LINEAR PROGRAMMING AND EXTENSIONS

R. Chandrasekaran
The University of Texas at Dallas

May 22, 2000

0.1 Ellipsoid Algorithm I:

Here we describe an algorithm for LP shown to work in polynomial time for the first time. We will begin first with the problem considered by L.G. Khachiyan as reported by Lovasz and Gacs.

Algorithm I:

Input:

$$I : [a^i x < b_i; 1 \leq i \leq m]$$
$$a^i \in \mathbf{Z}^n; b_i \in \mathbf{Z}; 1 \leq i \leq m.$$

Output: A solution $x \in \mathbf{Q}^n$ to I if one exists or an indication no such solution exists.

Definition 1 $L = \sum_{ij} \log(|a^i_j| + 1) + \sum_i \log(|b_i| + 1) + \log(nm) + 1.$

This is the *space* required to state the problem in binary encoding of all data.

Step 0: Set $x^0 = 0$; $A^0 = 2^L I$; $k = 0$; go to step 1.

Step 1: If x^k solves I, stop; if $k > 2(n+1)(2nL + n + L)$, stop with the statement "I is infeasible". If not, let $a^i x^k \geq b_i$ be a violated constraint in I. Define:

$$x^{k+1} = x^k - \tfrac{1}{n+1} \frac{A^k a^i}{\sqrt{(a^i A^k a^i}}$$
$$A^{k+1} = (\tfrac{n^2}{n^2-1}) \left(A^k - \tfrac{2}{n+1} \frac{(A^k a^i)(A^k a^i)^t}{a^i A^k a^i}\right)$$

and go to step 1.

Main Results:

Theorem 1 *The above algorithm "works".*

Lemma 2 *Every vertex of the polyhedron* $\{x : a^i x \leq b_i; 1 \leq i \leq m; x \geq 0\}$ *has coordinates that are rational numbers with numerator and denominator at most* $\frac{2^L}{nm}$*; also* $\|v\| < \frac{2^L}{m}$ *for all vertices of this polyhedron.*

Lemma 3 *If I has solutions, then the volume of solutions inside the sphere* $\{x : \|x\| < 2^L\}$ *is at least* $2^{-(n+1)L}$.

Lemma 4 *The system* $a^i x < b_i + 2^{-L}; 1 \leq i \leq m$ *has a solution iff the system* $a^i x \leq b_i; 1 \leq i \leq m$ *has a solution; moreover, a solution of one can be found from that of the other in polynomial time.*

Given a positive definite matrix A^0 and a point x^0, let the ellipsoid E be given by $E = \{y : (y - x^0)^t (A^0)^{-1} (y - x^0) \leq 1\}$. Let $a \neq 0 \in \mathbf{R}^n$. The sets $\frac{1}{2}E_a = E \cap \{x : (x - x^0)^t a \leq 0\}$ and $E^a = \{y : (y - x^1)^t (A^1)^{-1} (y - x^1) \leq 1\}$ satisfy:

Lemma 5 $\frac{1}{2}E_a \subset E^a$.

Lemma 6 *Let $\lambda(E)$ denote the volume of ellipsoid E. Then, $\lambda(E^a) = c(n)\lambda(E)$ where*

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

These lemmas are used to prove the theorem. We will show each of these in detail first and then use this to show how LP is solved.

0.1.1 Proofs:

Lemma 1: Let $v = (v_1, v_2, ..., v_n)$ be a vertex of $\{x : x \geq 0; a^i x \leq b_i; 1 \leq i \leq m\}$. By Cramer's rule, each v_i can be expressed as a ratio of determinants D_i and D whose entries are $0, 1, a^i_j$, or b_i.

Claim 1 $|D| < \frac{2^L}{nm}$*, and the same holds for D_i. This would imply the lemma.*

Proof: D is the sum of $m!$ terms each of which is a product of entries of D. Hence:

$$|D| \leq \sum_{m!\ terms} |\text{each term}|$$
$$\leq \prod_i \sum_j |d_{ij}| \leq \prod_i \prod_j (|d_{ij}| + 1) < \frac{2^L}{nm}$$

Lemma 2:

Claim 2 : *We may assume that I has a solution $x^0 > 0$.*

Proof: Let x^0 be a solution; if some components are negative, multiply those elements of the matrix by -1, and to the new system, we get a new solution with these components positive. *Note that this does not change the volume or L.* Thus, we may assume that $x^0 \geq 0$. But I is a strict inequality system; hence, we may assume that $x^0 > 0$ as claimed.

