POLYNOMIALLY BOUNDED ELLIPSOID ALGORITHMS FOR CONVEX QUADRATIC PROGRAMMING

TECHNICAL REPORT 80-3

by

Sung J. Chung and Katta G. Murty

Department of Industrial and Operations Engineering
The University of Michigan
Ann Arbor, Michigan 48109, USA

Research effort partially supported by the Air Force Office of Scientific Research, Air Force Systems Command, USAF, under grant No. AFOSR 78-3646. The United States Government is authorized to reproduce and distribute reprints for governmental purposes, notwithstanding any copyright notation hereon. This paper was typed by Mrs. Geraldine Cox.

June 1980

ABSTRACT

We show that the ellipsoid algorithm of N. F. Shor and L. G. Khachiyan, can be applied to solve convex quadratic programming problems with integer data in polynomially bounded time.

KEYWORDS

Convex quadratic programming, linear complementarity problem, nearest point problem, positive semi-definite matrix, ellipsoid algorithm, polynomially bounded algorithm.

1. Introduction

The ellipsoid algorithm of N. Z. Shor and L. G. Khachiyan [9,11,26] processes systems of linear inequalities and linear programming problems with computational requirements that are bounded above by a polynomial in the size of the problem. Here we show that the ellipsoid algorithm can be extended to solve convex quadratic programs with integer data in polynomial time. It is well known that every convex quadratic programming problem can be posed as a linear complementarity problem (abbreviated here as LCP, see references [5,16,21]), associated with a positive semi-definite (abbreviated in the paper as PSD) matrix, and vice versa; and hence the methods described here provide polynomially bounded algorithms for processing this special class of LCPs. This clearly establishes that convex quadratic programs and LCPs associated with PSD matrices belong to the class P of problems, which is the class of problems solvable by polynomially bounded algorithms. Algorithms described in this paper can only process LCPs associated with PSD matrices, and in fact S. J. Chung [3] has shown that the LCP associated with a general matrix is strongly NP-Complete. Even the LCP associated with a negative definite matrix (abbreviated in the sequel as ND matrix) is NP-Complete, and in Section 5, we briefly explore the fundamental difference between LCPs associated with PSD matrices and ND matrices, that accounts for the difference in their computational complexity.

Most of the work in this paper was carried out soon after the technical report of P. Gacs and L. Lovasz on Khachiyan's algorithm [9] became available in August 1979, and the version of the ellipsoid algorithm for solving nearest point problems appeared in the technical report [4]. Similar work has been carried out independently by several groups of researchers, among which we became aware of those of P. C. Jones and E. S. Marwil [12], I. Adler, R. P. McLean and J. S. Provan [1], and M. K. Kozlov, S. P. Tarasov and L. G. Khachiyan [14].

The organization of the paper is as follows: In Section 2 we present the nearest point problem which is a special convex quadratic programming problem that leads to an LCP with positive definite (abbreviated in the sequel as PD) symmetric matrix, describe the ellipsoid algorithm for solving it, and prove that it obtains the solution of the problem in polynomial time. Our estimates of the running time of this algorithm are generous in the sense that emphasis is placed on proving that the algorithm is polynomially bounded, but not so much in obtaining the exact worst case bound on the running time. This algorithm has been coded by Y. Fathi, and comparative computational experience of this algorithm, and other algorithms for solving the nearest point problem described in [7] is summarized at the end of Section 2. In Section 3 we discuss the application of the ellipsoid algorithm to solve LCPs associated with PD matrices and prove that it is polynomially bounded. In Section 4 we develop the application of the ellipsoid algorithm to solve LCPs associated with PSD matrices and prove that it is polynomially bounded.

We use regular style superscripts to distinguish between vectors, as in x^1, x^2. We also need exponents, and in order to distinguish between exponents and superscripts, we use only bold letters to indicate exponents, for example $\alpha^{\mathbf{r}}$ indicates α to the power of r.

For $x \in R^n$, $||x|| = \sqrt{\sum_{j=1}^{n} x_j^2}$ denotes the usual Euclidean norm of x.

If D is a matrix; we denote by $D_{i.}$ the ith row vector of D; and by $D_{.j}$ the jth column vector of D.

A vector $a = (a_1,\ldots,a_n)$ is nonnegative (denoted $a \geqq 0$) if $a_j \geqq 0$ for all j. It is positive (denoted $a > 0$) if a_j is strictly positive for all j. It is semi-positive (denoted $a \geq 0$) if $a \geqq 0$, but $a \neq 0$.

For applications of the LCP see [13, 17, 23].

2. THE NEAREST POINT PROBLEM

Let B be a given integer square nonsingular matrix of order n. Pos (B) = $\{x: x = Bz, z = (z_1,\ldots,z_n) \geqq 0\}$. For $x \in \text{Pos}(B)$, $z = B^{-1}x$ is known as the (nonnegative) combination vector corresponding to x. We consider the problem of finding the nearest point (in terms of the usual Euclidean distance) in the simplicial cone Pos(B) to a given integer point $b \in R^n$. This problem will be denoted by the symbol [B;b] and is called a nearest point problem of order n. For n = 1 the problem is trivial, so in the sequel we assume $n \geqq 2$. [B;b] is equivalent to the quadratic program: Find z to

$$\begin{aligned} &\text{Minimize} \quad -b^TBz + \frac{1}{2} z^T(B^TB)z \\ &\text{Subject to} \qquad z = (z_1,\ldots,z_n) \geqq 0 \end{aligned} \tag{1}$$

The solution of (1) can be obtained by solving the LCP (see [5,16,21])

$$\begin{aligned} &w - (B^TB)z = - B^Tb \\ &w \geqq 0,\ z \geqq 0 \\ &\quad w_jz_j = 0,\ j = 1 \text{ to } n \end{aligned} \tag{2}$$

where $w = (w_1,\ldots,w_n)^T$ is a column vector of variables in R^n. Let $M = B^TB$, $q = - B^Tb$. Then (2) is the LCP denoted by (q, M) and can be written in the familiar form

$$\begin{aligned} I\, w - M\, z &= q \\ w \geqq 0,\ z &\geqq 0 \\ w^T z &= 0 \end{aligned} \qquad (3)$$

Since M is a P-matrix (2) or (3) has a unique solution $(\bar{w}, \bar{z})$ (see [20,22,25]) and then $\bar{z}$ is the optimum solution of (1) (see [8, 22]). If $b \in \text{Pos}(B)$ then b is itself the solution of [B;b] and $(\bar{w} = 0,\ \bar{z} = B^{-1}b)$ is the unique solution of (2). So we assume that $b \notin \text{Pos}(B)$, and in this case, the solution of [B;b] is a point on the boundary of Pos(B). Since we are assuming that $b \notin \text{Pos}(B)$, $b \neq 0$.

In the LCP (3), the pair of variables (w_j, z_j) form the *jth complementary pair of variables* and each variable in this pair is the complement of the other. In any solution of (3), at least one variable in each of the complementary pairs must be zero. The vector $(y_1,\dots,y_n)$ is called a *complementary vector of variables* in (3) if $y_j \in \{w_j, z_j\}$ for each j = 1 to n. A complementary vector of variables for (3) is called a *complementary basic vector* if the set of column vectors corresponding to these variables in the system of equality constraints in (3) is linearly independent. A complementary basic vector for (3) is said to be a *complementary feasible basic vector for (3)* if the solution obtained by setting all the nonbasic variables to zero and then solving the remaining system of equality constraints in (3) for the values of the basic variables, satisfies the nonnegativity restrictions on all the variables; and in this case that solution obtained is known as the *complementary BFS* (basic feasible solution) of (3) corresponding to that complementary feasible basic vector.

SOME PRELIMINARY RESULTS:

THEOREM 1: The set of feasible solution of

$$\begin{aligned} B^{-1}x &\geqq 0 \\ B^{T}(x-b) &\geqq 0 \end{aligned} \qquad (4)$$

has a nonempty interior.

PROOF: We want to show that

$$\begin{aligned} B^{-1}x &> 0 \\ B^{T}(x-b) &> 0 \end{aligned} \qquad (5)$$

has a feasible solution x. Clearly (5) has a feasible solution iff

$$\begin{aligned} B^{-1}x &> 0 \\ B^{T}x-B^{T}b\, x_{n+1} &> 0 \\ x_{n+1} &> 0 \end{aligned} \qquad (6)$$

has a feasible solution $X = \begin{pmatrix} x \\ \cdots \\ x_{n+1} \end{pmatrix}$. By Gordan's theorem of the alternative (see [18]) (6) has a feasible solution X iff there exists no $\pi \in R^n$, $\mu \in R^n$, $\gamma \in R^1$ which together satisfy

$$\begin{aligned} \pi B^{-1} + \mu B^{T} &= 0 \\ - \mu B^{T} b + \gamma &= 0 \\ (\pi, \mu, \gamma) &\geq 0. \end{aligned} \qquad (7)$$

From the first n constraints in (7), we have $\mu B^T B = -\pi \leqq 0$. Since $B^T B$ is PD, we know that the system

$$\begin{aligned} \mu B^T B &\leqq 0 \\ \mu &\geqq 0 \end{aligned} \tag{8}$$

has the unique solution $\mu = 0$ (or otherwise there would exist a $\mu \ngtr 0$ such that $\mu B^T B \mu^T \leqq 0$, a contradiction to the positive definiteness of $B^T B$). So in any feasible solution to (7), μ will have to be zero, which implies in turn that π and γ will have to be zero too, a contradiction. So (7) cannot have a feasible solution. Hence the set of feasible solutions of (4) has a non-empty interior. Q.E.D.

THEOREM 2: Let K be the set of feasible solutions of (4). Let S be the sphere determined by

$$(x - b/2)^T (x - b/2) = b^T b/4 \tag{9}$$

$K \cap S$ consists of a single point, and this point is the nearest point in Pos(B) to b. Also, let E be the ball with S as boundary. Then $K \cap E$ is the set containing this single point.

PROOF: We want to prove that the system

$$\begin{aligned} B^{-1}x &\geqq 0 \\ B^T(x-b) &\geqq 0 \\ (x-b/2)^T (x-b/2) &= b^T b/4 \end{aligned} \tag{10}$$

has the nearest point in Pos(B) to b as the unique solution.

