JOURNAL OF ALGORITHMS 1, 1–13 (1980)

Khachiyan's Linear Programming Algorithm*

BENGT ASPVALL

Computer Science Department, Stanford University, Stanford, California 94305

AND

RICHARD E. STONE

Department of Operations Research, Stanford University, Stanford, California 94305

Received December 7, 1979

L. G. Khachiyan's polynomial time algorithm for determining whether a system of linear inequalities is satisfiable is presented together with a proof of its validity. The algorithm can be used to solve linear programs in polynomial time.

1. INTRODUCTION

Leonid Genrikhovich Khachiyan (Хачиян) published in *Doklady Akademiia Nauk SSSR* **244**:5 (1979) a polynomial time algorithm for solving the linear programming problem, in this paper henceforth denoted the LP problem. We present a simplified version of his algorithm together with a proof of its validity. No proof was given in Khachiyan's paper, and the proof presented here is based on the one by Gács and Lovász [1].

To determine the complexity of the LP problem was one of the foremost open problems in theoretical computer science. Although the LP problem did not seem to be NP-hard, no algorithm with subexponential worst-case behavior was known before Khachiyan's. (For further discussion of classes P and NP see, e.g., [2]).

In the next section we present a polynomial time algorithm for determining whether a system of strict linear inequalities, $A\mathbf{x} < \mathbf{b}$, with integer coefficients is satisfiable. The two key facts exploited are: (a) Strict inequalities are used; (b) A and $\mathbf{b}$ have integer coefficients. Fact (a) implies that a nonempty feasible region must be an open set, and so has positive

*This work was supported by National Science Foundation Grant MCS-77-23738, and by a National Science Foundation Fellowship.

0196-6774/80/010001–13$02.00/0

volume. Fact (b) adds a certain "discreteness" to the problem; many points in the feasible region that we wish to look at are not arbitrary points in $\mathbf{R}^n$, but have entries that are rational numbers with bounded denominators. Also, any two constraints in $A\mathbf{x} < \mathbf{b}$ that are not parallel hyperplanes have their "slopes" bounded away from each other. Hence we will show that if the feasible region is not empty, then there exists a set S in the feasible region, of some given volume, such that S is within some given distance of the origin.

The algorithm starts with a sphere centered at the origin and with radius large enough that it contains S. The general procedure then assumes that we currently have an ellipsoid containing S. If the center of the ellipsoid is infeasible, then a hyperplane parallel to a violated constraint and going through the center is used to cut the ellipsoid in half. One half will be completely infeasible, and we surround the other half with a smaller ellipsoid and repeat the procedure. Eventually, if we do not find a solution to $A\mathbf{x} < \mathbf{b}$, we end up with an ellipsoid, which is assumed to contain S, but whose volume is less than the volume of S. This contradiction implies an empty feasible region.

The algorithm is a simplified version of Khachiyan's algorithm, and can be used to solve the LP problem as described in Section 3. Section 4 is devoted to the complexity analysis. Since Khachiyan has been unknown to the computer science community, we include some of his previous works in the reference list. We also include references to two papers by Shor [8, 9], since Khachiyan's algorithm is based on N. Z. Shor's method of ellipsoids.

2. Systems of Strict Linear Inequalities

In this section we present an algorithm for determining whether a system of strict linear inequalities is satisfiable. The algorithm is constructive in that it supplies a feasible vector if one exists. Let

$$a_{i1}x_1 + \cdots + a_{in}x_n < b_i, \qquad i = 1, \ldots, m, m \geq 2, n \geq 2, \tag{2.1}$$

be a system of strict inequalities with integer coefficients. In the worst case the algorithm requires $O(n^3(m + n)L)$ arithmetic operations ($+$, $-$, $\times$, $/$, and $\sqrt{\ }$), where

$$L = \sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \lceil \log_2(|a_{ij}| + 1) \rceil + \sum_{1 \leq i \leq m} \lceil \log_2(|b_i| + 1) \rceil + \lceil \log_2 mn \rceil + 1 \tag{2.2}$$

is the length of the binary encoding of a given instance of (2.1).

We will use $A\mathbf{x} < \mathbf{b}$, where $A \in \mathbf{Z}^{m\times n}$ and $\mathbf{b} \in \mathbf{Z}^m$, as an alternative representation of (2.1); to refer to a single inequality of (2.1) we will often use the notation $\mathbf{a}_i^T\mathbf{x} < b_i$, where $\mathbf{0} \neq \mathbf{a}_i \in \mathbf{Z}^n$ and $b_i \in \mathbf{Z}$. (All vectors are assumed to be column vectors.)

ALGORITHM 1 (Khachiyan's algorithm).

Step 1. [Initialize.] Set $\mathbf{x}^{(0)} \leftarrow \mathbf{0}$, $B^{(0)} \leftarrow 2^{2L}I$, and $k \leftarrow 0$.