Thus, the polyhedron $\{x : x \geq 0; a^i x \leq b_i; 1 \leq i \leq m\}$ has an interior point (*a point that satisfies all inequalities as strict inequalities*). Since the polyhedron has no line, it has an extreme point, say v. By lemma 1, $v_i < \frac{2^L}{nm}$. Hence, the polyhedron above has an interior point x with $x < \frac{2^L}{nm} e$ and, hence, the polytope $\{x : x \geq 0; a^i x \leq b_i; x \leq \frac{2^L}{nm} e\}$ has an interior point. Hence, this last system has $n+1$ vertices not all in the same plane. This set has a volume equal at least that of the simplex $\{v^0, v^1, ..., v^n\}$ given by $\frac{1}{n!} \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ v^0 & v^1 & \cdots & v^n \end{bmatrix}$. By lemma 1, $v^i = \frac{u^i}{D_i}$ where u^i is an integral vector and D_i is integer number $< \frac{2^L}{nm}$. Hence, the volume $\lambda(S)$ of the simplex above satisfies:

$$\begin{aligned} \lambda(S) &\geq \frac{1}{n!} \frac{1}{\prod_{i=0}^{n} |D_i|} \left| \det \begin{bmatrix} D_0 & D_1 & \cdots & D_n \\ u^0 & u^1 & \cdots & u^n \end{bmatrix} \right| \\ &\geq \frac{1}{n!} \frac{n^{n+1}}{2^{(n+1)L}} \geq 2^{-(n+1)L} \end{aligned}$$

Thus, we have shown that the volume of solutions inside the cube $\{x : |x_j| < \frac{2^L}{nm}\}$ is at least $2^{-(n+1)L}$. This cube is entirely contained in the sphere for $n > 2$.

Ellipsoids:

Definition 2 *An ellipsoid is the image under a linear transformation of a sphere. Every linear transformation can be broken down into three fundamental ones: (i)translation; (ii)rotation; and (iii)dilation of axes. Translation is of the form: $x \mapsto x + a$ for a fixed a. Rotation is of the form: $x \mapsto Rx$ where R is an orthonormal matrix. (A matrix R is orthonormal if $R^t R = I$). The name arises from the fact the columns (and rows) of such a matrix are orthogonal to each other and the length of each is* 1*. Orthonormal transformations preserve distance, i.e., $d(x, y) = d(Rx, Ry) \; \forall \; x, y$. Dilation is of the form: $x \mapsto \Omega x$ where Ω is a diagonal matrix with nonnegative entries on the diagonal (usually positive). This is equivalent to scaling of variables. Thus, translation changes only the center of the sphere; rotation does not change the center, but spins the sphere to produce a new sphere which is the same as the old one. It is dilation that changes the shape of a sphere to that of an ellipsoid. If Ω has a zero on the diagonal, it is singular; then it collapses the sphere to a lower dimensional ellipsoid. Hence, if the ellipsoid is to have volume, then Ω must be nonsingular. We now state these facts algebraically.*

Definition 3 *Given a nonsingular matrix Q and a point x^0, the set*

$$E = \{y : y = Qz + x^0; \|z\| \leq 1\}$$

is an ellipsoid whose center is x^0.

Definition 4 *A matrix A is positive definite (positive semi-definite) if*

$$x^t Ax > 0 \, \forall \, x \neq 0 \; (\geq 0 \, \forall \, x)$$

Lemma 7 *Given an ellipsoid $E = (Q, x^0)$, $\exists$ a symmetric positive definite matrix $\ni E = \{y : (y - x^0)^t A^{-1}(y - x^0) \leq 1\}$.*

Proof: Take $A = QQ^t$.