Let $\bar{x}$ be the nearest point in Pos(B) to b. Let $\bar{z} = B^{-1}\bar{x}$, $\bar{w} = q + M\bar{z}$. By earlier discussion (also [8,22]), $(\bar{w}, \bar{z})$ is then the solution of the LCP (2) or (3). So $\bar{z} = B^{-1}\bar{x} \geqq 0$, $0 \leqq \bar{w} = q + M\bar{z} = - B^Tb + B^TB\, B^{-1}\bar{x} = B^T(\bar{x}-b)$, from the definition of M and q. And $(\bar{x} - b/2)^T (\bar{x} - b/2) - (b^Tb/4) = \bar{x}^T\bar{x} - \bar{x}^Tb = \bar{x}^T(\bar{x}-b) = \bar{z}^T B^T(\bar{x}-b) = \bar{z}^T\bar{w} = 0$ from (2). So $\bar{x}$ is a solution of (10).

Conversely, suppose $\bar{x}$ is a solution of (10). Define $\bar{z} = B^{-1}\bar{x}$, $\bar{w} = B^T(\bar{x}-b)$. From the last equation in (10) we have $0 = (\bar{x} - b/2)^T (\bar{x} - b/2) - (b^Tb/4) = \bar{x}^T(\bar{x}-b) = \bar{z}^T\bar{w}$. Also from the definition of M, q, we have $\bar{w} = B^T(\bar{x}-b) = -B^Tb + B^TB\, B^{-1}\bar{x} = q + M\bar{z}$. These facts imply that $(\bar{w}, \bar{z})$ defined here is a solution of the LCP (2) or (3), which by earlier discussion implies that $\bar{x}$ is the nearest point in Pos(B) to b. Also

$$E = \{x: (x - b/2)^T (x - b/2) \leqq b^Tb/4\}$$

For all $x \in K$ we have

$$\begin{aligned}(x - b/2)^T (x - b/2) &= x^T(x-b) + b^Tb/4 \\ &= (B^{-1}x)^T B^T(x-b) + b^Tb/4 \\ &\geqq b^Tb/4.\end{aligned}$$

Therefore $K \cap E = K \cap S$ Q.E.D.

THEOREM 3: The unique solution of (10) is an extreme point of K.

PROOF: From known results about LCPs [5,16,21,22], the unique solution of the LCP (q, M), $(\bar{w}, \bar{z})$, is an extreme point of (3). So $\bar{z}$ is an extreme point of

$$\begin{aligned} - Mz &\leqq q \\ z &\geqq 0 \end{aligned} \qquad (11)$$

Since $M = B^T B$, $q = -B^T b$, we notice that if z is a solution of (11), then $x = Bz$ solves (4); and conversely if x solves (4), then $z = B^{-1}x$ solves (11). Hence there is a 1-1 correspondence between solutions of (4) and (11). So, since $\bar{z}$ is an extreme point of (11); $\bar{x} = B^{-1}\bar{z}$, which is the unique solution of (10) by Theorem 2, must be an extreme point of (4). Q.E.D.

Let L_1 be the total number of digits required for specifying the data in $B = (b_{ij})$, $b = b_i$ in binary form. So we have approximately

$$L_1 = \lceil (1 + \log_2 n + \sum_{\substack{i=1 \text{ to } n \\ j=1 \text{ to } n}} (1 + \log_2(|b_{ij}| + 1)) + \sum_{i=1}^{n} (1 + \log_2(|b_i| + 1)) \rceil \quad (12)$$

Since $M = (m_{ij}) = B^T B$ and $q = (q_i) = -B^T b$, each m_{ij} or q_i is a sum of n terms, each term being a product of two entries from $(B \vdots b)$, or the square of an entry in $(B \vdots b)$. So each m_{ij} or q_i is of the form $\gamma_1\gamma_2 + \gamma_3\gamma_4 + \ldots + \gamma_{2n-1}\gamma_{2n}$ where the γ's are entries from $(B \vdots b)$. So we have

$$\log_2 (m_{ij}) = \log_2 (\gamma_1\gamma_2 + \ldots + \gamma_{2n-1}\gamma_{2n})$$

$$\leqq \log_2((|\gamma_1| + 2)(|\gamma_2| + 2) + \ldots + (|\gamma_{2n-1}| + 2)(|\gamma_{2n}| + 2))$$

$$\leqq \log_2((|\gamma_1| + 2)(|\gamma_2| + 2)(|\gamma_3| + 2) \cdots (|\gamma_{2n}| + 2)) \quad (13)$$

since each γ is an integer, $(|\gamma| + 2)$ is an integer greater than or equal to 2, and hence, the sum of terms like this is less than the product of these terms. Also $\log_2 (|\gamma| + 2) \leqq 1 + \log_2 (|\gamma| + 1)$. So from (13) and (12) we see that

$$\log_2(m_{ij}) \leqq L_1.$$

Let

$$L_2 = n(n+1)(L_1 + 1)$$

So, by the above, the total number of digits needed to specify the data in the system (3) is at most L_2.

THEOREM 4: If $(\bar{w}, \bar{z})$ is an extreme point of (3), then any $\bar{w}_i$ or $\bar{z}_i$ is either 0 or $> 2^{-L_2}$.

PROOF: Remembering that L_2 is the size of the system (3), this theorem follows from the results of [9,11]. Q.E.D.

From the results of [9,11], the absolute value of the determinant of B is at most $2^{L_1}/n$. The same bound also holds for the determinant of any submatrix of B. So there exists a positive integer $\beta < 2^{L_1}/n$ such that all the data in the system

$$\begin{aligned} \beta B^{-1} x &\geqq 0 \\ B^T(x-b) &\geqq 0 \end{aligned} \tag{14}$$

are integers. The absolute value of each entry in βB^{-1} is $< [(2^{L_1})/n]^2$ (since it is less than or equal to a subdeterminant of B times β). Hence the size of (14), the total number of digits in the data in (14), is at most L_3 where

$$L_3 = (n(2n + 1) + 1)\, L_1 \tag{15}$$

THEOREM 5: The length of any edge of K is $\geqq 2^{-L_3}$.

PROOF: If the edge is unbounded, the theorem is trivially true. Each bounded edge of K is the line segment joining two distinct adjacent extreme points of K. Let x^1, x^2 be any two distinct extreme points of K. From the results of [9,11] and the fact that (4) is the same as (14), we have

$$x^1 = (u_{11}/v_1, \ldots, u_{n1}/v_1)$$

$$x^2 = (u_{12}/v_2, \ldots, u_{n2}/v_2)$$

where v_1, v_2 and all the u_{ij}'s are integers; and v_1, v_2 are both nonzero; and $|v_1|$, $|v_2|$ and all $|u_{ij}|$ are $\leqq 2^{L_3}/n$. Since $x^1 \neq x^2$, either there exists a j such that $|u_{j1} - u_{j2}| \geqq 1$, or $u_{j1} = u_{j2}$ for all j and $|v_1 - v_2| \geqq 1$. These facts together imply that there exists a j such that $|x_j^1 - x_j^2| \geqq 2^{-L_3}$. This clearly implies that $||x^1 - x^2|| \geqq 2^{-L_3}$. Q.E.D.

THEOREM 6: Let ε be a positive number $< 2^{-2(n+1)^2 L_1}$ and let E_1 be the ball

$$(x - b/2)^T (x - b/2) \leqq (\varepsilon + \sqrt{b^T b/4})^2 \qquad (16)$$

Then the n-dimensional volume of $K \cap E_1$ is greater than or equal to $\varepsilon^n 2^{-(n+1)L_3}$.

PROOF: K, the set of feasible solutions of (4) or (14), is the intersection of the pointed cone $\{x: B^{-1}x \geqq 0\}$ with the translate of a pointed cone $\{x: B^T(x-b) \geqq 0\}$, with a nonempty interior by Theorem 1. The intersection $S \cap K$ consists of a single point, say V_0; and $E_1 \cap K$ contains all the points in K in an ε - neighborhood of V_0, and hence has a nonempty interior and a positive n-dimensional volume.

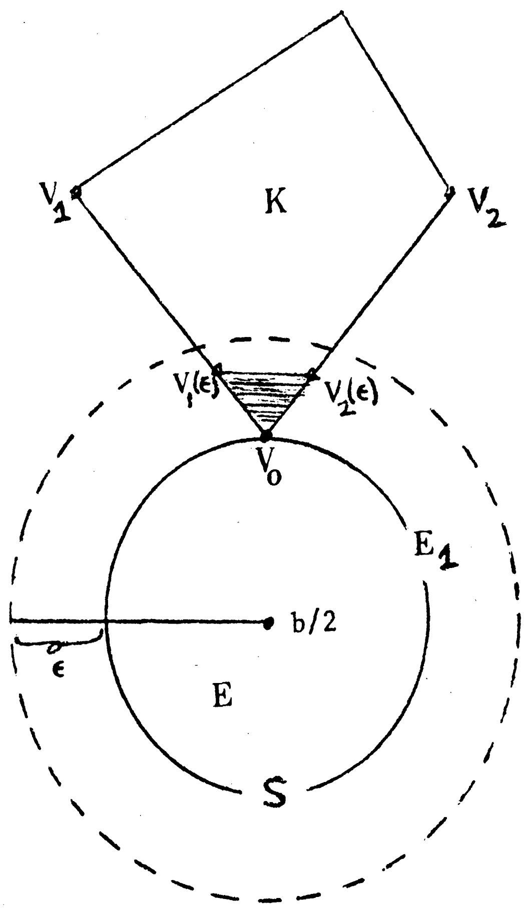

Figure 1: The volume of $E_1 \cap K$ is greater than or equal to the volume of the shaded simplex.