Step 2. [Terminate?] If $\mathbf{x}^{(k)}$ is a solution to (2.1), then terminate the algorithm and return $\mathbf{x}^{(k)}$ as a feasible solution. If $k < 4(n+1)^2L$, then go to Step 3. Otherwise, terminate the algorithm, responding that no solution exists.

Step 3. [Next iteration.] Select any inequality in (2.1) that is violated at $\mathbf{x}^{(k)}$, e.g. $\mathbf{a}_i^T\mathbf{x}^{(k)} \geq b_i$, and set

$$\mathbf{x}^{(k+1)} \leftarrow \mathbf{x}^{(k)} - \frac{1}{n+1}\frac{B^{(k)}\mathbf{a}_i}{\sqrt{\mathbf{a}_i^T B^{(k)}\mathbf{a}_i}} \tag{2.3}$$

and

$$B^{(k+1)} \leftarrow \frac{n^2}{n^2-1}\left[B^{(k)} - \frac{2}{n+1}\frac{\left(B^{(k)}\mathbf{a}_i\right)\left(B^{(k)}\mathbf{a}_i\right)^T}{\mathbf{a}_i^T B^{(k)}\mathbf{a}_i}\right]. \tag{2.4}$$

Set $k \leftarrow k+1$ and go to Step 2. □

Clearly, if Algorithm 1 returns a feasible vector $\mathbf{x}^{(k)}$, then (2.1) is satisfiable. The hard part is to show that the algorithm always finds a solution if one exists. Given a point $\mathbf{x}'$ and a symmetric positive definite matrix B, the set

$$E = \left\{\mathbf{x} \mid (\mathbf{x}-\mathbf{x}')^T B^{-1}(\mathbf{x}-\mathbf{x}') \leq 1\right\} \tag{2.5}$$

defines an ellipsoid with center $\mathbf{x}'$. Let $\frac{1}{2}E_a$ denote the semiellipsoid

$$\tfrac{1}{2}E_a = E \cap \left\{\mathbf{x} \mid \mathbf{a}^T(\mathbf{x}-\mathbf{x}') \leq 0\right\}, \tag{2.6}$$

and let E' be the set $\{\mathbf{y} \mid (\mathbf{y}-\mathbf{y}')^T B'^{-1}(\mathbf{y}-\mathbf{y}') \leq 1\}$, where

$$\mathbf{y}' = \mathbf{x}' - \frac{1}{n+1}\frac{B\mathbf{a}}{\sqrt{\mathbf{a}^T B\mathbf{a}}} \tag{2.7}$$

and

$$B' = \frac{n^2}{n^2-1}\left(B - \frac{2}{n+1}\frac{(B\mathbf{a})(B\mathbf{a})^T}{\mathbf{a}^T B\mathbf{a}}\right). \tag{2.8}$$

We will show that E' is an ellipsoid with center $\mathbf{y}'$, that $\frac{1}{2}E_a \subseteq E'$, and that $\lambda(E')$, the volume of E', is less than $\lambda(E)$.

LEMMA 1. *Every vertex* $\mathbf{v}$ *of the polyhedron*

$$\begin{aligned} A\mathbf{x} &\le \mathbf{b}, \\ \mathbf{x} &\ge \mathbf{0} \end{aligned}$$

satisfies $\|\mathbf{v}\|_\infty < 2^L/mn$. *Furthermore, its coordinates are rational numbers with denominators less than* $2^L/mn$ *in absolute value.*

Proof. Let D be the determinant of the basis matrix associated with some vertex $\mathbf{v} = (v_1, \ldots, v_n)$ of the polyhedron. From Cramer's rule, we know that each v_k is either zero or can be expressed as D_k/D, where $D, D_k \neq 0$ are determinants of matrices with entries from $\{0, 1, a_{ij}, b_i\}$; hence D and D_k are integers. Note that an element a_{ij} can only occur once in the matrix associated with D and once in the matrix associated with D_k; a similar situation holds for an element b_i. Let $\mathbf{d}_j$, for $1 \le j \le m$, be the column vectors of the matrix associated with D. Either the elements of a column vector $\mathbf{d}_j$ are all from $\{a_{ij}, b_i\}, j \in J \subseteq \{1, \ldots, m\}$, or $\mathbf{d}_j$ is a unit vector, $j \notin J$, where the latter alternative comes from the inequalities $x_i \ge 0$. Thus

$$|D| \le \prod_{1 \le j \le m} \|\mathbf{d}_j\|_2 \le \prod_{j \in J} \prod_{1 \le i \le m} (|d_{ij}| + 1) \le 2^{(L - \log_2 mn - 1)}$$

(the first step follows as $|D|$ is the volume of the hyperparallelepiped spanned by its column vectors), and we have $|D| < 2^L/mn$; the same bound holds also for $|D_k|$. □

