "size" of the problem.

Key words: ellipsoid method, linear programming, polynomial algorithm.

1 Introduction

A short, easy to understand version of the ellipsoid method is presented in this paper. Our aim was to give simple elementary proofs for key theorems, where a new constant was used for measuring the size of the problem. We do not improve theoretical bounds, and even do not claim that this version of the ellipsoid method is practically efficient.

The structure of this paper is as follows: First lower and upper bounds are presented for the volume (size) of polyhedrons defined by integer vectors. Then properties of m-dimensional ellipsoids, and minimal ellipsoids containing a half ellipsoid are discussed. A version of the ellipsoid method is presented in the fourth chapter and it is proved that this ellipsoid method decides in polynomial time, that a linear inequality system is consistent or not. Finally a polynomial procedure is presented, which generates a solution for linear inequality systems by calling repeatedly the above ellipsoid method (or any such algorithm, which only decides consistency of linear inequality systems .)

It is well known already for a long time, that in spite of its practical efficiency the simplex method is not a polynomial algorithm for solving linear programming problems (LP). First Klee and Minty [5] presented a tricky example on which simplex method is exponential. By modifying Klee's and Minty's polyhedron it is proved that almost all known versions of the simplex method are exponential.

First, in 1979 Khachian [4] gave a polynomial time algorithm for solving LP. Khachian's algorithm is known as ellipsoid method, since it is based on subsequent shrinking the volume of ellipsoids. In spite of its theoretical efficiency it turned out quickly that the ellipsoid method (any existing version) is practically inefficient for solving LP.

The second mile stone in the field of polynomial algorithms was Karmarkar's [3] projective method, which gave a better theoretical bound, and the practical efficiency of variants of this method for large problems is also better.

Our considerations are mainly based on the ideas presented in Gács' and Lovász' [2] and Khachian's [4] paper and Schrijver's [6] book, but a new constant is used for measuring the size of problems.

Matrices will be denoted by capital latin, vectors by small latin letters and scalars will be denoted by Greek letters. So an $m \times n$ matrix will be denoted by A, which has vectors $a^{(1)}, \ldots, a^{(m)}$ as its row vectors and vectors $a_1, \ldots, a_n$ as its column vectors, furthermore α_{ij} denotes its element in row i and column j.

2 Lower-and upper bounds

In this chapter lower (inner) and upper (outer) bounds are given for the volume of polyhedrons defined by integer vectors. The product of the norms of these vectors will be used to measure the "size" of the problem. This is different from the commonly used constant L, the "binary length of data".

Let $A : m \times n$ be an integer matrix and $c \in R^n$ an integer vector (i.e. α_{ij} and γ_j are integers for all i, j). Without restricting generality, we may assume that $rank(A) = m$.

Definition 1 *The number* $\sigma = |a^{(1)}| \times \ldots \times |a^{(i)}| \times \ldots \times |a^{(m)}| \times |c|$ *is called the size of the parameters where* $|a^{(i)}|$ *denotes the Euclidean norm of vector* $a^{(i)}$*.*

Let us consider the alternative problem pair:

$$A^T y \leq c \qquad \text{and} \qquad \begin{aligned} Ax &= 0 \\ cx &= -1 \\ x &\geq 0. \end{aligned}$$

It is well known [1] that one and only one of the above problems is consistent. The next lemma shoves, that if any of the two above problems has a solution, then it has a solution in the "σ cube", that is all the coordinates of the solution vector is less than or equal σ.

Lemma 1 *1. If* $A^T y \leq c$ *is consistent, then* $A^T y \leq c; \quad |\eta_i| \leq \sigma$ *for all index* i *is consistent. (Any basic solution has this property.)*

2. If $Ax = 0,\ cx = -1,\ x \geq 0$ *is consistent, then* $Ax = 0,\ cx = -1,\ x \geq 0,\ \xi_j \leq \sigma$ *for all* j *is consistent. (Any basic solution has this property.)*

Proof:

1. Helly's theorem implies that if the problem $A^T y \leq c$ is consistent then there is a base B and basic solution y, such that $B^T y = c_B$, $N^T y \leq c_N$ (here $A = (B, N)$ and $c = (c_B, c_N)$ respectively). Denote $b^{(i)}$ the i-th row of matrix B , then by Cramer rule we have:

$$\eta_i = \frac{det(B - b^{(i)}, c_B)}{det(B)}$$

The numerator can be estimated from above by Hadamard inequality, the denominator can be estimated from below by Leibniz expansion, so

$$|\eta_i| \leq \frac{|b^{(1)}| \times \ldots \times |b^{(m)}| \times |c_B|}{1}$$

The right hand side is obviously less than or equal to σ, so claim 1. is proved.