If one takes a sphere of radius α, a concentric sphere of radius $\alpha+\varepsilon$, and a hyperplane tangent to the smaller sphere at a boundary point x on it, then a tight upper bound on the distance from x of any point in the larger sphere on the side of the hyperplane opposite the smaller sphere is $\sqrt{2\alpha\,\varepsilon+\varepsilon^2}$. Also the radius of E is $\sqrt{b^Tb/4} < 2^{(L_1-1)}$. From Theorem 3, V_0 is an extreme point of K, and every edge of K through V_0 has a length $\geqq 2^{-L_3}$ by Theorem 5. These facts and the choice of ε here, together imply that every edge of K through V_0 intersects the boundary of E_1. Let $V_1,\ldots,V_n$ be points along the edges of K through V_0 that intersect the boundary of E_1, at a distance of at most 1 but greater than ε from V_0, such that $\{V_0, V_1\ldots V_n\}$ is affinely independent. The portion of the edge between V_0 and V_i lies inside E_1 for at least a length of ε. See Figure 1. If $V_i(\varepsilon)$ is the point on the edge joining V_0 and V_i at a distance of ε from V_0, the volume of $E_1 \cap K$ is greater than or equal to the volume of the simplex whose vertices are V_0, $V_i(\varepsilon)$ for i=1 to n. From the choice of V_i, $V_i(\varepsilon) - V_0 = \gamma(V_i - V_0)$ where $\gamma \geqq \varepsilon$. So in this case the volume of $E_1 \cap K$ is greater than or equal to

$$\frac{1}{n!}\left|(\text{determinant of } (\varepsilon(V_1 - V_0) \vdots \ldots \vdots \varepsilon(V_n - V_0))\right|$$

$$= \frac{\varepsilon^n}{n!}\left|(\text{determinant of } ((V_1 - V_0) \vdots \ldots \vdots (V_n - V_0))\right|$$

$$= \frac{\varepsilon^n}{n!}\left|(\text{determinant of} \begin{pmatrix} 1 & \vdots & 1 & \vdots & \ldots & \vdots & 1 \\ V_0 & \vdots & V_1 & \vdots & & \vdots & V_n \end{pmatrix}\right|$$

$$\geqq \varepsilon^n \, 2^{-(n+1)L_3}.$$

from the results in [9,11]. Q.E.D.

In the sequel, we will denote the unique point in $S \cap K$ by $\bar{x}$ (this was called V_0 in the proof of Theorem 6). Let $\bar{z} = B^{-1}\bar{x}$, $\bar{w} = B^T(\bar{x}-b)$. By earlier discussion $(\bar{w}, \bar{z})$ is the solution of the LCP (2) or (3), and it is an extreme point.

THEOREM 7: For any $\hat{x} \varepsilon E_1 \cap K$, define $\hat{z} = B^{-1}\hat{x}$ and $\hat{w} = B^T(\hat{x}-b)$. Then the following hold, for all j = 1 to n.

$$|\hat{x}_j - \bar{x}_j| \leqq 2^{L_1} \sqrt{\varepsilon}$$

$$|\hat{z}_j - \bar{z}_j| \leqq n2^{2L_1} \sqrt{\varepsilon}$$

$$|\hat{w}_j - \bar{w}_j| \leqq n2^{2L_1} \sqrt{\varepsilon}$$

PROOF: Using the results in [9,11] we see that the value of any entry in B^{-1} has an absolute value less than or equal to 2^{L_1}, and the same fact obviously holds for B^T. As mentioned in the proof of Theorem 6, if one takes a sphere of radius α, a concentric sphere of radius $\alpha+\varepsilon$, and a hyperplane tangent to the smaller sphere at a boundary point x on it, then a tight upper bound on the distance from x of any point in the larger sphere on the side of the hyperplane opposite the small sphere is $\sqrt{2\alpha\varepsilon + \varepsilon^2}$. As the radius of E is $\sqrt{b^T b/4} < 2^{L_1 - 1}$, the results in the theorem follow from this fact and the definitions of E, S, E_1, $\hat{w}$, $\hat{z}$. Q.E.D.

THEOREM 8: Let $\hat{x}$ be an arbitrary point in $E_1 \cap K$, and let $\hat{z}$, $\bar{z}$ be as defined above. If

$$\varepsilon \leqq 2^{-2(n+1)^2(L_1+1)} \tag{17}$$

then

$$\hat{z}_j \leqq \frac{1}{4} 2^{-L_2} \quad \text{if } j \text{ is such that } \bar{z}_j = 0 \tag{18}$$

$$\geqq (\frac{3}{4})2^{-L_2} = \delta, \text{ if } j \text{ is such that } \bar{z}_j > 0.$$

PROOF: This follows from the results proved in Theorems 7 and 4. Q.E.D.

THEOREM 9: Let $\bar{x}$ be the nearest point in Pos(B) to b, and $\bar{z} = B^{-1}\bar{x}$. Let

$$J = \{j: \bar{z}_j > 0\}.$$

Define the vector of variables $y = (y_j)$ by

$$y_j = z_j \quad \text{if } j \in J$$

$$= w_j \quad \text{if } j \notin J$$

Then y is a feasible basic vector for (2) or (3) and the complementary BFS corresponding to the basic vector y is the solution of this LCP.

PROOF: By the discussion earlier, if $\bar{w} = M\bar{z} + q$, then $(\bar{w}, \bar{z})$ is the solution of the LCP (2) or (3). This result that the basic vector y defined as above is a complementary feasible basic vector is well known about LCPs associated with positive definite matrices or even P-matrices [8,22]. Q.E.D.

THE ALGORITHM

Fix $\varepsilon = 2^{-2(n+1)^2(L_1+1)}$. Consider the following system of constraints

$$\begin{aligned} - B^{-1}x & \leqq 0 \\ - B^T(x-b) & \leqq 0 \end{aligned} \qquad (19)$$

which is the same as (14) or (4); and the quadratic constraint (16). Define

$$x^1 = (b/2),\ A_1 = I(\varepsilon + \sqrt{b^T b/4})^2 \qquad (20)$$

where I is the identity matrix of order n.

Given any point $x^k \varepsilon R^n$ and a symmetric positive definite matrix A_k of order n, define $E(x_k, A_k)$ to be the ellipsoid

$$E(x^k, A_k) = \{x: (x-x^k)^T A_k^{-1} (x-x^k) \leqq 1\} \qquad (21)$$

$E_1 = E(x^1, A_1)$ is the ball defined by (16). Here we describe a modification of Shor-Khachiyan's ellipsoid algorithm [9,11] to find a point in $E_1 \cap K$, that is, a point satisfying (19) and (16). Let $N = 8(n+1)^4(L_1+1)$. With x^1, A_1, E_1 go to Step 2.

GENERAL STEP r + 1

Let x^r, A_r, $E_r = E(x^r, A_r)$; be respectively the center, positive definite symmetric matrix, and the ellipsoid at the beginning of this step.

If x^r is feasible to both (19) and (16) it is the point we are seeking. In this case, terminate the ellipsoid algorithm. Call x^r as $\hat{x}$ and go to the *final step* described below.

If x^r violates at least one of the constraints in (19) or (16), select an inequality constraint

$$ax \leqq d \tag{22}$$

violated by x^r, as described in one of the two cases below.

CASE 1: $x^r \notin K$

So, in this case, x^r violates one or more constraints in (19). In this case select (22) to be the constraint in (19) that x^r violates most. Break ties arbitrarily.

CASE 2: $x^r \in K$ BUT $x^r \notin E_1$

So, in this case, x^r satisfies all the constraints in (19), but violates (16). Find the point of intersection ξ^r, of the line segment joining x^1 and x^r with the boundary of E_1,

$$(x - x^1)^T (x - x^1) = (\varepsilon + \sqrt{b^T b/4})^2 \tag{23}$$

Actually $\xi^r = \lambda x^1 + (1-\lambda)x^r$, where $\lambda = 1 - ((\varepsilon + \sqrt{b^T b/4}\ )/\ ||x^r - x^1||)$.
In this case, choose (22) to be the half-space not containing x^r, determined by the tangent plane of E_1 at its boundary point ξ^r. Thus in this case "ax = d" is the tangent plane of E_1 at ξ^r, and x^r violates (22). See Figure 2.

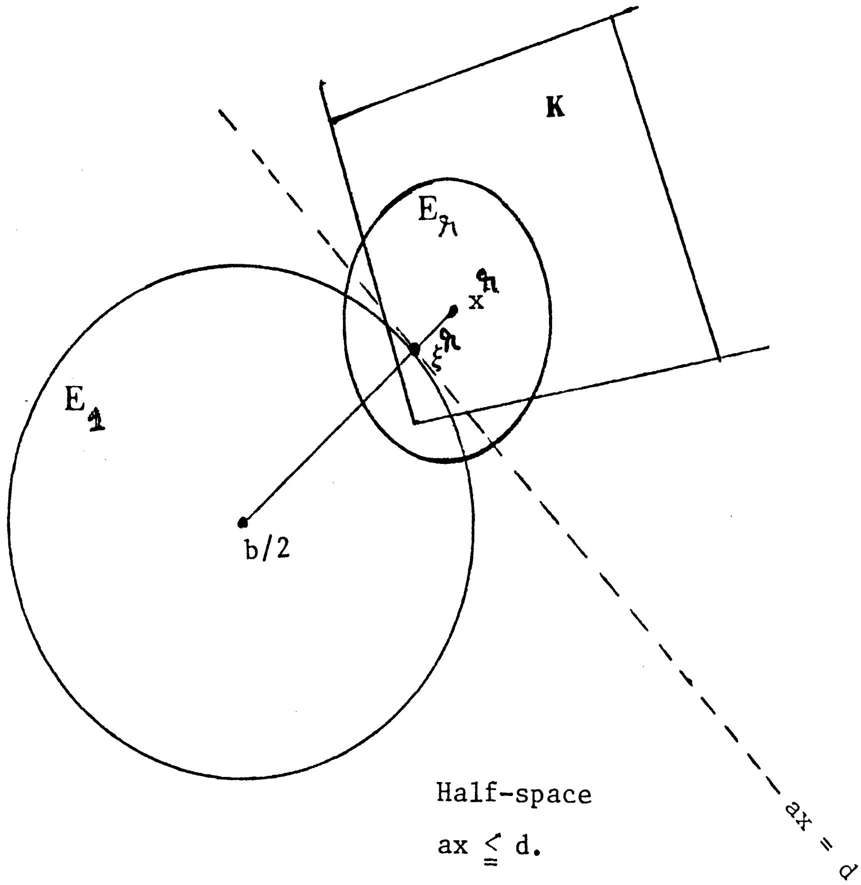

Figure 2: Construction of "ax $\leqq$ d" when x^r satisfies (19) but violates (16).

Now define (see [10,15] among others)

$$\gamma_r = \frac{d - ax^r}{\sqrt{a\ A_r a^T}}$$

$$x^{r+1} = x^r - \left(\frac{1 - \gamma_r n}{1 + n}\right) \left(\frac{A_r\ a^T}{\sqrt{aA_r a^T}}\right) \tag{24}$$

$$A_{r+1} = \left(\frac{(1-\gamma_r^2)n^2}{n^2-1}\right)\left(A_r - \left(\frac{2}{n+1}\right)\left(\frac{1-n\gamma_r}{1-\gamma_r}\right)\left(\frac{(A_r a^T)(A_r a^T)^T}{a\ A_r a^T}\right)\right)$$

With x^{r+1}, A_{r+1}, $E_{r+1} = E(x^{r+1}, A_{r+1})$ move to the next step in the algorithm.