COROLLARY 1. *Every vertex* $\mathbf{v}$ *of the polytope*

$$\begin{aligned} A\mathbf{x} &\le \mathbf{b}, \\ \mathbf{x} &\ge \mathbf{0}, \\ \mathbf{x} &\le \lfloor 2^L/n \rfloor \mathbf{e}, \end{aligned}$$

where $\mathbf{e} = (1, \ldots, 1)^T$, *has coordinates that are rational numbers with denominators less than* $2^L/mn$ *in absolute value.*

Proof. As in the proof of Lemma 1, either v_k is zero or v_k can be expressed as D_k/D, where $|D| \le \prod_{j \in J} \|\mathbf{d}_j\|_2$. But now $\mathbf{d}_j$ is a column from the matrix $(A^T, I)^T$ instead of from the matrix A. Let $\mathbf{d}'_i$, for $1 \le i \le m + n$, be the rows of the matrix whose columns are $\mathbf{d}_j$, $j \in J$. Then $|D| \le \prod_{1 \le i \le m+n} \|\mathbf{d}'_i\|_2 = \prod_{1 \le i \le m} \|\mathbf{d}'_i\|_2 < 2^L/mn$. □

LEMMA 2. *If* (2.1) *has a solution, then the volume of its solution space inside the sphere* $\|\mathbf{x}\|_2 \le 2^L$ *is at least* $2^{-(n+1)L}$.

Proof. Without loss of generality, we may assume that (2.1) has a solution in the positive orthant so that the polyhedron

$$\begin{aligned} A\mathbf{x} &\le \mathbf{b}, \\ \mathbf{x} &\ge \mathbf{0} \end{aligned} \tag{2.9}$$

has an interior point. Since the polyhedron contains no line extending infinitely in both directions, it has also a vertex $\mathbf{v}$. From Lemma 1, we know that $\|\mathbf{v}\|_\infty < \lfloor 2^L/n \rfloor$. Thus (2.9) has an interior point $\mathbf{x}^*$ with $\|\mathbf{x}^*\|_\infty < \lfloor 2^L/n \rfloor$, and hence so has the polytope

$$\begin{aligned} A\mathbf{x} &\le \mathbf{b}, \\ \mathbf{x} &\ge \mathbf{0}, \\ \mathbf{x} &\le \lfloor 2^L/n \rfloor \mathbf{e}. \end{aligned} \tag{2.10}$$

The polytope (2.10) must therefore have $n + 1$ vertices $\mathbf{v}_0, \ldots, \mathbf{v}_n$ that are not on a hyperplane, and its volume is at least

$$\frac{1}{n!}\left|\det\begin{pmatrix} 1 & \cdots & 1 \\ \mathbf{v}_0 & \cdots & \mathbf{v}_n \end{pmatrix}\right| > 0,$$

which is the volume of the simplex with $\mathbf{v}_0, \ldots, \mathbf{v}_n$ as vertices. From Corollary 1, we know that for some integer vector $\mathbf{u}_i$, the vector $\mathbf{v}_i$ can be expressed as $\mathbf{v}_i = (1/D_i)\mathbf{u}_i$, where $|D_i| < 2^L/n$ is an integer. Thus

$$\begin{aligned} \left|\det\begin{pmatrix} 1 & \cdots & 1 \\ \mathbf{v}_0 & \cdots & \mathbf{v}_n \end{pmatrix}\right| &= \frac{1}{|D_0| \cdots |D_n|}\left|\det\begin{pmatrix} D_0 & \cdots & D_n \\ \mathbf{u}_0 & \cdots & \mathbf{u}_n \end{pmatrix}\right| \\ &\ge \frac{1}{|D_0| \cdots |D_n|} > \left(\frac{2^L}{n}\right)^{-(n+1)}, \end{aligned}$$

where the second step follows from the fact that the determinants are nonzero integers. Thus the volume of the polytope (2.10) is at least $(2^L/n)^{-(n+1)}/n! > 2^{-(n+1)L}$. □

The contents of the following three lemmas are invariant under affine transformations. We will therefore assume that $\mathbf{x}' = \mathbf{0}$, $B = I$, and $\mathbf{a} = (-1, 0, \ldots, 0)^T$ in the proofs of the lemmas; i.e., the ellipsoid E is the unit sphere at the origin, and the intersecting half-space is $x_1 \ge 0$. Then

$$\mathbf{y}' = \left(\frac{1}{n+1}, 0, \ldots, 0\right)^T \tag{2.11}$$

and

$$B' = \operatorname{diag}\left(\frac{n^2}{(n+1)^2}, \frac{n^2}{n^2-1}, \ldots, \frac{n^2}{n^2-1}\right). \tag{2.12}$$

To help clarify why Lemmas 3, 4, and 5 are invariant under affine transforms, we show the following:

PROPOSITION 1. *Let B be an $n \times n$, symmetric, positive definite matrix, let $\mathbf{a} \neq \mathbf{0}$ and $\mathbf{x}'$ be n-vectors, and let α, β, and $\gamma < 1$ be positive constants. Define*

$$E = \{\mathbf{x} | \mathbf{x}^T\mathbf{x} \leq 1\},$$

$$\bar{E} = \{\mathbf{x} | (\mathbf{x} - \mathbf{x}')^T B^{-1}(\mathbf{x} - \mathbf{x}') \leq 1\}.$$

Let $\mathbf{v} = (-1, 0, \ldots, 0)^T$, and define

$$E' = \{\mathbf{x} | (\mathbf{x} + \alpha\mathbf{v})^T \beta (I - \gamma(\mathbf{v}\mathbf{v}^T))^{-1}(\mathbf{x} + \alpha\mathbf{v}) \leq 1\},$$

$$\bar{E}' = \left\{\mathbf{x} \middle| \left(\mathbf{x} - \mathbf{x}' + \alpha \frac{B\mathbf{a}}{\sqrt{\mathbf{a}^T B\mathbf{a}}}\right)^T \beta \left(B - \gamma \frac{(B\mathbf{a})(B\mathbf{a})^T}{\mathbf{a}^T B\mathbf{a}}\right)^{-1} \right.$$
$$\left. \times \left(\mathbf{x} - \mathbf{x}' + \alpha \frac{B\mathbf{a}}{\sqrt{\mathbf{a}^T B\mathbf{a}}}\right) \leq 1\right\}.$$

Then the affine transformation sending E to $\bar{E}$ also sends E' to $\bar{E}'$.

Proof. As B is a symmetric positive definite matrix, there exists a Cholesky factorization $B = LL^T$ of B, where L is a nonsingular matrix. Now we can select an orthogonal (rotation) matrix Q so that $\mathbf{v} = Q^T L^T \mathbf{a} / \|Q^T L^T \mathbf{a}\|_2$. (Note that $\|Q^T L^T \mathbf{a}\|_2^2 = \mathbf{a}^T L Q Q^T L^T \mathbf{a} = \mathbf{a}^T L L^T \mathbf{a} = \mathbf{a}^T B\mathbf{a}$.) Thus $T(\mathbf{x}) = \mathbf{x}' + LQ\mathbf{x}$ defines an invertible affine transformation, with $T^{-1}(\mathbf{x}) = Q^T L^{-1}(\mathbf{x} - \mathbf{x}')$. Hence

$$\begin{aligned} T(E) &= \{\mathbf{x} | (T^{-1}(\mathbf{x}))^T T^{-1}(\mathbf{x}) \leq 1\} \\ &= \{\mathbf{x} | (\mathbf{x} - \mathbf{x}')^T L^{T-1} Q Q^T L^{-1}(\mathbf{x} - \mathbf{x}') \leq 1\} \\ &= \{\mathbf{x} | (\mathbf{x} - \mathbf{x}')^T B^{-1}(\mathbf{x} - \mathbf{x}') \leq 1\} = \bar{E}. \end{aligned}$$

In the same way one shows that $T(E') = \bar{E}'$. □

We now see that the formulas of the algorithm express in a general affine system the sphere E and the derived ellipsoid E'. This is completely general as any ellipsoid with positive volume can be expressed as an invertible affine transform of the unit sphere. Since the relations "B' is positive definite" and "$\frac{1}{2}E_a \subseteq E'$" are invariant under affine transformations, as is the ratio $\lambda(E')/\lambda(E)$, we lose no generality by working with $\mathbf{x}' = \mathbf{0}$, $B = I$, and $\mathbf{a} = (-1, 0, \ldots, 0)^T$.

LEMMA 3. *If the matrix B is symmetric and positive definite, so is the matrix B' (i.e., the set E' defines an ellipsoid).*

Proof. Clearly, B' is symmetric, so we want to show that $\mathbf{x}^T B'\mathbf{x} > 0$ for all $\mathbf{x} \neq \mathbf{0}$. We have

$$\mathbf{x}^T B'\mathbf{x} = \frac{n^2}{(n+1)^2} x_1^2 + \frac{n^2}{n^2-1}\left(\|\mathbf{x}\|_2^2 - x_1^2\right) = \frac{n^2}{n^2-1}\left(\|\mathbf{x}\|_2^2 - \frac{2}{n+1} x_1^2\right),$$

and since either $0 = x_1^2 = \|\mathbf{x}\|_2^2$ or $(2/(n+1))x_1^2 < x_1^2 \leq \|\mathbf{x}\|_2^2$ for $n \geq 2$, the lemma follows. □

LEMMA 4. *The semiellipsoid $\frac{1}{2}E_a$ is completely contained in the ellipsoid E'.*