Lemma 8 *Given a positive definite symmetric matrix A and a point x^0, the set $E = \{y : (y - x^0)^t A^{-1}(y - x^0) \leq 1\}$ is an ellipsoid with center x^0.*

Proof: A matrix of the above type can be factored and written as $A = QQ^t$ for some nonsingular Q. This process is sometimes called "*completion of squares*" and is most often done on the quadratic form $x^t A^1 x$ as described below:

$x^t A^1 x = \sum_i \sum_j a^1_{ij} x_i x_j = (v^1)^t A^2 v^1$ where $v^1 = E^1 x$ with $E^1_{1.} = [A^1_{1.}/a^1_{11}]$ and E^1 is an elementary matrix with the first row different from that of I. $A^2 = ((E^1)^{-1})^t A^1 (E^1)^{-1}$ with $A^2_{1.} = a_{11} e_1 = (A^2_{.1})^t$. If A^1 is positive definite then so is A^2. Repeating the process we can write $x^t A^1 x = v^t (S^{-1})^t A^1 S^{-1} v$ where $v = Sx$ and $S = E^n .....E^1$. $(S^{-1})^t A^1 S^{-1}$ is a diagonal matrix D with positive diagonal elements. $\sqrt{D}$ has the obvious connotation and $A^1 = S^t DS = S^t \sqrt{D}.\sqrt{D}.S = QQ^t$ where $Q = S^t \sqrt{D}$. *Note that this also shows that if during this process we get a negative element on the diagonal that the original matrix is not positive definite and there is a vector to show that it is not. In this case D has negative elements on the diagonal and hence v can be taken to be a unit vector to show that A^1 is not positive definite. Of course the square root operation need not be done exactly.*

Lemma 9 *Given an ellipsoid $E = (Q, x^0)$, a nonsingular matrix P and a point p^0, the map $x \mapsto Px + p^0$, the image of E is an ellipsoid.*

Proof: The image of E is $E' = (PQ, \; Px^0 + p^0)$. Thus, the set of ellipsoids is a family of geometric objects closed under linear transformations. There are, of course, other families of geometric objects having this property, and they can be (and have been) used for such algorithms.

0.1.2 Volumes:

Here we establish the volumes of simple bodies and how volume of a body changes under linear transformations. Geometrically, translations and rotations do not affect the volume. Dilations do by a factor equivalent to the determinant of the matrix. We will show that any linear transformation can be decomposed into a series of simple transformations.

Lemma 10 *Let Q be a nonsingular matrix. Then Q is a product of matrices of the form:*

$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ x & \cdots & \cdots & 1 & \cdots & \cdots & x \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix} \textit{ and } \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ & & \cdots & \alpha^i & \cdots & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

where $\alpha^i \neq 0$ and x can be any number; blank spaces are zeroes. Then, $\det\ Q =$ *product of the α's.*

Proof: By "product form," we know that Q is a product of "elementary" matrices of the form:

$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \beta & \cdots & \cdots & \alpha & \cdots & \cdots & \gamma \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

where $\alpha \neq 0$; but this is the product of:

$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \beta & \cdots & \cdots & 1 & \cdots & \cdots & \gamma \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ & & & \alpha & & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

and hence the result.

Lemma 11 *Consider the map:* $x \mapsto (x_1 + \sum_{i=2}^{n} \alpha_i x_i, x_2, ..., x_n)$. *(This corresponds to the first of the above two types of matrices.) Let* C *be the unit cube* $\{x : 0 \leq x_i \leq 1\}$ *and let* $K(C)$ *be its image under this transformation. Then, vol*$(K(C)) = 1$.

Proof: $\mathrm{vol}(K(C) = \int_0^1 dy_n ... \int_0^1 dy_2 \int_{\sum_{i=2}^{n} \alpha_i y_i}^{1+\sum_{i=2}^{n} \alpha_i y_i} dy_1 = 1$

Lemma 12 *Consider the map:* $x \mapsto (x_1, x_2, ..., \alpha x_i, ..., x_n)$. *(We will assume that* $\alpha \neq 0$*.) Let* $S(C)$ *be the image of the cube* C *defined as before. vol*$(S(C)) = |\alpha|$.

Proof: $S(c) = \{y : 0 \leq y_j \leq 1 \ \forall \ j \neq i; 0 \leq |\frac{y_i}{\alpha}| \leq 1\}$. The lemma follows by integration. Please note that this is the second type transformation mentioned above.

Lemma 13 *Let* Q *be a nonsingular matrix and* x^0 *be a point, and* S *be a set and* $I(S)$ *be its image under the transformation:* $x \mapsto Qx + x^0$. *Then, vol*$(I(S)) = |\det Q|$*vol*(S).

Proof: Follows from the previous lemmas.

