KHACHIAN'S ALGORITHM FOR LINEAR PROGRAMMING

by

Peter Gács and Laszlo Lovász

STAN-CS-79-750
July 1979

DEPARTMENT OF COMPUTER SCIENCE
School of Humanities and Sciences
STANFORD UNIVERSITY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER STAN-CS-79-750	2. GOVT ACCESSION NO.
4. TITLE (and Subtitle) Khachian's Algorithm for Linear Programming	5. TYPE OF REPORT & PERIOD COVERED technical, July 1979
	6. PERFORMING ORG. REPORT NUMBER STAN-CS-79-750
7. AUTHOR(s) Peter Gács and Laszlo Lovász	8. CONTRACT OR GRANT NUMBER(s) [illegible]
9. PERFORMING ORGANIZATION NAME AND ADDRESS Department of Computer Science Stanford University Stanford, California 94305 USA	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Office of Naval Research Department of the Navy Arlington, Va 22217	12. REPORT DATE July 1979
	13. NUMBER OF PAGES 12
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) ONR Representative - Philip Surra Durand Aeromautics Building, Room 165 Stanford University Stanford, Ca. 94305	15. SECURITY CLASS. (of this report) Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Releasable without limitations on dissemination.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

(see reverse side)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCL[illegible]

SECURITY CLASSIFIC[illegible]

L. G. Khachian's algorithm to check the solvability of a system of linear inequalities with integral coefficients is described. The running time of the algorithm is polynomial in the number of digits of the coefficients. It can be applied to solve linear programs in polynomial time.

Khachian's Algorithm for Linear Programming

Peter Gács and Laszlo Lovász

Computer Science Department
Stanford University
Stanford, California 94305

Abstract.

L. G. Khachian's algorithm to check the solvability of a system of linear inequalities with integral coefficients is described. The running time of the algorithm is polynomial in the number of digits of the coefficients. It can be applied to solve linear programs in polynomial time.

This research was supported in part by National Science Foundation grant MCS-77-23738 and by Office of Naval Research contract N00014-76-C-0330. Reproduction in whole or in part is permitted for any purpose of the United States government.

L. G. Khachian [Doklady Akademii Nauk SSSR, 1979, Vol. 244, No. 5, 1093-1096] published a polynomial-bounded algorithm to solve linear programming. These are some notes on this paper. We have ignored his considerations which concern the precision of real computations, in order to make the underlying idea clearer, on the other hand, proofs which are missing from his paper are given in an appendix.

Let

$$(1) \qquad a_i x < b_i \qquad (i = 1, \ldots, m, \quad a_i \in Z^n, \quad b_i \in Z)$$

be a system of strict linear inequalities with integral coefficients. We present an algorithm which decides whether or not (1) is solvable, and yields a solution if it is.

Define

$$L = \sum_{i,j} \log(|a_{ij}| + 1) + \sum_i \log(|b_i| + 1) + \log nm + 1$$

L is the space needed to state the problem.

The Algorithm.

We define a sequence $x_0, x_1, \ldots \in R^n$ and a sequence of symmetric positive definite matrices $A_0, A_1, \ldots$ recursively as follows. $x_0 = 0$, $A_0 = 2^L I$. Assume that (x_k, A_k) is defined. Check if x_k is a solution of (1). If it is, stop. If not, pick any inequality in (1) which is violated:

$$a_i x_k \geq b_i ,$$

and set

$$x_{k+1} = x_k - \frac{1}{n+1} \frac{A_k a_i}{\sqrt{a_i^T A_k a_i}} ,$$

$$A_{k+1} = \frac{n^2}{n^2-1} \left(A_k - \frac{2}{n+1} \frac{(A_k a_i)\cdot(A_k a_i)^T}{a_i^T A_k a_i} \right) .$$

(Note that the multiplication of vector $A_k a_i$ with itself in the second term results in an $n \times n$ matrix.)

In practice, we will compute only certain approximations of x_k and A_k by decimals of a certain precision. It can be shown that approximations within $\exp(-10nL)$ preserve the validity of the following theorem.

Theorem. If the algorithm stops, x_k is a solution of (1). If the algorithm does not stop in $6n^2L$ steps, then (1) is not solvable.

The first assertion is, of course, just a repetition of the stopping rule for the algorithm. To prove the crucial second statement, we shall need a series of lemmas, along with a geometric description of what's happening.