Proof. If $\mathbf{y}$ is any point in $\frac{1}{2}E_a$, then $\|\mathbf{y}\|_2 \leq 1$ and $0 \leq -\mathbf{a}^T\mathbf{y} = y_1 \leq 1$. We want to show that $\mathbf{y} \in E'$, i.e.,

$$(\mathbf{y} - \mathbf{y}')^T B'^{-1}(\mathbf{y} - \mathbf{y}') \leq 1.$$

Expanding the left-hand side, we get

$$\begin{aligned}(\mathbf{y} - \mathbf{y}')^T B'^{-1}(\mathbf{y} - \mathbf{y}') &= \mathbf{y}^T B'^{-1}\mathbf{y} - 2\mathbf{y}^T B'^{-1}\mathbf{y}' + \mathbf{y}'^T B'^{-1}\mathbf{y}' \\ &= \frac{n^2-1}{n^2}\|\mathbf{y}\|_2^2 + 2\frac{n+1}{n^2} y_1^2 - 2\frac{n+1}{n^2} y_1 + \frac{1}{n^2} \\ &= \frac{n^2-1}{n^2}\left(\|\mathbf{y}\|_2^2 - 1\right) + 2\frac{n+1}{n^2} y_1(y_1 - 1) + 1 \leq 1.\end{aligned}$$

□

Note that in the proof of Lemma 4, we have $(\mathbf{y} - \mathbf{y}')^T B'^{-1}(\mathbf{y} - \mathbf{y}') = 1$ if and only if $\|\mathbf{y}\|_2 = 1$ and either $y_1 = 0$ or $y_1 = 1$. We give a geometrical interpretation of E'. Take a hyperplane $\mathbf{a}^T\mathbf{x} = d$, where $d < \mathbf{a}^T\mathbf{x}'$, which is tangent to E at the point $\mathbf{x}'' = \mathbf{x}' - B\mathbf{a}/\sqrt{\mathbf{a}^T B\mathbf{a}}$. Then the ellipsoid E' is the unique ellipsoid of minimum n-dimensional volume that intersects the hyperplane $\mathbf{a}^T(\mathbf{x} - \mathbf{x}') = 0$ in the same ellipsoid (of dimension $n-1$) as E and is tangent to the hyperplane $\mathbf{a}^T\mathbf{x} = d$ at $\mathbf{x}''$.

LEMMA 5. *The volumes of the two ellipsoids E' and E satisfy $\lambda(E') = c(n)\lambda(E)$, where*

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

Proof. Again we assume that $B = I$, so that B' is given by (2.12). Following the ideas of Proposition 1, we have $E' = T(E)$, where $T(\mathbf{x}) = \mathbf{x}'$

$+ L\mathbf{x}$ and $B' = LL^T$. Thus from linear algebra we know that $\lambda(E') = \det L \times \lambda(E)$ and hence

$$\lambda(E') = \sqrt{\det B'}\,\lambda(E) = \frac{n}{n+1}\left(\frac{n^2}{n^2-1}\right)^{(n-1)/2}\lambda(E) = c(n)\lambda(E).$$

From the Taylor expansion of the exponential, we have

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

and

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

Thus

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

THEOREM 1. *Algorithm* 1 *returns a feasible vector* $\mathbf{x}^{(k)}$ *if and only if* (2.1) *is satisfiable.*

Proof. The "only if" part of the theorem is trivially true, so suppose Algorithm 1 terminates without having found a solution although (2.1) has a solution. Then by Lemma 2, the set S of solutions inside $E^{(0)}$ has volume $\lambda(S) \geq 2^{-(n+1)L}$. Furthermore, the set S is a subset of $E^{(l)}$, where $l = 4(n+1)^2L$. This follows, since the inequality $\mathbf{a}_i^T\mathbf{x} < b_i$, chosen during the kth iteration of the algorithm, is violated at the point $\mathbf{x}^{(k)}$, so $\mathbf{a}_i^T\mathbf{x} < b_i \leq \mathbf{a}_i^T\mathbf{x}^{(k)}$. Thus S is contained in the set $\{\mathbf{x}|\mathbf{a}_i^T(\mathbf{x} - \mathbf{x}^{(k)}) \leq 0\}$, and we conclude that

$$S \subseteq E^{(k)} \cap \left\{\mathbf{x}|\mathbf{a}_i^T(\mathbf{x} - \mathbf{x}^{(k)}) \leq 0\right\} \subseteq E^{(k+1)}, \qquad 0 \leq k < l = 4(n+1)^2L,$$

where the second step follows from Lemma 4. Together with Lemma 5, this implies that

$$\lambda(S) \leq \lambda(E^{(l)}) < 2^{-l/(2(n+1))}\lambda(E^{(0)}) < 2^{-2(n+1)L}(2 \times 2^L)^n < 2^{-(n+1)L}$$

(the last step follows since $n < L$); but this is a contradiction, and the theorem is proved. $\square$

3. LINEAR PROGRAMMING

From the previous section we know how to determine, in polynomial time, whether a system of strict inequalities has a solution. In this section we show how to use this result to solve the linear programming problem in polynomial time.