0.1.3 Orthonormal Matrices & Gram — Schmidt Process:

Lemma 14 $R^t R = I \implies \|y - x\| = \|Ry - Rx\| \ \forall \ x$ *and* y *(Please note that the converse is also true). In particular* $\|Rz\| \leq 1 \iff \|z\| \leq 1$ *if* R *is orthonormal.*

Lemma 15 *Given a vector* $a \neq 0$*,* $\exists$ *orthonormal* $R \ni Ra = \|a\| e_1$.

Proof: Given any set of linearly independent vectors $[a^1, a^2, ..., a^n]$ in $\mathbf{R}^n$, we construct an orthonormal matrix R with $Ra^1 = \|a^1\| e_1$ by the Gram — Schmidt "orthogonalization" process described below:

Let $u^1 = \frac{a^1}{\|a^1\|}; v^k = a^k - \sum_{i=1}^{k-1} ((u^i)^t a^k) u^i$; and $u^k = \frac{v^k}{\|v^k\|}$ for $k \geq 2$. Let $R^t = [u^1, u^2, ..., u^n]$. This is the required R. In the lemma, we have $a^1 = a \neq 0$; so we can choose the remaining a's to be unit vectors and, hence, the lemma.

Theorem 16 *Given $x^0 \in \mathbf{R}^n$, a nonsingular matrix Q, and a vector $0 \neq b \in \mathbf{R}^n$, $\exists$ an orthonormal matrix $R \ni$ for the map: $x \mapsto f(x) = RQ^{-1}(y - x^0)$:*

1. $f(x^0) = 0$
2. $RQ^t b = \alpha e_1$ for some $\alpha > 0$
3. $f(E) = \{z : \|z\| \leq 1\}$, where $E = (Q, x^0)$ is the ellipsoid of Q and x^0
4. $f(H) = \{y : y^t e_1 \leq 0\}$ where $H = \{y : (y - x^0)^t b \leq 0\}$.

Proof: Let $a = Q^t b$ in the previous lemma; we get an orthonormal R satisfying (ii) where $\alpha = \|a\| \neq 0$ since $b \neq 0$ and Q is nonsingular. (i) is satisfied for all R.

(iii) $E(Q, x^0) = \{y : y = Qz + x^0; \|z\| \leq 1\}$
$f(E) = \{y : y = RQ^{-1}((Qz + x^0) - x^0); \|z\| \leq 1\}$
$= \{y : y = Rz; \|z\| \leq 1\}$
$= \{y : \|y\| \leq 1\}$
(iv) Note that $f^{-1}(y) = QR^t y + x^0$. Hence,
$f(H) = \{y : y = RQ^{-1}(z - x^0);\ (z - x^0)^t b \leq o\}$
$= \{y : ((QR^t y + x^0) - x^0)^t b \leq 0\}$
$= \{y : y^t RQ^t b \leq 0\}$
$= \{y : y^t e_1 \leq 0\}$.

Thus, this transformation changes the ellipsoid to a sphere with unit radius and origin as the center and the "cutting plane" to the plane $\perp$ the first axis. See the diagram below:

Lemma 17 *Let $E = \{y : (y - x^0)^t A^{-1}(y - x^0)$ be an ellipsoid ($A = QQ^t$ for some nonsingular Q) and $a \neq 0$. Let A^1, x^1 be defined as in the algorithm:*

$$x^1 = x^0 - \frac{1}{n+1}\frac{Aa}{\sqrt{a^t Aa}}$$

and

$$A^1 = \frac{n^2}{n^2 - 1}[A - \frac{2}{n+1}\frac{(Aa)(Aa)^t}{a^t Aa}$$

Then, $E^1 = \{y : (y - x^1)^t (A^1)^{-1}(y - x^1) \leq 1\}$ is an ellipsoid and $\frac{1}{2}E = E \cap \{y : (y - x)^t a \leq 0\} \subset E^1$.

Please note that the set of feasible solutions within the sphere mentioned before is contained in the above intersection and hence in the next ellipsoid. Thus, it is contained in all the ellipsoids of the algorithm. We will show in the next lemma that the last of these has a very small volume (insufficient if the number of steps exceeds the prescribed value) and this will then prove the theorem.