Let $x_0 \in R^n$ and A a positive definite matrix. Then

$$(x-x_0)^T A^{-1} (x-x_0) \leq 1$$

defines an ellipsoid $E = (x,A)$ with center x . Let $a \in R^n$, $a \neq 0$. Then we shall denote by E^a the ellipsoid (x_0', A') , where

$$x_0' = x_0 - \frac{1}{n+1} A \frac{a}{\sqrt{a^T A a}} ,$$

$$A' = \frac{n^2}{n^2-1}\left(A - \frac{2}{n+1}\ \frac{(Aa)(Aa)^T}{a^TAa}\right) \quad .$$

We shall denote the semi-ellipsoid

$$E \cap \{x:\ (x-x_0)a \leq 0\}$$

by $\frac{1}{2} E_a$.

Let us remark (although this is not needed in the proof) that geometrically this construction means the following. Take a hyperplane $ax = d$, $d < ax_0$, which is tangent to E at point y . Then

$$x_0 - y = A \frac{a}{\sqrt{a^TAa}} \quad .$$

Now E^a will be the (unique) ellipsoid which touches the hyperplane $ax = d$ at y and intersects the hyperplane $ax = ax_0$ in the same ellipsoid as E .

So here come the lemmas. The first three are facts of number-theoretic nature which probably are familiar to many people who have investigated the complexity of algorithmic problems in linear algebra. We use the notation $|x|_\infty = \max_i x_i$, $|x|_2 = \sqrt{\sum_i x_i^2}$.

<u>Lemma 1</u>. Every vertex v of the polyhedron

$$a_i x \leq b_i \qquad (i = 1,\ldots,m)$$

$$x \geq 0$$

satisfies $|v|_\infty < 2^L/n$, and its entries are rational numbers with denominator at most 2^L .

<u>Lemma 2</u>. If (1) has a solution, then the volume of its solutions inside the cube $|x_i| \leq 2^L$ is at least 2^{-nL} .

Lemma 3. Suppose that the system

$$a_i x \; < \; b_i + 2^{-L} \qquad (i = 1,\dots,m)$$

has a solution. Then

$$a_i x \; \le \; b_i \qquad (i = 1,\dots,m)$$

has a solution.

Lemma 4. $\frac{1}{2} E_a \subset E^a$.

Lemma 5. $\lambda(E^a) \; = \; c(n)\lambda(E)$,

where

$$c(n) \; = \; \left(\frac{n^2}{n^2-1} \right)^{(n-1)/2} \frac{n}{n+1} \; < \; e^{-(1/2(n+1))} .$$

and $\lambda(X)$ is the volume of the set X .

The proof of the theorem is quite easy now. Suppose that the procedure does not stop after $k = 6n^2L$ steps, and yet (1) is solvable. Then by Lemma 2, the set P of its solutions x inside E_0 has $\lambda(P) \ge 2^{-nL}$. By Lemma 4, $P \subset E_k$. But by Lemma 5,

$$\lambda(E_k) \; < \; e^{-(k/2(n+1))} \lambda(E_0) \; < \; e^{-(k/2(n+1))} 2^{2Ln} \; < \; 2^{-nL} ,$$

a contradiction.

If one would like to decide the solvability of a system of the form

(2) $$a_i x \; \le \; b_i \qquad (i = 1,\dots,n)$$

then we may consider instead the system

(3) $$\lceil 2^L \rceil a_i x \; < \; \lceil 2^L \rceil b_i + 1 \qquad (i = 1,\dots,n) .$$

By Lemma 3, this is solvable iff (2) is solvable.

If we want to solve a linear programming problem

$$\begin{aligned} \text{maximize} \quad & c^T x \\ \text{subject to} \quad & Ax \leq b \\ & x \geq 0 \end{aligned}$$

then consider the system of inequalities

$$\begin{aligned} c^T x &= b^T y \\ Ax &\leq b \\ x &\geq 0 \\ A^T y &\geq c \\ y &\geq 0 \; . \end{aligned}$$

This is solvable iff the original program has a feasible solution and a finite optimum, and for any solution (x, y) of this system, x is an optimal solution of the program.