From the duality theorem of the linear programming problem, the *primal* program

$$\max_{\mathbf{x}} \mathbf{c}^T\mathbf{x}$$
$$\text{subject to } \begin{cases} A\mathbf{x} \le \mathbf{b} \\ \mathbf{x} \ge \mathbf{0} \end{cases} \tag{3.1}$$

has a *dual* version

$$\min_{\mathbf{y}} \mathbf{b}^T\mathbf{y}$$
$$\text{subject to } \begin{cases} A^T\mathbf{y} \ge \mathbf{c} \\ \mathbf{y} \ge \mathbf{0} \end{cases} \tag{3.2}$$

such that $\max_{\mathbf{x}} \mathbf{c}^T\mathbf{x} = \min_{\mathbf{y}} \mathbf{b}^T\mathbf{y}$ if and only if (3.1) has a finite optimum. It follows that the system of inequalities

$$\begin{aligned} \mathbf{c}^T\mathbf{x} &\ge \mathbf{b}^T\mathbf{y}, \\ A\mathbf{x} &\le \mathbf{b}, \\ \mathbf{x} &\ge \mathbf{0}, \\ A^T\mathbf{y} &\ge \mathbf{c}, \\ \mathbf{y} &\ge \mathbf{0} \end{aligned} \tag{3.3}$$

has a solution if and only if (3.1) has a finite optimum. Furthermore, if $(\mathbf{x}^T, \mathbf{y}^T)^T$ is a solution of (3.3), then $\mathbf{x}$ is an optimal solution of (3.1). It remains to be shown that Algorithm 1 can be used to determine whether a system $A\mathbf{x} \le \mathbf{b}$ has a solution, and if so how to find a feasible solution; the proof of the following lemma is constructive.

LEMMA 6. *The system of linear inequalities*

$$\mathbf{a}_i^T\mathbf{x} \le b_i, \qquad i = 1, \dots, m, \tag{3.4}$$

has a solution if and only if the system of strict linear inequalities

$$\mathbf{a}_i^T\mathbf{x} < b_i + 2^{-L}, \qquad i = 1, \dots, m, \tag{3.5}$$

has a solution.

Proof. If system (3.4) has a solution, then (3.5) must have a solution. We show that the converse is also true by constructing a feasible solution to (3.4) given a solution to (3.5).

For $\mathbf{x} \in \mathbf{R}^n$, define $\theta_i(\mathbf{x}) = \mathbf{a}_i^T\mathbf{x} - b_i$, for $1 \leq i \leq m$, and let $\mathbf{x}_0 \in \mathbf{R}^n$ be arbitrary. We claim that the following is true:

(a) There exists an $\mathbf{x}_1 \in \mathbf{R}^n$ such that $\theta_i(\mathbf{x}_1) \leq \max\{0, \theta_i(\mathbf{x}_0)\}$, for $1 \leq i \leq m$;

(b) The space spanned by $\{\mathbf{a}_i | \theta_i(\mathbf{x}_1) \geq 0\}$ contains every other vector $\mathbf{a}_j$.

Proof of claim. Since $\mathbf{x}_0$ trivially satisfies (a), it suffices to show that if $\mathbf{x}_0$ does not satisfy (b), then we can compute an $\mathbf{x}_1$ such that $\mathbf{x}_1$ satisfies (a) and

$$\{\mathbf{a}_i | \theta_i(\mathbf{x}_1) \geq 0\} \supset \{\mathbf{a}_i | \theta_i(\mathbf{x}_0) \geq 0\}.$$

By repeating this procedure at most m times, we obtain an $\mathbf{x}_1$ satisfying both (a) and (b).

Without loss of generality, let us assume that $\theta_1(\mathbf{x}_0) \geq 0, \ldots, \theta_k(\mathbf{x}_0) \geq 0$ and $\theta_{k+1}(\mathbf{x}_0) < 0, \ldots, \theta_m(\mathbf{x}_0) < 0$. Suppose that $\mathbf{a}_l$, for some $k < l \leq m$, is not a linear combination of $\mathbf{a}_1, \ldots, \mathbf{a}_k$. Then the system of linear equations

$$\mathbf{a}_i^T\mathbf{y} = 0, \qquad i = 1, \ldots, k,$$
$$\mathbf{a}_l^T\mathbf{y} = 1$$

is solvable. Let $\mathbf{y}_0$ be a solution, and consider $\mathbf{x}_1 = \mathbf{x}_0 + t\mathbf{y}_0$, where

$$t = \min\left\{ \frac{-\theta_j(\mathbf{x}_0)}{\mathbf{a}_j^T\mathbf{y}_0} \middle| \mathbf{a}_j^T\mathbf{y}_0 > 0, k < j \leq m \right\}.$$