After at most N steps, this ellipsoid algorithm will terminate with the point x^r in the terminal step lying in $E_1 \cap K$. Then go to the final step discussed below.

FINAL STEP:

Let the center of the ellipsoid in the terminal step be $\hat{x}$ (this is the point x^r in the last step r of the ellipsoid algorithm). Let $\hat{z} = B^{-1}\hat{x}$. Define J to be

$$J = \{j\colon j \text{ such that } \hat{z}_j \geqq (\tfrac{3}{4})\ 2^{-L_2} = \delta\}$$

Define $y = (y_j)$ by

$$\begin{aligned} y_j &= z_j \quad \text{if } j \in J \\ &= w_j \quad \text{if } j \notin J \end{aligned}$$

Then y is a complementary feasible basic vector for (2) or (3), and the BFS corresponding to it is the solution of the LCP (2) or (3). If $(\bar{w}, \bar{z})$ is the solution, $\bar{x} = B\bar{z}$ is the nearest point in Pos(B) to b.

PROOF OF THE ALGORITHM

Let x^r, A_r, $E_r = E(x^r, A_r)$, be the center, positive definite symmetric matrix, and the ellipsoid at the beginning of step r + 1. The inequality (22) is choosen in this step r + 1 in such a way that x^r violates it. In the hyperplane "ax = d" decrease d until a value d_1 is reached such that the translate "$ax = d_1$" is a tangent plane to the ellipsoid E_r, and suppose the boundary point of E_r where this is a tangent plane is η_r. Then $E_{r+1} = E(x^{r+1}, A_{r+1})$ is the minimum volume ellipsoid that contains $E_r \cap \{x: ax \leqq d\}$, (the shaded region in Figure 3), has η_r as a boundary point and has the same tangent plane at η_r as E_r.

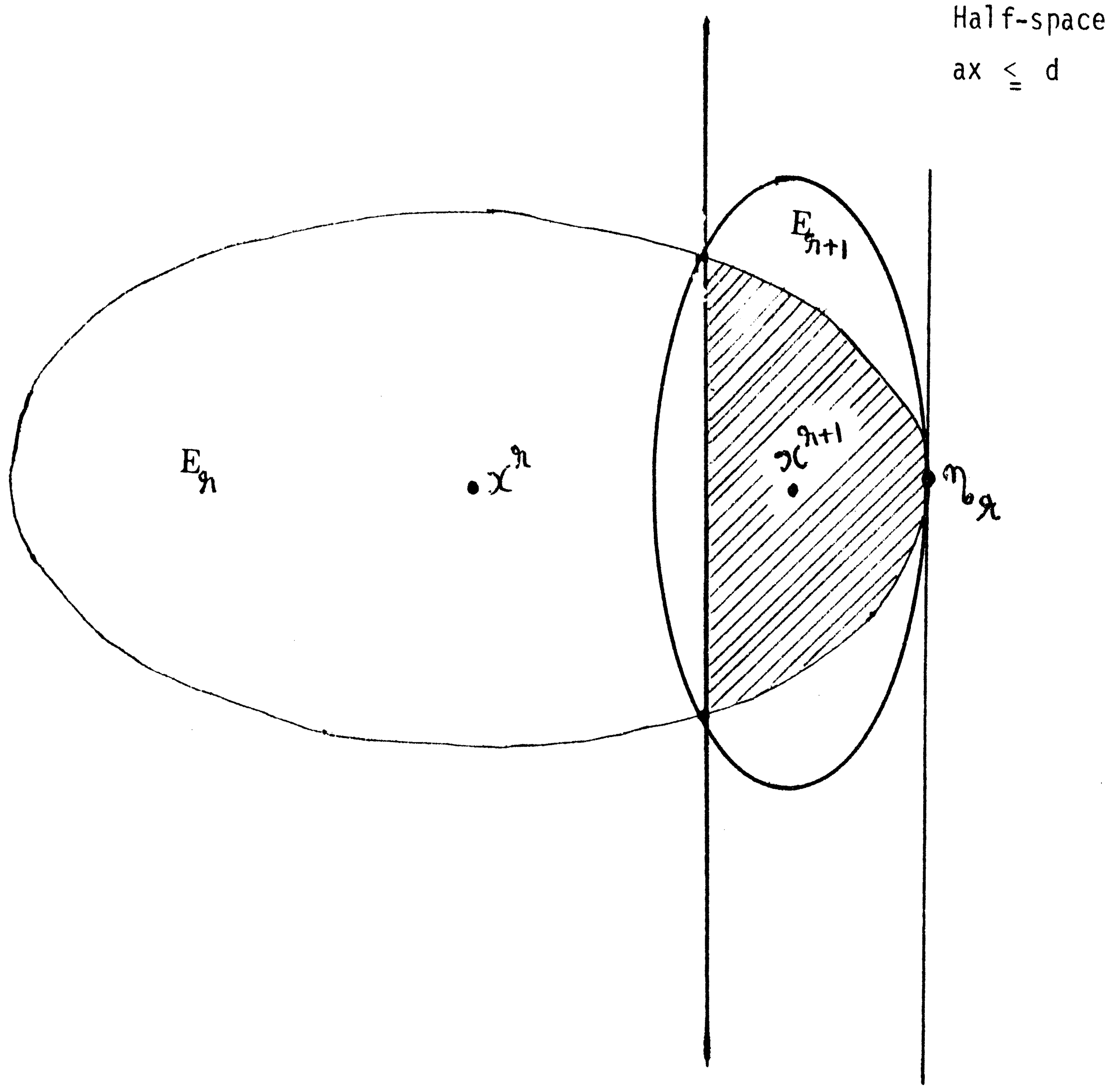

Figure 3: Construction of the new ellipsoid E_{r+1} in the modification of Shor-Khachiyan's algorithm.

From the manner in which the inequality (22) is selected, it is clear that if $E_r \supset E_1 \cap K$, then $E_{r+1} \supset E_1 \cap K$. Arguing inductively on r, we conclude that every ellipsoid E_r constructed during the algorithm satisfies

$$E_r \supset E_1 \cap K \tag{25}$$

From Theorem 6, the volume of $E_1 \cap K$ is $\geqq 2^{-4n(n+1)^2(L_1+1)}$. From [9,11], the volume of E_r gets multiplied by a factor of $e^{-(1/2(n+1))}$ or less, after each step in Shor-Khachiyan's algorithm. E_1 is a ball whose radius is $(\varepsilon + \sqrt{b^Tb/4})$ and we know that $b^Tb < 2^{2L_1}$. So the volume of E_1 is at most 2^{2nL_1}. The algorithm terminates in step r, if the center x^r satisfies (19) and (16), that is, it is a point in $E_1 \cap K$. If termination does not occur upto step $N = 8(n+1)^4(L_1+1)$, the volume of E_N is at most $2^{2L_1n} e^{-(N/2(n+1))} < 2^{-4n(n+1)^2(L_1+1)}$. From the fact that the volume of $E_1 \cap K > 2^{-4n(n+1)^2(L_1+1)}$ this is a contradiction to (25). So for some $r \leqq N$, we will have $x^r \varepsilon E_1 \cap K$, and in that step the algorithm terminates. The validity of the remaining portion of the algorithm follows from Theorems 7, 8, 9.

Since the algorithm terminates after at most $N = 8(n+1)^4(L_1+1)$ steps, the algorithm is obviously polynomially bounded.

In practice, it is impossible to run the algorithm using exact arithmetic. To run the algorithm with finite-precision (for example, if all the computationns are performed to approximation within $2^{-n^4L_1}$) requires that the ellipsoids be expanded by a small amount in each iteration. This has been completely analyzed in [11], and those results can be applied to this algorithm directly.

Eventhough the algorithm developed here is a polynomially bounded algorithm for the nearest point problem, it is not clear that it will be efficient to solve practical problems. In particular, this algorithm is not likely to beat those discussed in [8] for practical efficiency.

COMPUTATIONAL COMPARISON

Y. Fathi [7] did a comparative study in which this ellipsoid algorithm has been compared with two other algorithms for the nearest point problem. We provide a summary of his results here. In the table below, algorithm I refers to an algorithm discussed by P. Wolfe in [27], algorithm II refers to an algorithm developed by Y. Fathi and K. G. Murty in [8], and algorithm III refers to the ellipsoid algorithm discussed in this section. In the study the matrix B was generated randomly, with its entries to be integers between -5 and + 5. The b-vector was also generated randomly with its entries to be integers between -20 and + 20. Instead of using computer times for the comparison, he counted the number of iterations of various types and from it estimated the total number of multiplication, division operations required before termination on each problem. Problems with n = 10, 20, 30, 40, 50 were tried and each entry in the table is an average for several problems (between 10 (for n = 50) to 50 (for smaller n) problems). Double precision was used. It was not possible to take the values of ε and δ as small as those recommended in the algorithm. Mostly he tried $\varepsilon, \delta = 0.1$ (the computational effort before termination in algorithm III reported in the table below refers to $\varepsilon, \delta = 0.1$), and with this, sometimes the complementary basic vector obtained at termination of the algorithm turned out to be infeasible (this result is called an *unsuccessful run*). He noticed that if the values of these tolerances were decreased, the probability of an unsuccessful run decreases; but the computational effort required before termination increases, both happening very rapidly.

n	Average Number of Multiplication, Division Operations Required Before Termination in		
	Algorithm I	Algorithm II	Algorithm III (Ellipsoid Algorithm)
10	Too small	Too small	33,303
20	39,096	16,266	381,060
30	123,644	42,592	1,764,092
40	514,822	170,643	5,207,180
50	896,919	324,126	11,286,717

These empirical results suggest that the ellipsoid algorithm cannot compete with other existing algorithms for the nearest point problem, in practical efficiency. The same comment seems to hold for the other ellipsoid algorithms discussed next in Sections 3, 4.