Appendix

Proof of Lemma 1. Let $v = (v_1,\ldots,v_n)$. By Cramer's rule, each v_i can be expressed as

$$v_i = D_i/D ,$$

where D_i and D are determinants whose entries are 0, 1, a_{ij} or b_i. Hence D and D_i are integers, and

$$|D| \geq 1 ,$$

$$|D| \leq \prod \text{(norms of row vectors)}$$

$$< 2^L/nm < 2^L/n ,$$

and the same holds for the D_i's. This implies the assertion.

Proof of Lemma 2. We may assume that (1) has a solution $x_0 > 0$. So the polyhedron

$$(4) \qquad \begin{aligned} a_i x &\leq b_i \qquad (i = 1,\ldots,m) \\ x &\geq 0 \end{aligned}$$

has an interior point. Since it contains no line, it also has a vertex $v = (v_1,\ldots,v_n)$. By Lemma 1, we know that $v_i < 2^L/n < \lfloor 2^L \rfloor$. It follows that the polyhedron (4) has an interior point $x = (x_1,\ldots,x_n)$ with $x_j < \lfloor 2^L \rfloor$, and so the polytope

$$(5) \qquad \begin{cases} a_i x \leq b_i & (i = 1,\ldots,m) \\ x \geq 0 & \\ x_j \leq \lfloor 2^L \rfloor & (j = 1,\ldots,n) \end{cases}$$

has an interior point. Hence, it has $n+1$ vertices $v_0,\ldots,v_n$ which are not on a hyperplane. So (5) has volume at least

$$\frac{1}{n!}\det\begin{pmatrix} 1 & 1 & & 1 \\ & & \cdots & \\ v_0 & v_1 & & v_n \end{pmatrix} .$$

Here, by Lemma 1, we get that

$$v_i = \frac{1}{D_i} u_i ,$$

where u_i is an integer vector and D_i is an integer $< 2^L/n$. So

$$\det\begin{pmatrix} 1 & \cdots & 1 \\ v_1 & \cdots & v_n \end{pmatrix} = \frac{1}{|D_1| \cdots |D_n|} \det\begin{pmatrix} D_1 & \cdots & D_n \\ u_1 & \cdots & u_n \end{pmatrix}$$

$$\geq \frac{1}{|D_1| \cdots |D_n|} \geq 2^{-nL} \cdot n^n$$

since the determinant in the second expression is a non-zero integer. So the volume of the polytope (5) is at least $\frac{1}{n!} 2^{-nL} n^n > 2^{-nL}$.

Proof of Lemma 3. For $x \in R^n$, set

$$\theta_i(x) = a_i x - b_i .$$

Let $x_0 \in R^n$ be arbitrary.

Claim 1. There exists an $x_1 \in R^n$ such that

(1) $\theta_i(x_1) \leq \max(0, \theta_i(x_0))$ $(i = 1,\ldots,m)$

and

(2) The vectors $\{a_i: \theta_i(x_1) \geq 0\}$ span every other vector a_i .

To prove the claim, it suffices to show that if x_0 does not satisfy (2) then we can find a vector x_1 such that x_1 satisfies (1) and $\theta_i(x_1) \geq 0$ holds, for more indices i than $\theta_i(x_0) \geq 0$. Repeating this at most m times we must obtain an x_1 satisfying both (1) and (2).

Let, say $\theta_1(x_0),\ldots,\theta_k(x_0) \geq 0$, $\theta_{k+1}(x_0),\ldots,\theta_m(x_0) < 0$. Suppose that a_ν $(\nu > k)$ is not a linear combination of $a_1,\ldots,a_k$. Then the system of linear equations

$$\begin{aligned} a_i y &= 0 \qquad (i = 1,\ldots,k) \\ a_\nu y &= 1 \end{aligned}$$

is solvable. Let y_0 be a solution and consider

$$x_1 = x_0 + ty_0 \ ,$$

where

$$t = \max\{s \in R: sa_j y_0 + \theta_j \leq 0 \ (j = k+1,\ldots,m)\}$$

t is finite, in fact $t \leq -\theta_\nu$.

Then by the choice of t,

$$\theta_i(x_1) = ta_i y_0 + \theta_i(x_0) \begin{cases} = \theta_i(x_0) & \text{if } 1 \leq i \leq k \ , \\ \leq 0 & \text{if } k+1 \leq i \leq m \ , \end{cases}$$

and equality holds for at least one $1 \leq i \leq m$. This proves the Claim.