2. If the problem is consistent, then by Charatheodory theorem it has a basic solution $\overline{x} = (\overline{x}_B, 0)$ with a base $\overline{B}$, where $\overline{B} = \begin{pmatrix} B \\ c_B \end{pmatrix}$ a matrix of size $(m+1) \times (m+1)$, $\overline{x}_B \in R_+^{m+1}$; $\overline{B}\overline{x}_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\overline{x}_B \geq 0$. Using again Cramer's rule we have

$$\xi_j = \frac{det\left(\overline{B} - \overline{a}_j, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)}{det(B)}.$$

As in part 1. using Hadamar's inequality and Leibnitz expansion we have

$$|\xi_j| \leq \frac{|b_1| \times \ldots \times |b_{m+1}| \times 1}{1} \leq \sigma.$$

Our proof is complete. $\square$

The above results and Farkas' theorem implies the following theorem.

Theorem 1 *If $A^T y \leq c$ is inconsistent, then $A^T y \leq c + \frac{1}{mn\sigma} e$ is inconsistent. (here $e = (1, \ldots, 1)$).*

Proof:
If $A^T y \leq c$ is inconsistent, then the Farkas theorem says that the system

$$Ax = 0, \quad cx = -1, \quad x \geq 0$$

is consistent, which by claim 2. implies that

$$Ax = 0, \quad cx = -1, \quad x \geq 0, \quad \xi_j \leq \sigma \text{ for all } j.$$

is consistent. This has the following equivalent form:

$$Ex + Eu = \sigma e, \quad Ax = 0, \quad cx = -1, \quad x \geq 0, \quad u \geq 0$$

This problem is consistent, so the Farkas theorem implies that

$$\begin{aligned} Ez + A^T y + \vartheta c &\leq 0 \\ z &\leq 0 \\ \sigma z^T e &> 0 \end{aligned}$$

is inconstant. Then by choosing $\vartheta = -1$ and $z = \; - \frac{1}{mn\sigma} \; e$, the resulted system

$$A^T y \leq c + \frac{1}{mn\sigma} e$$

is inconsistent again since the third and second assumptions are fulfilled by this choice.
$\square$

Corollary 1 *Inequality system $A^T y \leq c$ is consistent if and only if the inequality system*

$$\begin{aligned} A^T y &\leq c + \frac{1}{mn\sigma} e \\ |\eta_i| &\leq \sigma + \frac{1}{mn\sigma} \quad \textit{for all } i \end{aligned}$$

is consistent.

Proof:
By claim 1. of Lemma 1, if $A^Ty \le c$ is consistent then the system $A^Ty \le c$, $|\eta_i| \le \sigma$ for all i, is consistent, which obviously implies that $A^Ty \le c + \frac{1}{mn\sigma}e$, $|\eta_i| \le \sigma + \frac{1}{mn\sigma}$ for all i, is consistent.

On the other hand, if $A^Ty \le c$ is inconsistent, then by Theorem 1 $A^Ty \le c + \frac{1}{mn\sigma}e$ is inconsistent as well. Which implies the inconsistency of the desired inequality system. $\square$

Corollary 2 *If the inequality system*

$$\begin{aligned} A^Ty &\le c + \frac{1}{mn\sigma}e \\ |\eta_i| &\le \sigma + \frac{1}{m^2n\sigma^2} \quad \textit{for all } i \end{aligned}$$

is consistent, then the set of solutions contains a cube with edge length $\frac{1}{m^2n\sigma}$.