3. LCPs ASSOCIATED WITH PD MATRICES

In this section M denotes a given PD matrix of order n (symmetric or not) with integer entries, and q denotes a given integer column vector in R^n. We consider the LCP (q, M), which is to find $w \in R^n$, $z \in R^n$ satisfying

$$\begin{aligned} I\,w - Mz &= q \\ w \geqq 0, \quad z &\geqq 0 \\ w^T z &= 0 \end{aligned} \tag{26}$$

In this section we let K denote the set of feasible solutions of

$$\begin{aligned} Mz + q &\geqq 0 \\ z &\geqq 0 \end{aligned} \tag{27}$$

We let E denote the ellipsoid which is the set of all $z \in R^n$ satisfying

$$z^T(Mz + q) \leqq 0 \tag{28}$$

and let Bd(E) be the boundary of E, that is, it is the set of all z satisfying

$$z^T(Mz + q) = 0 \tag{29}$$

THEOREM 11: K, the set of feasible solutions of (27), has a nonempty interior.

PROOF: Remembering that M is PD, the proof of this theorem is similar to that of Theorem 1 in Section 2. Q.E.D.

THEOREM 12: $E \cap K = Bd(E) \cap K$, and this contains a single point $\bar{z}$ where $(\bar{w} = M\bar{z} + q, \bar{z})$ is the unique solution of the LCP (26).

PROOF: Since M is PD, the LCP (q, M) has a unique solution [20, 22, 25]; and if this solution is $(\bar{w}, \bar{z})$, then $\bar{z}$ is the unique point satisfying (27) and (29). So $Bd(E) \cap K = \{\bar{z}\}$. (27), (28) together imply (29), so $E \cap K = Bd(E) \cap K$. Q.E.D.

Define

$$L = \lceil(1 + \log_2 n + \sum_{i,j} (1 + \log_2(|m_{ij}| + 1)) + \sum_i (1 + \log_2(|q_i| + 1))\rceil$$

$$E_\varepsilon = \{z: \; z^T(Mz + q) \leqq \varepsilon\} \text{ for } \varepsilon > 0$$

$$E_0 = \{z: \; z^T z \leqq 2^{2L}\}.$$

THEOREM 13: If $(\bar{w}, \bar{z})$ is the unique solution of (26), then $(\bar{w}, \bar{z})$ is a BFS of (26), and $\bar{z}$ is an extreme point of K. Also every extreme point z of K other than $\bar{z}$ satisfies $z^T(Mz + q) > 2^{-2L}$.

PROOF: The fact that $(\bar{w}, \bar{z})$ is BFS of (26) is a well known result in linear complimentarity. [5, 16, 21]. This implies that $\bar{z}$ is an extreme point of K.

By the results in [9, 11] at every BFS (w, z) of (26), for each i, either w_i is 0 or $> 2^{-L}$, and similarly either z_i is 0 or $> 2^{-L}$. This implies that at any extreme point z of K, for each i either z_i is 0 or $> 2^{-L}$ and similarly either $M_{i.} z + q_i$ is 0 or $> 2^{-L}$. Since $(\bar{w}, \bar{z})$ is the unique solution of the LCP (26), at every extreme point z of K other than $\bar{z}$, we must have $z^T(Mz + q) = \sum_{i=1}^{n} z_i(M_{i.}z + q_i) > 0$, so we must have at least one i where both $z_i > 0$ and $M_{i.} z + q_i > 0$. Combining these results we conclude that every extreme point z of K other than $\bar{z}$ satisfies $z^T(Mz + q) > 2^{-2L}$. Q.E.D.

THEOREM 14: For ε positive and $\leqq 2^{-2L}$, the n-dimensional volume of $E_0 \cap E_\varepsilon \cap K$ is $\geqq \varepsilon^n 2^{-(3n+1)L}$.

PROOF: Obviously $\bar{z} \varepsilon E_\varepsilon \cap K$, and by Theorem 13, no other extreme point z of K lies in $E_\varepsilon \cap K$ for $0 \leqq \varepsilon \leqq 2^{-2L}$. So for every value of ε in the specified range, every edge of K through $\bar{z}$ intersects E_ε. Also, since K has a nonempty interior by Theorem 11, $E_\varepsilon \cap K$ has a positive n-dimensional volume. K might be unbounded, but by the results in [9, 11], at every extreme point of K, both z_i and $M_i z + q_i$ are $\leqq 2^L/n$ for each i. To the constraints in (27), augment the additional bound constraints that both z_i and $M_i z + q_i$ are $\leqq 2^L/n$ for each i, and let $\hat{K}$ denote the set of feasible solution of (27) together with these bound constraints. By the above facts, every edge of $\hat{K}$ through $\bar{z}$ is either an edge of K (if it is a bounded edge of K), or a portion of an edge of K (if it is an unbounded edge of K). Let $z^1,\dots,z^n$ be adjacent extreme points of $\bar{z}$ in $\hat{K}$ such that $\{\bar{z}, z^1,\dots,z^n\}$ is affinely independent. The above facts imply that all these points $\bar{z}$, z^t, t = 1 to n are in E_0. Define $f(z) = z^T(Mz + q)$. Since M is PD, f(z) is convex. Let $\lambda = \varepsilon\, 2^{-2L}$. So for each t = 1 to n

$$\begin{aligned} f(\bar{z} + \lambda(z^t - \bar{z})) &\leqq (1-\lambda)\, f(\bar{z}) + \lambda f(z^t) \\ &= \lambda\, f(z^t) \\ &= \lambda \sum_{i=1}^{n} z_i^t\, (M_{i.}\, z^t + q_i) \\ &\leqq \lambda \sum_{i=1}^{n} \left(\frac{2^L}{n} \times \frac{2^L}{n} \right) \\ &\leqq \varepsilon\,. \end{aligned}$$

This implies that the line segment $[\bar{z}, \bar{z} + \lambda(z^t - \bar{z})]$ completely lies inside $E_0 \cap E_\varepsilon \cap K$. So the volume of $E_0 \cap E_\varepsilon \cap K$ is

$\geqq$ the volume of the simplex whose vertices are $\bar{z}$, $\bar{z} + \lambda(z^t - \bar{z})$, $t = 1$ to n.

$$= \frac{1}{n!} \left| \text{determinant of } (\lambda(z^1 - \bar{z}) \vdots \ldots \vdots \lambda(z^t - \bar{z})) \right|$$

$$\geqq \lambda^n \, 2^{-(n+1)L}, \quad \text{by the results in [9]}$$

$$\geqq \varepsilon^n \; 2^{-(3n+1)L}$$

Q.E.D.

THEOREM 15: Let $\varepsilon_0 = 2^{-(6L+1)}$. For any point $\hat{z} \in E_0 \cap E_{\varepsilon_0} \cap K$, we have

either $\hat{z}_i \leqq \sqrt{\varepsilon_0} < 2^{-3L}$

or $M_{i.} \hat{z} + q_i \leqq \sqrt{\varepsilon_0} < 2^{-3L}$

PROOF: For any i, if both $\hat{z}_i$ and $M_{i.}\hat{z} + q_i$ are $> \sqrt{\varepsilon_0}$, then $\hat{z}(M\hat{z} + q) > \varepsilon_0$, contradiction to the fact that $\hat{z} \in E_0 \cap E_{\varepsilon_0} \cap K$. Q.E.D.

THEOREM 16: Let $\hat{z}$ be any point in $E_0 \cap E_{\varepsilon_0} \cap K$. Define

$$y_i = w_i \quad \text{if} \quad \hat{z}_i < 2^{-3L}$$

$$= z_i \quad \text{if} \quad \hat{z}_i \geqq 2^{-3L}$$

Then $(y_1, \ldots, y_n)$ is a complementary feasible basis for (26), and the BFS of (26) corresponding to the basic vector $(y_1, \ldots, y_n)$ is $(\bar{w}, \bar{z})$, the solution of the LCP (q, M).

PROOF: Let $J_1 = \{i: \hat{z}_i \geqq 2^{-3L}\}$ and $J_2 = \{i: \hat{z}_i < 2^{-3L}\}$. So $J_1 \cap J_2 = \phi$ and $J_1 \cup J_2 = \{1, 2, \ldots, n\}$. By Theorem 15, $M_{i.}\hat{z} + q_i < 2^{-3L}$ for each $i \varepsilon J_1$.

In [9] P. Gács and L. Lovász proved the following lemma: Consider the system of constraints

$$A_{i.} x \leqq b_i, \quad i = 1 \text{ to } m \tag{30}$$

with integer data, and let ℓ be the size of this system. Suppose $\hat{x}$ is a solution of

$$A_{i.} x \leqq b_i + 2^{-\ell}, \quad i = 1 \text{ to } m$$

such that $A_{i.} \hat{x} \geqq b_i$, $i = 1$ to k, and let $r \leqq k$ be such that $\{A_{1.}, \ldots, A_{r.}\}$ span $\{A_{1.}, \ldots, A_{m.}\}$ linearly. Let $\bar{x}$ be any solution of the system of equations

$$A_{i.} x = b_i, \; i = 1 \text{ to } r.$$

Then $\bar{x}$ is a solution of (30).

We will use this lemma in proving this theorem. Consider the system, where e is a vector of all 1's in R^n,

$$\begin{aligned} -Mz &\leqq q + 2^{-3L} e \\ -z &\leqq 0 + 2^{-3L} e \\ M_{i.}z &\leqq -q_i + 2^{-3L}, \quad \text{for } i \varepsilon J_1 \\ z_i &\leqq 0 + 2^{-3L}, \quad \text{for } i \varepsilon J_2. \end{aligned} \tag{31}$$

We know that $\hat{z}$ solves (31) and in addition $\hat{z}$ also satisfies

$$M_{i\bullet}\hat{z} \geqq -q_i \quad \text{for } i \in J_1$$

$$z_i \geqq 0 \quad \text{for } i \in J_2.$$

Also, since M is PD, the set $\{M_{i\bullet}: i \in J_1\} \cup \{I_{i\bullet}: i \in J_2\}$ linearly spans all the row vectors in the system (31). By using the theorem of P. Gács and L. Lovász mentioned above on this system, we conclude that if $\tilde{z}$ is a solution of the system of equations,

$$\begin{aligned} M_{i\bullet}z &= -q_i \quad \text{for } i \in J_1 \\ z_i &= 0 \quad \text{for } i \in J_2 \end{aligned} \tag{32}$$

then $\tilde{z}$ would be a solution of

$$\begin{aligned} -Mz &\leqq q \\ -z &\leqq 0 \\ M_{i\bullet}z &= -q_i \quad \text{for } i \in J_1 \\ z_i &= 0 \quad \text{for } i \in J_2. \end{aligned} \tag{33}$$

From (33) we know that $M\tilde{z} + q \geqq 0$, $\tilde{z} \geqq 0$ and since $\tilde{z}_i = 0$ for all $i \in J_2$ and $M_{i\bullet}\tilde{z} + q_i = 0$ for all $i \in J_1$ we conclude that $\tilde{z}^T(M\tilde{z} + q) = 0$ (since $J_1 \cap J_2 = \phi$ and $J_1 \cup J_2 = \{1,\ldots,n\}$). So $\tilde{z}$ is a solution of the LCP (q, M). From (32) we notice that $(\tilde{w} = M\tilde{z} + q, \tilde{z})$ is the solution of the system of remaining equality constraints in (26) after setting $w_i = 0$ for $i \in J_1$ and $z_i = 0$ for $i \in J_2$, that is, it is the basic solution of (26) corresponding to the complementary basic vector $y = (y_1,\ldots,y_n)$ defined in the theorem. So y is a complementary feasible basic vector for (26) and the BFS of (26) corresponding to it is the unique solution of the LCP (q, M).