Since $\theta_j(\mathbf{x}_0) < 0$, for $k < j \leq m$, and $\mathbf{a}_l^T\mathbf{y} = 1$, we have $0 < t \leq -\theta_l(\mathbf{x}_0)$. Thus

$$\theta_i(\mathbf{x}_1) = \theta_i(\mathbf{x}_0 + t\mathbf{y}_0) = t\mathbf{a}_i^T\mathbf{y}_0 + \theta_i(\mathbf{x}_0) \begin{cases} = t \times 0 + \theta_i(\mathbf{x}_0) & \text{if } 1 \leq i \leq k \\ \leq 0 & \text{if } k < i \leq m, \end{cases}$$

where equality holds for some i_0, $k < i_0 \leq m$. Thus we have $\{\mathbf{a}_i | \theta_i(\mathbf{x}_1) \geq 0\} \supseteq \{\mathbf{a}_i | \theta_i(\mathbf{x}_0) \geq 0\} \cup \{\mathbf{a}_{i_0}\}$, which proves the claim (note that $\max\{0, \theta_i(\mathbf{x}_0)\} = \max\{0, \theta_i(\mathbf{x}_1)\}$ for the inductive step).

Let us assume that $\mathbf{x}_0$ satisfies the system of strict linear inequalities (3.5) (thus $\theta_i(\mathbf{x}_0) < 2^{-L}$), and that $\mathbf{a}_i^T\mathbf{x}_0 \geq b_i$, for $1 \leq i \leq k$. Furthermore, let us assume that the labeling is such that $\mathbf{a}_1, \ldots, \mathbf{a}_r$ are linearly independent and span $\mathbf{a}_{r+1}, \ldots, \mathbf{a}_k$. From our claim, we can assume that $\mathbf{a}_1, \ldots, \mathbf{a}_r$ also span $\mathbf{a}_{k+1}, \ldots, \mathbf{a}_m$.

Let $\mathbf{z}$ be a solution of the system of linear equations $\mathbf{a}_j^T\mathbf{z} = b_j$, for $j = 1, \ldots, r$; we show that $\mathbf{z}$ satisfies (3.4). From Cramer's rule and the proof of Lemma 1, we know that $\mathbf{a}_i = \Sigma_{1\le j\le r}(D_j/D)\mathbf{a}_j$, for $1 \le i \le m$, where $D > 0$ and D_j are integers with absolute value less than $2^L/mn$. Thus

$$\begin{aligned} D(\mathbf{a}_i^T\mathbf{z} - b_i) &= \sum_{1\le j\le r} D_j\mathbf{a}_j^T\mathbf{z} - Db_i \\ &= \sum_{1\le j\le r} D_j b_j - Db_i \\ &= \sum_{1\le j\le r} D_j\big(\mathbf{a}_j^T\mathbf{x}_0 - \theta_j(\mathbf{x}_0)\big) - D\big(\mathbf{a}_i^T\mathbf{x}_0 - \theta_i(\mathbf{x}_0)\big) \\ &= D\theta_i(\mathbf{x}_0) - \sum_{1\le j\le r} D_j\theta_j(\mathbf{x}_0) \\ &< D2^{-L} + \sum_{1\le j\le r} |D_j|2^{-L} \\ &< \frac{1}{mn} + \frac{m}{mn} < 1. \end{aligned}$$

Since the left-hand side is an integer, as is seen in the second line, and since $D > 0$, we have $\mathbf{a}_i^T\mathbf{z} - b_i \le 0$; i.e., $\mathbf{z}$ satisfies (3.4). □

4. COMPLEXITY

In this section we analyze the complexity of Khachiyan's algorithm as it has been presented in the previous sections. We show also how to avoid achieving the worst-case behavior whenever the given system of linear inequalities is unsatisfiable. Since the purpose of this paper is to present Khachiyan's algorithm, we will not deal with implementation considerations—there will undoubtedly be a vast number of papers written on this subject in the near future.

To be technically accurate, we must show that the algorithm can work with finite arithmetic and still be polynomial. Of course, the algorithm must be modified by making the ellipsoids a little larger to account for rounding errors, and then to allow more iterations since it will now take longer for the ellipsoids to shrink to the appropriate size. The algorithm can be proved to work with finite precision using $O(nL)$-bit numbers. For instance, if we use $300(n + 1)L$ binary digits after the "decimal" point, multiply each new matrix by a factor of $2^{1/(4(n+1)^2)}$, and allow $10(n + 1)^2L$ iterations, the algorithm remains valid [10].