Proof:
Using Corollary 1 we know that $A^Ty \le c$ is consistent. Let $\overline{y}$ be a solution of this inequality system. Let $\epsilon = (\epsilon_1, \ldots, \epsilon_m)$ be a binary vector, i.e. $\epsilon_i \in \{0,1\}$ for all i. Denote $y = \overline{y} + \frac{1}{m^2n\sigma^2}\epsilon$. ($y$ is a vertex of the cube in question.) It is enough to show that

$$A^Ty \le c + \frac{1}{mn\sigma}e \quad \text{and} \quad |\eta_i| \le \sigma + \frac{1}{m^2n\sigma^2} \text{ for all } i.$$

The last inequalities obviously holds, so one have to show that $A^Ty \le c + \frac{1}{mn\sigma}e$. We have $A^Ty = A^T\overline{y} + \frac{1}{m^2n\sigma^2}A^T\epsilon \le c + \frac{1}{m^2n\sigma^2}A^T\epsilon$, so we have to show that $A^T\epsilon \le m\sigma e$.

Obviously $A^T\epsilon = \epsilon_1 a^{(1)} + \ldots + \epsilon_m a^{(m)}$ and using the inequality $x \le |x|e$ which trivially holds for integer vectors we have

$$A^T\epsilon \le e|A^T\epsilon| = e|\epsilon_1 a^{(1)} + \ldots + \epsilon_m a^{(m)}| \le e\sum_{i=1}^m \epsilon_i |a^{(i)}| \le e\sum_{i=1}^m |a^{(i)}| \le e\sum_{i=1}^m \prod_{j=1}^m |a^{(j)}| \le m\sigma e.$$

The proof is complete. $\square$

In this section such polyhedron was constructed for polyhedrons that is empty if and only if the original polyhedron is empty, and the new polyhedron contains a "small" cube, which guarantees that its volume is strictly positive.

3 Ellipsoids

Ellipsoids, and an ellipsoid transformation are examined in this section. It will be shown that the transformed ellipsoid contains a suitable half ellipsoid of the original ellipsoid and its volume is less than the volume of the original ellipsoid. In fact the ratio of the volumes of the two ellipsoids can be estimated by a fixed number, which is less than one.

Definition 2 *If $P : m \times m$ is a positive semidefinite matrix, and $z \in R^m$ then the set*

$$E = ell(z, P) = \{x \in R^m | (x - z)^T P^{-1} (x - z)\}$$

is called **ellipsoid**.

Vector z is referees as the *center* of the ellipsoid. It is well known, that the set $\{x | a^T (x - z) \leq 0\}$ is the halfspace, which boundary contains point z and the normal vector of this halfspace is vector a.

Definition 3 *Let an ellipsoid $E = ell(z, P)$ and a vector $a \in R^m$ be given. Let $E' = ell(z', P')$ be given as follows:*

$$\begin{aligned} z' &= z - \frac{1}{m+1} \frac{Pa}{\sqrt{a^T P a}} \\ P' &= \frac{m^2}{m^2 - 1} \left(P - \frac{2}{m+1} \frac{P a a^T P}{a^T P a} \right). \end{aligned}$$

Now we will verify that E' is really an ellipsoid and it contains the half ellipsoid $E \cap \{x | a^T (x - z) \leq 0\}$.

Lemma 2 *Matrix P' is positive semidefinite.*

Proof:
One have to show, that

$$x^T P x - \frac{2}{m+1} \frac{x^T P a a^T P x}{a^T P a} \geq 0$$

for all $x \in R^m$. Since $m \geq 1$,it is enough to show that

$$(x^T P x)(a^T P a) \geq (x^T P a)(a^T P x).$$

Matrix P is positive semidefinite so by Cholesky factorization there is a matrix S with $P = S^T S$. So the above inequality is

$$(Sx)^2 (Sa)^2 \geq ((Sx)(Sa))^2$$

which is the Cauchy-Swartz-Bunyakowski inequality. □

Lemma 3 *Ellipsoid E' contains the half ellipsoid of E defined by vector a, that is*

$$E \cap \left\{ x | a^T (x - z) \leq 0 \right\} \subseteq E'.$$

Proof:
Let x be a point of the right hand side, that is $a^T(x-z) \leq 0$ and $(x-z)^T P^{-1}(x-z) \leq 1$. One have to show that it is a point of E. It is easy to check that

$$P'^{-1} = \frac{m^2-1}{m^2}\left(P^{-1} + \frac{2}{m-1}\frac{aa^T}{a^TPa}\right),$$

i . e .