Assume now that x_0 is such that

$$a_i x_0 < b_i + 2^{-L} \qquad (i = 1,\ldots,m) \ .$$

Let, say $a_i x_0 \geq b_i$ for $i = 1,\ldots,k$. Choose the labelling so that $a_1,\ldots,a_r$ are linearly independent but $a_{r+1},\ldots,a_k$ are spanned by them. By the Claim, we may assume that $a_{k+1},\ldots,a_n$ are also spanned by $a_1,\ldots,a_r$.

Now let z be a solution of the system of linear equations

$$a_i z = b_i \quad (i = 1, \dots, r) .$$

We show that z satisfies

$$a_i z \le b_i$$

for every $1 \le i \le m$. We know that

$$a_i = \sum_{j=1}^{r} \lambda_j a_j$$

with some real numbers λ_j. In fact by Cramer's rule we also know that

$$\lambda_j = D_j / D ,$$

where D_j and D are determinants formed by some entries of the vectors a_i and hence they are integers with absolute value less than $2^L/n$. Now

$$D(a_i z - b_i) = \sum_{j=1}^{r} D_j a_j z - D b_i$$
$$= \sum_{j=1}^{r} D_j b_j - D b_i .$$

To estimate the right hand side, use that

$$\sum_{j=1}^{r} D_j b_j - D b_i = \sum_{j=1}^{r} D_j (a_j x_0 - \theta_j(x_0)) - D(a_i x_0 - \theta(x_0))$$
$$= D \cdot \theta_i(x_0) - \sum_{j=1}^{r} D_j \theta_j(x_0)$$
$$\le D \cdot 2^{-L} + \sum_{j=1}^{r} |D_j| 2^{-L} < 1 ,$$

and since the left hand side is an integer,

$$\sum_{j=1}^{r} D_j b_j - D b_i \le 0 ,$$

which proves the assertion.

Proof of Lemma 4. We may assume that $x_0 = 0$, $A = I$ (i.e., the ellipsoid is the unit sphere about 0) and that $a = (-1,0,\dots,0)^T$, since the contents of the lemma is invariant under affine transformations of the space.

Then

$$x_0' = \left(\frac{1}{n+1}, 0, \dots, 0 \right)^T$$

and

$$A' = \operatorname{diag} \left(\frac{n^2}{(n+1)^2}, \frac{n^2}{n^2-1}, \dots, \frac{n^2}{n^2-1} \right) .$$

Suppose $x \in \frac{1}{2} E_a$. Then $|x|_2 \le 1$, $1 \ge \xi_1 = -a^T x \ge 0$. We have to show that

$$(x-x_0')^T A'^{-1} (x-x_0') \le 1 .$$

But

$$\begin{aligned}(x-x_0')^T A'^{-1}(x-x_0') &= x^T A'^{-1} x - 2x^T A'^{-1} x_0' + x_0'^T A'^{-1} x_0' \\ &= \frac{n^2-1}{n^2} x^2 + \frac{2n+2}{n^2} \xi_1^2 - 2 \frac{n+1}{n^2} \xi_1 + \frac{1}{n^2} \\ &= \frac{n^2-1}{n^2} (x^2-1) + \frac{2n+2}{n^2} \xi_1(\xi_1-1) + 1 \le 1 .\end{aligned}$$

Proof of Lemma 5. We may assume again that E is the unit sphere about 0 and $a = (1,0,\dots,0)^T$, since affine transformations do not change the proportion of volumes. By a well-known formula,

$$\lambda(E^a) = \frac{\sqrt{\det A'}}{\sqrt{\det A}} \cdot \lambda(E) = \sqrt{\det A'}\, \lambda(E)$$

$$= \frac{n}{n+1} \left(\frac{n^2}{n^2-1} \right)^{(n-1)/2} \cdot \lambda(E) = c(n) \cdot \lambda(E) .$$

To estimate this factor use that

$$\frac{n^2}{n^2-1} = 1 + \frac{1}{n^2-1} < e^{1/(n^2-1)}$$

and

$$\frac{n}{n+1} = 1 - \frac{1}{n+1} < e^{-1/(n+1)} \quad .$$

Substituting these bounds we get

$$c(n) < e^{-1/(2(n+1))} \quad .$$