Proof: It can be shown that by simple calculation that

$$(A^1)^{-1} = \frac{n^2-1}{n^2}[A^{-1} + \frac{2}{n-1}\frac{aa^t}{a^tAa}]$$

which is clearly symmetric and positive definite and hence it follows that A^1 is also positive definite. Now consider the map $x \mapsto f(x) = RQ^{-1}(x - x^0)$. We will show the following:

1. $f(E)$ is the sphere with origin as the center and unit radius
2. $f(\frac{1}{2}E)$ is the half sphere containing the "left" half of the first axis
3. $f(\frac{1}{2}E) \subseteq f(E^1)$ and, hence, $\frac{1}{2}E \subseteq E^1$
4. $f(E^1)$ is an ellipsoid and, hence, E^1 is also an ellipsoid (this has already been shown above).

(i) and (ii) have already been shown. To show (iii) and (iv), we first study what the outcome of the algorithm is if we start with $f(E)$ instead of E. *We will show that the output is* $f(E^1)$. For this purpose, let $A = I$ and $x^0 = 0$, and $a = e_1$.

$A^2 = \frac{n^2}{n^2-1}\left[I - \frac{2}{n+1}e_1e_1^t\right]$

$$= \begin{bmatrix} \alpha & & & \\ & \alpha & & \\ & & \alpha & \\ & & & \alpha \end{bmatrix} - \begin{bmatrix} \alpha\beta & & & \\ & & & \\ & & & \\ & & & \end{bmatrix} = \begin{bmatrix} \gamma & & & \\ & \alpha & & \\ & & \alpha & \\ & & & \alpha \end{bmatrix}$$

where $\alpha = \frac{n^2}{n^2-1}; \beta = \frac{2}{n+1}$, and $\gamma = \alpha - \alpha\beta = \frac{n^2}{(n+1)^2}$, and $x^2 = -\frac{e_1}{n+1}$. Since A^2 is a diagonal matrix with positive entries on the diagonal, it is clearly positive definite. Hence, $E^2(x^2, A^2)$ is an ellipsoid. Also, to show that this contains the "left" half of the sphere, we have to show that $[z : \|z\| \leq 1; z^te_1 = z_1 \leq 0] \Longrightarrow [z : (z - x^2)^t(A^2)^{-1}(z - x^2) \leq 1]$. Note that $\|z\| \leq 1 \Longrightarrow |z_1| \leq 1$ and, hence, $-z_1 \leq 1$.

$(z - x^2)^t (A^2)^{-1} (z - x^2) = z^t (A^2)^{-1} z - 2z^t (A^2)^{-1} x^2 + (x^2)^t (A^2)^{-1} x^2$
$= \frac{1}{n^2}[(n^2 - 1)\|z\|^2 + 2(n+1)(z_1^2 + z_1) + 1]$
$= \frac{n^2-1}{n^2}(\|z\|^2 - 1) + (2\frac{n+1}{n^2} z_1(z_1 + 1) + 1$
$\leq 1.$

We will now show that the ellipsoid $E^2 = f(E^1)$; this will prove that E^1 is an ellipsoid and the rest of the lemma.

$E^2 = \{y : (y - x^2)^t (A^2)^{-1} (y - x^2) \leq 1\}$
$RQ^{-1}(x^1 - x^0) = RQ^{-1}[x^0 - \frac{1}{n+1} \frac{QQ^t a}{\sqrt{a^t QQ^t a}} - x^0]$
$= -\frac{1}{n+1} \frac{RQ^t a}{\|Q^t a\|}$
$= -\frac{1}{n+1} e_1 = x^2$
$E^1 = \{y : (y - x^1)^t (A^1)^{-1} (y - x^1) \leq 1\}$
$f(E^1) = \{z : (QR^t z + x^0 - x^1)^t (A^1)^{-1} (QR^t z + x^0 - x^1) \leq 1\}$
$= \{z : (z - RQ^{-1}(x^1 - x^0))^t RQ^t (A^1)^{-1} QR^t (z - RQ^{-1}(x^1 - x^0)) \leq 1\}$
$= \{z : (z - x^2)^t RQ^t (A^1)^{-1} QR^t (z - x^2) \leq 1\}$

To show that $f(E^1) = E^2$, we have to show that $(A^2)^{-1} = RQ^t (A^1)^{-1} QR^t$ or, equivalently, that $A^2 = RQ^{-1} A^1 (RQ^{-1})^t$ which we do now.