$$\left(P - \frac{2}{m-1}\frac{Paa^TP}{a^TPa}\right)\left(P^{-1} + \frac{2}{m-1}\frac{aa^T}{a^TPa}\right) =$$

$$E + \left(-\frac{2}{m+1} + \frac{2}{m-1} + \frac{4}{m^2-1}\right)\frac{Paa^T}{a^TPa} = E.$$

So one have to show that

$$\left(x - z + \frac{1}{m+1} + \frac{Pa}{\sqrt{a^TPa}}\right)^T \frac{m^2-1}{m^2}\left(P^{-1} + \frac{2}{m-1}\frac{aa^T}{a^TPa}\right)$$
$$\left(x - z + \frac{1}{m+1} + \frac{Pa}{\sqrt{a^TPa}}\right) \leq 1.$$

hold for all x which is in the half ellipsoid. Denote $\alpha = \sqrt{a^TPa}$ and $\beta = a^T(x-z)$. Then

$$\left((x-z)^T + \frac{1}{\alpha(m+1)}a^TP\right)^T\left(\frac{m^2-1}{m^2}P^{-1} + \frac{2(m+1)}{m^2\alpha^2}aa^T\right)\left((x-z) + \frac{Pa}{(m+1)\alpha}\right) =$$

$$\frac{m^2-1}{m^2}(x-z)^TP^{-1}(x-z) + 2\frac{m^2-1}{m^2}\frac{1}{(m+1)\alpha}(x-z)^TP^{-1}Pa + \frac{m^2-1}{m^2}\frac{a^TPP^{-1}Pa}{(m+1)^2\alpha^2} +$$
$$\frac{2(m+1)}{m^2\alpha^2}(x-z)^Taa^T(x-z) + 2\frac{2(m+1)}{m^2\alpha^2}\frac{1}{(m+1)\alpha}(x-z)^Taa^TPa +$$
$$\frac{1}{(m+1)^2\alpha^2}\frac{2(m+1)}{m^2\alpha^2}a^TPaa^TPa \leq$$

$$\frac{m^2-1}{m^2} + 2\frac{m-1}{m^2}\frac{\beta}{\alpha} + \frac{m-1}{m^2(m+1)} + \frac{2(m+1)}{m^2}\frac{\beta^2}{\alpha^2} + \frac{4}{m^2}\frac{\beta}{\alpha} + \frac{2}{m^2(m+1)} =$$

Since $\beta \leq 0$, so our task is only to show that $\alpha + \beta \geq 0$ i. e.

$$\sqrt{a^TPa} + a^T(x-z) \geq 0.$$

We know, that $|S^{-1}(x-z)|^2 = (x-z)^TP^{-1}(x-z) \leq 1$, so using Cauchy-Swarz-Bunyakowski inequality we have

$$-\beta = -a^T(x-z) = (-a^TS)(S^{-1}(x-z)) \leq |Sa||S^{-1}(x-z) \leq \alpha 1 \leq 1,$$

which completes the proof. $\square$

Finally in this section it is proved that the volume of E' is less than the volume of E. It is well known that the ratio of the volumes of ellipsoids is equal to the square root of the ratio of the determinants of the corresponding positive semidefinite matrices.

Lemma 4 $\frac{vol(E')}{vol(E)} < \exp\left(\frac{-1}{2(m+1)}\right)$

Proof:
As it was mentioned above

$$\frac{vol(E')}{vol(E)} = \sqrt{\frac{det(P')}{det(P)}}.$$

It is well known from linear algebra, that for any nonsingular square matrix B, vector b and number α the, equality $det(B + \alpha bb^T) = (1 + \alpha b^T B^{-1} b) det(B)$ holds. So

$$det(P') = \left(\frac{m^2}{m^2-1}\right)^m \left(1 - \frac{2}{(m+1)a^T Pa} a^T PP^{-1}Pa\right) det(P) =$$

$$\left(\frac{m^2}{m^2-1}\right)^m \left(1 - \frac{2}{m+1}\right) det(P) = \left(1 + \frac{1}{m^2-1}\right)^{m-1} \left(\frac{1}{m+1}\right)^2 det(P) =$$

$$\left(1 + \frac{1}{m^2-1}\right)^{m-1} \left(1 - \frac{1}{m+1}\right)^2 det(P).$$