Q.E.D.

THE ALGORITHM

Fix $\varepsilon = \varepsilon_0 = 2^{-(6L+1)}$. For any point $\tilde{z} \in R^n$ and a PD symmetric matrix A, let $E(\tilde{z}, A)$ denote the ellipsoid $\{z: (z - \tilde{z})^T A^{-1} (z - \tilde{z}) \leqq 1\}$ So $E_0 = E(0, 2^{2L} I)$. In this section define $N = 2(n+1)^2(11L+1)$. With $z^0 = 0$, $A_0 = 2^{2L} I$, $E(z^0, A_0)$ go to Step 1.

GENERAL STEP r+1

Let z^r, A_r, $E_r = E(z^r, A_r)$; be respectively the center, PD symmetric matrix, and the ellipsoid at the beginning of this step. If z^r is feasible to (34), (35)

$$\begin{aligned} -Mz - q &\leqq 0 \\ -z &\leqq 0 \end{aligned} \tag{34}$$

$$z^T(Mz + q) \leqq \varepsilon \tag{35}$$

terminate the ellipsoid algorithm, call z^r as $\hat{z}$ and go to the *final step* described below.

If z^r violates at least one of the constraints in (34), (35) select an inequality constraint

$$az \leqq d \tag{36}$$

violated by z^r by the following: If z^r violates (34), take (36) to be the constraint in (34) that z^r violates most. Break ties arbitrarily. If z^r satisfies (34) but violates (35), choose (36) to be the half-space not containing z^r, determined by the tangent plane of E_{ε_0} at its boundary point ξ^r, where ξ^r is the point of intersection of the line segment joining the center of E_{ε_0} and z^r with the boundary of E_{ε_0}.

The center of E_{ε_0} is $z' = -\left(\frac{M+M^T}{2}\right)^{-1}\frac{q}{2}$, and $\xi^r = \lambda z' + (1-\lambda)z^r$ where λ is the positive root of the quadratic equation

$$(\lambda z' + (1-\lambda)z^r)^T(M(\lambda z' + (1-\lambda)z^r) + q) = \varepsilon_0.$$

Now define γ_r, A_{r+1} as in (24) and

$$z^{r+1} = z^r - \left(\frac{1-\gamma_r n}{1+n}\right)\left(\frac{A_r a^T}{\sqrt{aA_r a^T}}\right) \qquad (37)$$

With z^{r+1}, A_{r+1}, $E_{r+1} = E(z^{r+1}, A_{r+1})$, move to the next step in the ellipsoid algorithm.

After at most N steps, this ellipsoid algorithm will terminate with the point z^r in the terminal step lying in $E_0 \cap E_{\varepsilon_0} \cap K$. Then go to the final step described below.

FINAL STEP

Let the center of the ellipsoid in the terminal step be $\hat{z}$. Using $\hat{z}$, find the complementary BFS of (26) as outlined in Theorem 16.

PROOF OF THE ALGORITHM

The updating formulas used in this ellipsoid algorithm are the same as those used in the algorithm of Section 2. Hence using the same arguments as in Section 2, we can verify that $E_r \supset E_0 \cap E_{\xi_0} \cap K$ for all r. The volume of E_0 is $< 2^{2Ln}$. After each step in the ellipsoid algorithm. the volume of the current ellipsoid E_r gets multiplied by a factor of $e^{-(1/2(n+1)}$ or less. So if the ellipsoid algorithm does not terminate even after N steps, the volume of $E_N \leqq (e^{-(n+1)(11L+1)})(2^{2Ln}) < 2^{-L(9n+1)-n}$ contradiction to the fact that $E_N \supset E_0 \cap E_{\varepsilon_0} \cap K$ and Theorem 14. So for some $r \leqq N$, we will have $z^r \in E_0 \cap E_{\varepsilon_0} \cap K$, and in that step the ellipsoid algorithm terminates. Hence the algorithm is obviously polynomially bounded.

Comments made in Section 2 about the precision of computation required, remain valid here also.

4. LCPs ASSOCIATED WITH PSD MATRICES

In this section we consider the LCP (26) where M denotes a given PSD matrix of order n (symmetric or not) with integer entries, and q denotes a given integer column vector in R^n. Let K denote the set of feasible solutions of (27). Since M is only PSD here, K may have an empty interior, and in fact K may even be empty. Let E be defined by (28) and let Bd(E) be defined by (29) as in Section 3. Also let L, E_ε, be as defined in Section 3. Here E, E_ε may not be ellipsoids because M is only PSD. We let $e = (1,\dots,1)^T$ denote the column vector in R^n all of whose entries are 1.

THEOREM 17: In this case the LCP (26) has a solution iff $K \neq \phi$. If $K \neq \phi$, there exists a solution, $(\bar{w}, \bar{z})$, to the LCP (26), which is a BFS of (26), and in this case $\bar{z}$ is an extreme point of K. When $K \neq \phi$, the LCP (26) may have many solutions, but the set of all solutions of (26) is a convex set which is $E \cap K = \mathrm{Bd}(E) \cap K$.

PROOF: Since M is PSD, the fact that (26) has a solution iff $K \neq \phi$ is a standard result in linear complementarity [5, 16, 21]. When $K \neq \phi$, Lemke's complementary pivot algorithm produces a solution, $(\bar{w}, \bar{z})$, to (26), which is a BFS of (26) [5, 16, 21], and obviously if $(\bar{w}, \bar{z})$ is a BFS of (26), $\bar{z}$ is an extreme point of K. The set of all solutions of (26) is obviously $\mathrm{Bd}(E) \cap K$, and from the definition of K (from (27)) and E(from (28)) it is clear that in this case $\mathrm{Bd}(E) \cap K = E \cap K$, and since both E and K are convex sets (E is convex because M is PSD), this set is convex. Q.E.D.

In this section we define E_0 to be

$$E_0 = \{z: z^T z \leqq 2^{2(L+1)}\} \tag{38}$$

THEOREM 18: When $K \neq \phi$, $E_0 \cap E_\varepsilon \cap K$ contains all the extreme points z of K such that $(w = Mz + q, z)$ is a solution of (26).

PROOF: By the results in [9, 11] if $(\bar{w}, \bar{z})$ is a solution of (26) which is a BFS, then $\bar{z} \varepsilon E_0$. The rest follows from Theorem 17. Q.E.D.

In this case $E_0 \cap E_\varepsilon \cap K$ may not contain all the z which lead to solutions of (26), Theorem 18 only guarantees that $E_0 \cap E_\varepsilon \cap K$ contains all the z which are extreme points of K that lead to solutions of (26). Since M is PSD, the LCP (q, M) may have solutions which are ray solutions, and if so, the set of solutions of (26) may in fact be unbounded and hence all of it may not lie in E_0.

THEOREM 19: If z_i is positive in some solution of (26), then its complement w_i is zero in all solutions of (26). Similarly if w_i is positive in some solutions of (26), then z_i is zero in all solutions of (26).

PROOF: By Theorem 17, the set of all solutions of (26) is a convex set. So if (w^1, z^1), (w^2, z^2) are two solutions of (26) satisfying the properties that $z_i^1 > 0$ and $w_i^2 > 0$, then other points on the line segment joining (w^1, z^1), (w^2, z^2) cannot be solutions of (26) (because they violate the complementarity constraint $w_i z_i = 0$ in (26)) contradicting the fact that the set of solutions of (26) is a convex set. Q.E.D.

THEOREM 20: If $\bar{z}$ is an extreme point of K that leads to a solution of (26), then for each i either $\bar{z}_i = 0$ or $2^{-L} \leqq \bar{z}_i \leqq 2^L/n$. Also either $M_{i.}\bar{z} + q_i$ is zero or $2^{-L} \leqq M_{i.}\bar{z} + q_i \leqq 2^L/n$. Also at every extreme point of z of K that does not lead to a solution of (26), we will have $z^T(Mz + q) > 2^{-2L}$.

PROOF: Similar to the proof of Theorem 13 in Section 3. Q.E.D.

THEOREM 21: $K \neq \phi$ iff the set of solutions of

$$\begin{aligned} Mz + q &\geqq -2^{-10L} e \\ z &\geqq -2^{-10L} e \end{aligned} \tag{39}$$

has a nonempty interior.

PROOF: By the results in [9], (39) is feasible if and only if $K \neq \phi$. Also any point in K is an interior point of the set of feasible solutions of (39). Q.E.D.

Let K_1 denote the set of feasible solutions of (39).

THEOREM 22: Let $\varepsilon_0 = 2^{-(6L+1)}$. For any point $\hat{z} \varepsilon E_0 \cap E_{\varepsilon_0} \cap K_1$, we have for each i = 1 to n,

$$\text{either} \quad \hat{z}_i < 2^{-3L}$$

$$\text{or} \quad M_{i.}\hat{z} + q_i < 2^{-3L}$$

PROOF: Suppose that $\hat{z}_i \geqq 2^{-3L}$ and $M_{i.}\hat{z} + q_i \geqq 2^{-3L}$. Since $\hat{z} \varepsilon E_{\varepsilon_0}$, $\hat{z}^T(M\hat{z} + q) \leqq 2^{-(6L+1)}$. Then we have

$$\begin{aligned} \sum_{\substack{t=1 \\ \neq i}}^{n} \hat{z}_t(M_{t.} \hat{z} + q_t) &\leqq 2^{-(6L+1)} - 2^{-6L} \\ &\leqq -2^{-(6L+1)} \end{aligned}$$

But from (39) and the definition of E_0,

$$\begin{aligned} \sum_{\substack{t=1 \\ \neq i}}^{n} \hat{z}_t (M_t \hat{z} + q_t) &\geqq -(n-1)\, 2^{-10L} (2^{2L+1} + 2^L) \\ &> -2^{-(6L+1)} \end{aligned}$$

a contradiction. Q.E.D.