$RQ^{-1} A^1 (RQ^{-1})^t$
$= \frac{n^2}{n^2-1}[RQ^{-1} A (RQ^{-1})^t - \frac{2}{n+1} \frac{(RQ^{-1})(Aa)^t (RQ^{-1})^t}{a^t Aa}]$

Letting $A = QQ^t$, we get the desired result. This completes this lemma.

Lemma 18 *Given E and E^1 as in the previous lemma, $\lambda(E^1) = c(n)\lambda(E)$ where $c(n) = \frac{n}{n+1}\left(\frac{n^2}{n^2-1}\right)^{\frac{n-1}{2}} < e^{-\frac{1}{2(n+1)}}$.*

Proof: Since f is an affine transformation, $\frac{\lambda(E^1)}{\lambda(E)} = \frac{\lambda(f(E^1))}{\lambda(f(E))} = \frac{\lambda(f(E^2))}{\lambda(S)}$ where S is the unit sphere centered at the origin. But E^2 is an ellipsoid with Q^2 a diagonal matrix, all of whose diagonal entries are $\frac{n}{\sqrt{n^2-1}}$ except the first which is $\frac{n}{n+1}$. Hence,

$\frac{\lambda(E^1)}{\lambda(E)} = |\det\ Q^2| = \left(\frac{n^2}{n^2-1}\right)^{\frac{n-1}{2}} [\frac{n}{n+1}]$

"Clearly" $e^x > 1 + x$ for $x > 0$; hence,

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

Consider $g(x) = e^{-x} - 1 + x$; $g(0) = 0$; $g'(x) = 1 - e^{-x} > 0\ \forall\ x > 0$; hence, $g(x) > 0\ \forall\ x > 0$; hence, $e^{-x} > 1 - x\ \forall\ x > 0$. Hence,

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

Theorem 19 *If the algorithm runs for more than $2(n+1)(2nL+n+L)$ iterations, then I has no feasible solutions.*

Proof:

$$\lambda(E^k) < e^{-\frac{k}{2(n+1)}}\lambda(S) < e^{-\frac{k}{2(n+1)}}2^{n(L+1)} < 2^{n(L+1)-\frac{k}{2(n+1)}}$$

But $\lambda(E^k) > 2^{-\frac{1}{(n+1)L}}$, and hence,

$$n(L+1) - \frac{k}{2(n+1)} \geq -(n+1)L$$

Hence, $k \leq 2(n+1)(2nL+n+L)$. Thus, if k exceeds this $\exists$ no solution to system I as promised.

0.1.4 Application to LP:

Lemma 20 *The system*

$$II : a^i x < b_i + 2^{-L}; 1 \leq i \leq m$$

has a solution iff the system

$$III : a^i x \leq b_i; 1 \leq i \leq m$$

has a solution; moreover, a solution of one can be found from that of the other is polynomial time. Please note that the space required for encoding II is polynomially related to that of III.

Proof: "Clearly" a solution to III is a solution to II. To go the other way, consider the LP:

$$\begin{gathered}\min\ t\\ a^i x - s_i \leq b_i\\ s_i \leq t; s_i \geq 0; 1 \leq i \leq m\end{gathered}$$

If x is a solution to II, then (x,s,t) is a solution to the LP with $t < 2^{-L}$, where $s_i = \max(0, a^i x - b_i)$ and $t = \max_i s_i$. Hence, $\exists$ an extreme solution to the LP which is optimal and has value $< 2^{-L}$ in this case. But all the coordinates of all vertices of the LP are rational numbers with numerator and denominator $< 2^{-L}$. Hence, $t^* = 0$ and starting from the feasible solution to II which is feasible to the LP and has value $< 2^{-L}$, we can find in polynomial time the optimal solution of the LP which has $t^* = 0$ and, hence, is feasible to III.

Lemma 21 *Every LP can be written in the form of inequalities III.*

This concludes Ellipsoid I discussion. In Ellipsoid II we will not use L; instead the actual values that occur in the polytope will be used. Also we will discuss various applications of this to show polynomiality. *Please note that the algorithm uses the "square root" operation – this is not "legitimate" in the usual sense. However, this objection can be overcome by calculating the square root approximately and then expanding the containing ellipsoid a little. The details are found in Ellipsoid II.*