Using the inequality $1 + x < exp(x)$ we have

$$det(P') < exp\left(\frac{m-1}{m^2-1}\right) exp\left(\frac{-2}{m+1}\right) det(P) = exp\left(\frac{-1}{m+1}\right) det(P).$$

So

$$\frac{vol(E')}{vol(E)} < \sqrt{\frac{exp\left(\frac{-1}{m+1}\right) det(P)}{det(P)}} = exp\left(\frac{-1}{2(m+1)}\right).$$

$\square$

Remark, that E' is the minimal ellipsoid that contains the half ellipsoid. We do not need this fact in the ellipsoid method, so to prove this is left to the reader.

4 The ellipsoid method

Here the ellipsoid method is presented which decides if a linear inequality system $A^T y \leq c$ is consistent or not.

Algorithm:

Initialization: Let a matrix $A : m \times n$ and a vector $c \in R^n$ be given. Let us compute σ and let $E_0 = ell(z_0, P_0) = ell(0, 2\sigma E)$ be the globe with radius 2σ, the initial ellipsoid.

Termination:
– If z_k satisfies $A^T z_k \leq c + \frac{1}{mn\sigma} e$, then STOP, inequality system $A^T y \leq c$ is consistent.
– If $k = N > 2m(m+l)\log(4\sigma^3 m^2 n)$, then STOP, the inequality system is inconsistent.

General step:
– If z does not satisfies $A^T z_k \leq c + \frac{1}{mn\sigma} e$, then there is an index j for which

$$a_j^T z_k \leq \gamma_j + \frac{1}{mn\sigma}$$

According to definition 2.2. let $a := a_j,\ z_{k+1} = z',\ P_{k+1} = P'$ and $k = k+1$.

As it was proved (Corollary 2) inequality system $A^T y \leq c$ is consistent if and only if $A^T y \leq c + \frac{1}{mn\sigma} e$ is consistent. So we have to show that in case of $k = N$ the inequality system is really inconsistent.

Theorem 2 *Inequality system $A^T y \leq c$ is inconsistent if the above algorithm takes more then $2m(m+l)\log(4\sigma^3 m^2 n)$ steps .*

Proof:
By means of Corollary 2 enough to show that inequality system $A^T y \leq c + \frac{1}{mn\sigma} e$, $|\eta_i| \leq \sigma + \frac{1}{m^2 n \sigma^2}$ for all i is inconsistent in this case. Corollary 2 says that its solution set contains a cube with edge length $\frac{1}{m^2 n \sigma^2}$ if it is not empty. The volume of this cube is $\left(\frac{1}{m^2 n \sigma^2}\right)^m$.

Lemma 3 implies that this cube is contained in all of the ellipsoids generated by the Algorithms, and the volume of the actual ellipsoid after N steps can be estimated by Lemma 4 as follows:

$$vol(E_N) < \exp\left(\frac{-N}{2(m+1)}\right) vol(E_0) < \exp\left(\frac{-N}{2(m+1)}\right)(4\sigma)^m.$$

If this value is less than $\left(\frac{1}{m^2 n \sigma^2}\right)^m$, that is the volume of the ellipsoid is less than the volume of the contained cube, then we have a contradiction, that is the inequality system is inconsistent.

$$\exp\left(\frac{-N}{2(m+1)}\right)(4\sigma)^m < \left(\frac{1}{m^2 n \sigma^2}\right)^m$$

which holds if

$$N \; > \; 2m(m+1)\log(4m^2n\sigma^3).$$

The proof is complete. $\square$

Since the number of steps of the algorithms can be bounded by a polynomial, so this is a *polynomial time algorithm*. This way a polynomial time algorithm was constructed in this section which decides whether inequality system $A^Ty \leq c$ is consistent or not. Unfortunately our algorithm gives a solution only for inequality system $A^Ty \leq c + \frac{1}{mn\sigma}e$, and the solution of this system is not necessarily a solution for system $A^Ty \leq c$.
In the next chapter a polynomial procedure is presented for generating a solution of the original inequality system. This procedure subsequently calls the algorithm of this chapter.