THEOREM 23: Let $\varepsilon_0 = 2^{-(6L+1)}$. If $K \neq \phi$, the n-dimensional volume of $E_0 \cap E_{\varepsilon_0} \cap K_1$ is $\geqq 2^{-11nL}$.

PROOF: Assume $K \neq \phi$. So by earlier results (26) has a solution. Let $(\bar{w}, \bar{z})$ be a complementary BFS of (26). So by Theorem 17, $\bar{z} \in Bd(E) \cap K$. Define the hypercube C_λ (for $\lambda > 0$)

$$C_\lambda = \{z: z \in R^n, |z_j - \bar{z}_j| \leqq \lambda/2 \quad \text{for all } j = 1 \text{ to } n\}.$$

Then, clearly, the n-dimensional volume of C_λ is λ^n. We will now prove that $C_\lambda \subset K_1 \cap E_0 \cap E_{\varepsilon_0}$ for $\lambda \leqq 2^{-11L}$. Since the radius of E_0 is 2^{L+1}, $C_\lambda \subset E_0$ by the definition C_λ and the fact that $||\bar{z}|| < 2^L$ from Theorem 20. Let $\hat{z}$ be any point in C_λ. Since $\bar{z}_i \geqq 0$, $M_{i.}\,\bar{z} + q_i \geqq 0$ for all $i = 1$ to n, we have

$$\hat{z}_i \geqq \bar{z}_i - \lambda/2 \geqq -\lambda/2 \geqq -2^{-10L}$$

$$M_{i.}\hat{z} + q_i \geqq M_{i.}\bar{z} + q_i - (\lambda/2)\left(\sum_{j=1}^{n} |m_{ij}|\right)$$

$$\geqq -2^{-(11L+1)} \times 2^L \geqq -2^{-10L}$$

So $C_\lambda \subset K_1$. Also, since $\bar{z}^T(M\bar{z} + q) = 0$ (since $(\bar{w} = M\bar{z} + q, \bar{z})$ solves (26)), we have

$$\hat{z}^T(M\hat{z}+q) = (\hat{z}-\bar{z})^T (M\bar{z}+q+M^T\bar{z}) + (\hat{z}-\bar{z})^T M(\hat{z}-\bar{z})$$

$$\leqq (\lambda/2)\, n(2^L+2^L\, 2^L) + (\lambda/2)^2 \sum_{i,j} |m_{ij}|$$

$$\leqq 2^{-(11L+1)}\, n\, 2^{2L+2} + n^2\, 2^{L-2(11L+1)}$$

$$\leqq \varepsilon_0$$

This implies that $C_\lambda \subset E_{\varepsilon_0}$. Hence $C_\lambda \subset K_1 \cap E_0 \cap E_{\varepsilon_0}$. Now letting $\lambda = 2^{-11L}$, the volume of C_λ is 2^{-11nL}, and these facts imply the theorem. Q.E.D.

Let $\hat{z}$ be any point in $E_0 \cap E_{\varepsilon_0} \cap K_1$. Define

$$J_1^- = \{i: M_{i\cdot}\hat{z} + q_i \leqq 0\}$$

$$J_1^+ = \{i: 0 < M_{i\cdot}\hat{z} + q_i < 2^{-3L}\}$$

$$J_2^- = \{i: \hat{z}_i \leqq 0\}$$

$$J_2^+ = \{i: 0 < \hat{z}_i < 2^{-3L}\}.$$

Then by Theorem 22,

$$J_1^- \cup J_1^+ \cup J_2^- \cup J_2^+ = \{1,\ldots,n\}. \quad (40)$$

Furthermore, $\hat{z}$ is a solution of

$$\begin{aligned} -Mz &\leqq q + 2^{-3L}e \\ -z &\leqq 2^{-3L}e \\ M_{i\cdot}z &\leqq -q_i + 2^{-3L}, \text{ for } i \in J_1^+ \\ z_i &\leqq 2^{-3L}, \quad \text{for } i \in J_2^+ \end{aligned} \quad (41)$$

THEOREM 24: Let $\hat{z}$ be any point in $E_0 \cap E_{\varepsilon_0} \cap K_1$. Let I be the unit matrix of order n. In [9] P. Gács and L. Lovász describe a constructive procedure for obtaining a new solution, which we will denote by the same symbol $\hat{z}$, such that if J_1^-, J_1^+, J_2^-, J_2^+ are the index sets corresponding to this new $\hat{z}$, then the new $\hat{z}$ also satisfies (41), and there exists a linearly independent subset D of row vectors.

$$D \subset \{M_{i.} : i \in J_1^- \cup J_1^+\} \cup \{I_{i.} : i \in J_2^- \cup J_2^+\}$$

such that D spans linearly $\{M_{i.} : i = 1 \text{ to } n\} \cup \{I_{i.} : i = 1 \text{ to } n\}$. Furthermore, if $\bar{z}$ is a solution of

$$-M_{i.}z = q_i, \text{ for } i \text{ such that } M_{i.} \in D$$

$$z_i = 0 \quad \text{for } i \text{ such that } I_{i.} \in D$$

then $(\bar{w} = M\bar{z} + q, \bar{z})$ is a solution of (26).

PROOF: This theorem follows from the results of P. Gács and L. Lovász in [9], applied on (41). We know that $\hat{z}$ satisfies

$$- M_{i.}\hat{z} \geqq q_i, \quad \text{for } i \in J_1^-$$

$$M_{i.}\hat{z} \geqq -q_i, \quad \text{for } i \in J_1^+$$

$$- \hat{z}_i \geqq 0, \quad \text{for } i \in J_2^-$$

$$\hat{z}_i \geqq 0, \quad \text{for } i \in J_2^+.$$

By the results in [9], $\bar{z}$ is a solution of

$$- Mz \leqq q$$

$$-z \leqq 0$$

Furthermore, $\bar{z}$ satisfies

$$M_{i.}\bar{z} = -q_i, \quad \text{for } i \in J_1^- \cup J_1^+$$

$$\bar{z}_i = 0, \quad \text{for } i \in J_2^- \cup J_2^+$$

by the spanning property of D and the results in [9]. By (40), this implies that at least one of $\bar{w}_i$ or $\bar{z}_i$ is zero for each i = 1 to n. All these facts together clearly imply that $(\bar{w}, \bar{z})$ is a solution of the LCP (26). Q.E.D.

THE ALGORITHM

Apply the ellipsoid algorithm discussed in Section 3, to get a point $\hat{z}$ in $E_0 \cap E_{\varepsilon_0} \cap K_1$, initiating the algorithm with $z^0 = 0$, $A_0 = 2^{2(L+1)}I$, $E_0 = E(z^0, A_0)$. The volume of E_0 here is $< 2^{2n(L+1)}$, and if $K \neq \phi$, the volume of $E_0 \cap E_{\varepsilon_0} \cap K_1$ is $> 2^{-11nL}$ by Theorem 23. Hence if $K \neq \phi$, this ellipsoid algorithm will terminate in at most $2(n+1)^2$ (13L+1) steps with a point $\hat{z} \in E_0 \cap E_{\varepsilon_0} \cap K_1$. So, if the ellipsoid algorithm did not find a point in $E_0 \cap E_{\varepsilon_0} \cap K_1$ even after $2(n+1)^2(13L+1)$, we can conclude that $K = \phi$, that is, that the LCP (26) has no solution. On the other hand, if a point $\hat{z}$ in $E_0 \cap E_{\varepsilon_0} \cap K_1$ is obtained in the ellipsoid algorithm, then using it, obtain a solution $(\bar{w}, \bar{z})$ of the LCP (26) as discussed in Theorem 24.

5. OTHER LCPs

The ellipsoid algorithms discussed in Sections 2, 3, 4 can only process LCPs associated with PSD matrices (the class of these LCPs is equivalent to the class of convex quadratic programs). There are other polynomially bounded algorithms for other special classes of LCPs. One prime example of this is the very efficient $O(n^3)$ algorithm of R. Chandrasekharan and R. Saigal [2, 24] for processing LCPs associated with z-matrices. Also in [6, 19] it was shown that LCPs satisfying certain properties can be solved as linear programs, and these LCPs are therefore polynomially solvable using Shor-Khachiyan's ellipsoid algorithm [9, 11] on the resulting linear program.

For the general LCP, the prospects of finding a polynomially bounded algorithm are not very promising, in view of the result in [3] where it is shown that this problem is NP-complete. Let $a_1,\ldots,a_n$, b be positive integers and let $\tilde{M}_{n+2}$ and $\tilde{q}(n+2)$ be the following matrices

$$\tilde{M}_{n+2} = \left(\begin{array}{c|cc} -I_n & 0 & 0 \\ \hline e_n^T & -n & 0 \\ -e_n^T & 0 & -n \end{array}\right) \qquad \tilde{q}(n+2) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \\ -b \\ b \end{pmatrix}$$

where I_n denotes the unit matrix of order n, and e_n is the column vector in R^n all of whose entries are 1. Also consider the 0-1 equality constraint Knapsack feasibility problem

$$\sum_{i=1}^{n} a_i x_i = b \qquad (42)$$

$$x_i = 0 \text{ or } 1 \quad \text{for all } i = 1 \text{ to } n.$$

In [3], the following result was proved: If $(\tilde{w}, \tilde{z})$ is a solution of the LCP $(\tilde{q}(n+2), \tilde{M}_{n+2})$; define $\tilde{x}_i = \tilde{z}_i/a_i$, for i = 1 to n; then $\tilde{x} = (\tilde{x}_1,\dots,\tilde{x}_n)^T$ is a solution of (42). Conversely if $\hat{x} = (\hat{x}_1,\dots,\hat{x}_n)^T$ is a solution of (42); define $\hat{w}_{n+1} = \hat{z}_{n+1} = \hat{w}_{n+2} = \hat{z}_{n+2} = 0$, and $\hat{z}_i = a_i\,\hat{x}_i$, $\hat{w}_i = a_i(1 - \hat{x}_i$ i = 1 to n; then $(\hat{w} = (\hat{w}_1,\dots,\hat{w}_{n+2}), \hat{z} = (\hat{z}_1,\dots,\hat{z}_{n+2}))$ is a solution of the LCP $(\tilde{q}(n+2), \tilde{M}_{n+2})$. Since (42) is a well known NP-complete problem, this shows that the LCP $(\tilde{q}_{n+2}, \tilde{M}_{n+2})$ is NP-complete. One can clearly verify that the matrix $\tilde{M}_{n+2}$ is ND. This shows that even the LCPs associated with ND matrices are NP-complete.