The complexity measure will be the number of arithmetic operations ($+$, $-$, $\times$, $/$, and $\sqrt{}$) used in the worst case. The worst-case behavior of Algorithm 1 occurs when a given system (2.1) does not have a solution, and the number of iterations is then $4(n + 1)^2L$. During each iteration the algorithm finds a violated inequality, which takes $O(mn)$ operations in the worst case; computing the new ellipsoid (i.e., the new vector $\mathbf{x}^{(k+1)}$ and the new matrix $B^{(k+1)}$ using formulas (2.3) and (2.4), respectively) requires $O(n^2)$ operations. (Note that no matrix multiplications are performed, and that the vector product $(B\mathbf{a})(B\mathbf{a})^T$ yields an $n \times n$ matrix.) Thus the algorithm requires in the worst case $4(n + 1)^2L$ iterations, each one using $O((m + n)n)$ arithmetic operations.

If we want to find a feasible vector for a system of form (3.4), we must perform some additional computation. Algorithm 1 returns a feasible vector for the system $2^L\mathbf{a}_i^T\mathbf{x} < 2^Lb_i + 1$. Note that the factor 2^L, used to obtain an integer system, expands the input size to $O(mnL)$. Following the constructive proof of Lemma 6, we construct a set $\{\mathbf{a}_i | \theta_i(\mathbf{x}_1) \geq 0\}$ spanning every other vector $\mathbf{a}_j$. In the worst case this requires solving m systems of linear equations each of size at most $n \times n$, which takes $O(mn^3)$ time. The total number of arithmetic operations required to construct a solution to (3.4) is dominated by the cost of solving these systems of equations. We conclude that it takes at most $O((m + n)mn^4L)$ arithmetic operations to find a feasible vector for a system of form (3.4); the same bound holds for finding an optimal solution to a linear program.

As we have seen, Algorithm 1 requires $4(n + 1)^2L$ iterations if the given system of linear inequalities has no solution; if the given system has a solution, the algorithm terminates earlier. From the theory of linear programming, it is known that the system

$$\begin{aligned} A\mathbf{x} &\leq \mathbf{b}, \\ \mathbf{x} &\geq \mathbf{0} \end{aligned}$$

has a solution if and only if the system

$$\begin{aligned} A^T\mathbf{y} &\geq \mathbf{0}, \\ \mathbf{y} &\geq \mathbf{0}, \\ \mathbf{b}^T\mathbf{y} &< 0 \end{aligned}$$

is unsatisfiable. By running Algorithm 1 in parallel on the systems of strict linear inequalities corresponding to these two systems, we must find a feasible vector to exactly one of them. The algorithm may now terminate before the full number of iterations even if the original system has no solution, although the computational effort during each iteration is approximately doubled.

REFERENCES

1. P. GÁCS AND L. LOVÁSZ, "Khachiyan's Algorithm for Linear Programming," Technical Report STAN-CS-79-750, Computer Science Department, Stanford University, 1979.

2. M. R. Garey and D. S. Johnson, "Computers and Intractability," Freeman, San Francisco, 1979.
3. L. G. Khachiyan, Convergence rate of the game processes for solving matrix games, *Ž. Vyčisl. Mat. i Mat. Fiz.* **17**:6 (1977), 1421–1431 [English transl., *USSR Computational Math. and Math. Phys.* **17**:6 (1977), 78–88].
4. L. G. Khachiyan, Concerning the convergence of an iterative process for estimating equilibrium points, *Mex. Tverd. Deforn. Tela i Rodstven. Probl. Analiza*, Moskva (1978), 90–95.
5. L. G. Khachiyan and A. I. Erlikh, On the convergence of game processes with differing choice of steps by the partners, *Ekonom. i Mat. Metody* **14**:2 (1978), 332–334.
6. L. G. Khachiyan and A. I. Erlikh, Serial game processes of solution of convex programming problems, *Izv. Akad. Nauk SSSR Teckn. Kibernet.*, No. 2 (1978), 193–196 [English transl., *Engrg. Cybernetics* **16**:2 (1978), 147–151].
7. L. G. Khachiyan, A polynomial algorithm in linear programming, *Dokl. Akad. Nauk SSSR N. S.* **244**:5 (1979), 1093–1096 [English transl., *Soviet Math. Dokl.* **20**:1 (1979), 191–194].
8. N. Z. Shor, Convergence rate of the gradient descent method with dilatation of the space, *Kibernetika*, No. 2 (1970), 80–85 [English transl., *Cybernetics* **6**:2 (1970), 102–108].
9. N. Z. Shor, Cut-off method with space extension in convex programming problems, *Kibernetika*, No. 1 (1977), 94–95 [English transl., *Cybernetics* **13**:1 (1977), 94–95].
10. R. E. Stone, "Khachiyan's Algorithm with Finite Precision," Working Paper SOL 80-1, Department of Operations Research, Stanford University, 1980.