5 Find a solution

Using a polynomial time algorithm (as a black box), which decides whether an inequality system is consistent or not, and Gaussian elimination, a solution of inequality system $A^Ty \leq c$ can be find in polynomial time.

Theorem 3 *If we have an algorithm (e.g. ellipsoid method) which decides the consistency of a linear inequality system, then a solution can be found in polynomial time.*

Proof:
By calling at most m times the algorithm and solving an equation system by Gaussian elimination a solution can be obtained.
Perform the following algorithm.

Algorithm

Step 0. Decide that inequality system

$$a_1^Ty \leq \gamma_1, \; \ldots, \; a_n^Ty \leq \gamma_n$$

is consistent or not. If it is inconsistent STOP.

Step 1. If it is consistent then decide that inequality system

$$a_1^Ty = \gamma_1, \; a_2^Ty \leq \gamma_2, \; \ldots, \; a_n^Ty \leq \gamma_n$$

is consistent or not. If not, then it is enough to solve inequality system $a_2^Ty \leq \gamma_2, \; \ldots, \; a_n^Ty \leq \gamma_n$ since in this case for all solution of this system $a_1^Ty < \gamma_1$ holds. Let $n := n-1$ and return to the previous step.

Step 2. If it is consistent then decide that inequality system

$$a_1^T y = \gamma_1, \;\; a_2^T y = \gamma_2, \;\; a_3^T y \le \gamma_3, \;\; \ldots, \;\; a_n^T y \le \gamma_n$$

is consistent or not. ...

Step k. If it is consistent then decide that inequality system

$$a_1^T y = \gamma_1, \;\; \ldots, \;\; a_k^T y = \gamma_k, \;\; a_{k+1}^T y \le \gamma_{k+1}, \;\; \ldots, \;\; a_n^T y \le \gamma_n$$

is consistent or not. If not, then it is enough to solve inequality system $a_1^T y = \gamma_1, \; \ldots, \; a_{k-1}^T y = \gamma_{k-1}, \; a_{k+1}^T y \le \gamma_{k+1}, \; \ldots, \; a_n^T y \le \gamma_n$ since for all solution of this system $a_k^T y < \gamma_k$ holds. Let $n := n - 1$ and return to the previous step.

Step k+1. If it is consistent then decide that inequality system

$$a_1^T y = \gamma_1, \;\; \ldots, \;\; a_k^T y = \gamma_k, \;\; a_{k+1}^T y = \gamma_{k+1}, \;\; a_{k+2}^T y \le \gamma_{k+2}, \;\; \ldots, \;\; a_n^T y \le \gamma_n$$

is consistent or not. ...

This algorithm finds a solution in polynomial time for inequality system $A^T y \le c$, since in the last step an equation system is to be solved, that can be done by Gaussian elimination. □

Finally, remark again that the presented ellipsoid method is not the sharpest version of the ellipsoid method. Our aim was to present the main ideas, and present such a simple, complete version of the ellipsoid method which can be part of a university course. Furthermore using constant σ for measuring the size of the problem is new.

References

[1] Dantzig G.B., "Linear Programming and extensions", Princeton University Press, Princeton, N.J., 1963.

[2] Gács P., and Lovász L., "Khachians algorithm for linear programming", Mathematical Programming Study 14, (1981) 61-68.

[3] Karmarkar N., "A new polynomial time algorithm for linear programming", Combinatorica 4, (1984) 373-395.

[4] Khachian L.G., " A polynomial algorithm for linear programming", Doklady Akad. Nauk USSR 244, (1979) 1093 - 1096.

[5] Klee V. and Minty G.J., "How good is the simplex algorithm?'; in Inequalities III. (O. Shisha, ed.) Academic Press, New York, (1972) 159-175.

[6] Schrijver A., "Theory of Linear and Integer Programming", John Wiley and Sons, 1986.