Let M be a given ND matrix with integer entries, and let $q \in R^n$ be a given integer column vector. In this case the LCP (q, M) may not have a solution; and even if it does, the solution may not be unique. From the results in [20] we do know that the number of distinct solutions of the LCP (q, M) in this case is finite. Let K be the set of feasible solutions of

$$\begin{aligned} z &\geqq 0 \\ Mz + q &\geqq 0 \end{aligned} \tag{43}$$

and let E be the ellipsoid

$$z^T(Mz + q) \geqq 0. \tag{44}$$

Since M is ND, the inequality (44) defines an ellipsoid in R^n. Let Bd(E) be the boundary of E.

Clearly any point $z \in Bd(E) \cap K$ satisfies the property that $(w = Mz + q, z)$ is a solution of the LCP (q, M) and vice versa. So solving the LCP (q, M) is equivalent to the problem of finding a point

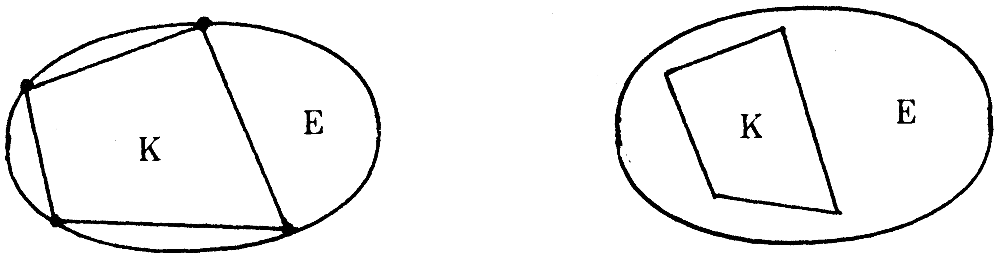

Figure 4: When M is ND, E and K may be as in one of the figures given here. Points of K on the boundary of E, if any, lead to solutions of the LCP(q, M).

in Bd(E) $\cap$ K. However, in this case, from (43), (44) we notice that $K \subset E$, and in general, $Bd(E) \cap K \subsetneq E \cap K$. See Figure 4. So the nice property that $E \cap K = Bd(E) \cap K$ which held for LCPs associated with PSD matrices does not hold here anymore, which makes the LCP associated with an ND matrix much harder. In this case (i.e., with M being ND), it is possible to find a point in $E \cap K$ using an ellipsoid algorithm (actually since $K \subset E$ here, a point in K can be found by the Shor-Khachiyan algorithm of [9, 11], and that point will also lie in E), but the point in $E \cap K$ obtained by the algorithm may not be on the boundary of E, and hence may not lead to a solution of the LCP (q, M). In fact, finding a point in Bd(E) $\cap$ K is a concave minimization problem, and that's why it is NP-complete.

The status of the LCPs (q, M) where M is a P but not a PSD matrix, is unresolved. In this case the LCP(q, M) is known to have a unique solution [20, 25], but the sets $\{z: z^T(Mz + q) \leqq 0\}$ or $\{z: z^T(Mz + q) \geqq 0\}$ are not ellipsoids. The interesting question is whether a polynomially bounded algorithm exists for solving this special class of LCPs. This still remains an open question. It is also not known whether these LCPs are NP-complete.

REFERENCES

1. I. Adler, R. P. McClean and J. S. Provan, "An Application of the Khachiyan-Shor Algorithm to a Class of Linear Complementarity Problems", Cowles Foundation discussion paper No. 549, Cowles Foundation for research in Economics, Yale University, Box 2125, Yale Station, New Haven, Connecticut 06520.

2. R. Chandrasekharan, "A Special Class of the Complementary Pivot Problem", *OPSEARCH,* 7, pp. 263-268, 1970.

3. S. J. Chung, "The Linear Complementarity Problem is NP-Complete", to appear in *Mathematical Programming.*

4. S. J. Chung and K. G. Murty, "A Polynomially Bounded Algorithm for Positive Definite Symmetric LCPs", Technical Report 79-10, Department of Industrial and Operations Engineering, The University of Michigan, Ann Arbor, Michigan 48109, December 1979.

5. R. W. Cottle and G. B. Dantzig, "Complementary Pivot Theory of Mathematical Programming", *Linear Algebra and its Applications,* 1, pp. 103-125, 1968.

6. R. W. Cottle and J. S. Pang, "On Solving Linear Complementarity Problems as Linear Programs", pp. 88-107 in *Mathematical Programming Study 7,* 1978.

7. Y. Fathi, "Comparative Study of the Ellipsoid Algorithm and Other Algorithms for the Nearest Point Problem", Department of Industrial and Operations Engineering, The University of Michigan, Ann Arbor, Michigan 48109, USA, June 1980.

8. Y. Fathi and K. G. Murty, "The Nearest Point Problem", Technical Report No. 79-7, Department of Industrial and Operations Engineering, The University of Michigan, Ann Arbor, Michigan 48109, U.S.A., 1979.

9. P. Gács and L. Lovász, "Khachiyan's Algorithm for Linear Programming", Computer Science Department, Stanford University, August 1979.

10. D. Goldfard and M. J. Todd, "Modificiation and Implementation of the Shor-Khachiyan Algorithm for Linear Programming", Technical Report No. 446, School of Operations Research and Industrial Engineering, College of Engineering, Cornell University, Ithaca, New York, January 1980.

11. L. G. Hacijan, "A Polynomial Algorithm in Linear Programming", *Soviet Math. Dokl.,* No. 1, 20, pp. 191-194, 1979.

12. P.C. Jones and E. S. Marwil, "Solving Linear Complementarity Problems with Khachiyan's Algorithm", E. G. & G. Idaho, Inc., P. O. B. 1625, Idaho Falls, Idaho 83415, January 1980.

13. I. Kaneko, "Piecewise Linear Elastic-Plastic Analysis", *International Journal for Numerical Methods in Engineering,* 14, 5, pp. 757-767, 1979.

14. M. K. Kozlov, S. P. Tarasov and L. G. Hachijan, "Polynomial Solvability of Convex Quadratic Programming", *Soviet Mathematics Doklady,* 20, 1979, No. 5.

15. K. K. Kubota, Private Communication.

16. C. E. Lemke, "Bimatrix Equilibrium Points and Mathematical Programming", *Management Science,* 11, pp. 681-689, 1965.

17. C. E. Lemke, and J. T. Howson, "Equilibrium Points of Bimatrix Games", *SIAM Journal of Applied Mathematics,* 12, pp. 413-423, 1964.

18. O. L. Mangasarian, *Nonlinear Programming,* McGraw-Hill, 1969.

19. O. L. Mangasarian, "Simplified Characterizations of Linear Complementarity Problems Solvable as Linear Programs", *Mathematics of Operations Research,* 4, pp. 268-273, 1979.

20. K. G. Murty, "On the Number of Solutions of the Complementarity Problem and Spanning Properties of Complementary Cones", *Linear Algebra and its Applications,* 5, pp. 65-108, 1972.

21. K. G. Murty, Chapter 16 in *Linear and Combinatorial Programming,* Wiley, 1976.

22. K. G. Murty, "On the Linear Complementarity Problem", pp. 425-439 in Band 31, "Continuous Optimization" of *Proceedings of the Third Symposium on Operations Research,* Universitat Mannheim, Sept. 6-8, 1978, Edited by W. Oettli and F. Steffens, published by Verlagrgruppe, Athenaum/Hain/Scriptor/Hanstein.

23. J. S. Pang, I. Kaneko and W. P. Hallman, "On the Solution of Some (Parametric) Linear Complementarity Problems with Applications to Portfolio Selection, Structural Engineering and Acturial Graduation", *Mathematical Programming,* 16, 3, pp. 325-347, May 1979.

24. R. Saigal, "A Note on a Special Linear Complementarity Problem", *OPRESEARCH,* 7, 3, pp. 175-183, September 1970.

25. H. Samuelson, R. M. Thrall and O. Wesler, "A Partition Theorem for Euclidean n-space", *Proceedings of American Mathematical Society,* 9, pp. 805-807, 1958.

26. N. Z. Shor, "Convergence Rate of the Gradient Descent Method with Dilation of the Space", *Kibernetika* 6 (No. 2, March-April 1970), translated in *Cybernetics*, 6, pp. 102-108, 1970.

27. P. Wolfe, "Finding the Nearest Point in a Polytope", IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598. Revised, January 1976.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
79-10

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
"Polynomially Bounded Ellipsoid Algorithms for Convex Quadratic Programming."

5. TYPE OF REPORT & PERIOD COVERED
Technical research report.

6. PERFORMING ORG. REPORT NUMBER
79-10

7. AUTHOR(s)
S. J. Chung and K. G. Murty

8. CONTRACT OR GRANT NUMBER(s)
Grant AFOSR 78-3646

9. PERFORMING ORGANIZATION NAME AND ADDRESS
University of Michigan
Ann Arbor, Michigan 48109, U.S.A.

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Directorate of Mathematical & Information Sciences
Department of the Air Force, Air Force Office of Scientific Research (AFSC), Bolling Air Force Base
Washington, D.C. 20332

12. REPORT DATE
June, 1980

13. NUMBER OF PAGES
47

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

15. SECURITY CLASS. (of this report)

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Unlimited.

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

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Convex quadratic programming, linear complementarity problem, nearest point problem, positive semi-definite matrix, ellipsoid algorithm, polynomially bounded algorithm.

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)
We show that the ellipsoid algorithm of N. F. Shor and L. G. Khachiyan, can be applied to solve convex quadratic programming problems with integer data in polynomially bounded time.

DD FORM 1 JAN 73 1473

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

SECURITY CLASSIFICATION OF THIS PAGE(*When Data Entered*)

SECURITY CLASSIFICATION OF THIS PAGE(*When Data Entered*)