A New Proof of the Ellipsoid Algorithm

By

SAMANTHA CAPOZZO

SENIOR THESIS

Submitted in partial satisfaction of the requirements for Highest Honors for the degree of

BACHELOR OF SCIENCE

in

MATHEMATICS

in the

COLLEGE OF LETTERS AND SCIENCE

of the

UNIVERSITY OF CALIFORNIA,

DAVIS

Approved:

Jesús A. De Loera

June 2011

ABSTRACT.

Linear programming is described by Howard Karloff as "the process of minimizing a linear objective function, subject to a finite number of linear equality and inequality constraints". Linear optimization is one of the main tools used in applied mathematics and economics. It finds applications in fields ranging from image processing to logistic distribution of goods. The first algorithm that was used to solve linear programs was the Simplex Method. Other popular algorithms are the Interior Point Methods. In 1979, Leonid Khachiyan invented the first ever polynomial-time algorithm to solve linear programs, the Ellipsoid Algorithm (see [**13**] for the first appearance). The algorithm is based on the geometry of ellipsoids and how a sequence of progressively smaller ellipsoids contains convex sets. Its ability to run in polynomial-time makes the Ellipsoid Algorithm an important theoretical tool that can be used as the basis of many other algorithmic applications in various fields.

In my senior thesis, I will present the details of the Ellipsoid Algorithm and my work with Professor Jesus De Loera on simplifying the steps of the algorithm and presenting a clear and concise proof that will be accessible to undergraduates.

Contents

CHAPTER 1

Preliminaries

1.1. Linear Programming

Linear programming can be described by the following (primal) optimization problem:

$$\begin{aligned} \min \quad & \mathbf{c}^T\mathbf{x} \\ \text{subject to} \quad & A\mathbf{x} = \mathbf{b} \\ & \mathbf{x} \geq 0 \end{aligned}$$

which can be described in words as "the process of minimizing a linear objective function, subject to a finite number of linear equality and inequality constraints" [**11**]. Although this may sound technical and complicated, it is used frequently in our every day lives, as we will discuss in detail in Chapter 3. In Chapter 2, we will formally present the linear programming algorithm known as the Ellipsoid Algorithm, along with a detailed proof. First, we will begin with a historical background on the algorithm, followed by several definitions that are needed to understand the algorithm and its proof.

1.2. The History of the Ellipsoid Algorithm

The Simplex Method, developed by George Dantzig in 1947, was the algorithm that sparked an interest in optimization and laid the foundation for further research and development. According to [**19**], optimization developed rapidly during the 1950's and 1960's. It was applicable in many fields, including engineering, science, and industry, which inspired researchers to pursue studies surrounding optimization and linear programming. This research led to the development of several other algorithms, including the Ellipsoid Algorithm (an alternative to the well-known Simplex Method), which was originally developed by N. Z. Shor, D. B. Yudin, and A. S. Nemirovskiĭ in the 1970's.

In 1979, Leonid Khachiyan showed that an adapted version of the algorithm was "the first polynomial-time linear programming algorithm" [**11**]. By doing so, Khachiyan had successfully solved a very important open theoretical problem. [**9**]

FIGURE 1. A photo of Leonid Khachiyan.

As described by [**19**], the Ellipsoid Algorithm

> "is related to the following geometric fact: if an ellipsoid in a d-space is cut in half by a hyperplane through its center, each half-ellipsoid can be enclosed in a new ellipsoid whose volume is smaller than the original...the new ellipsoid can be represented by parameters that are easily computed from those for the original ellipsoid and those describing the hyperplane".

1.3. Motivation

The Ellipsoid Algorithm turned out to be lacking computationally (in practice) but theoretically beautiful; for practical uses, the Simplex Method has proved to be superior, but for theoretical purposes, the Ellipsoid Algorithm is a valuable tool for "analyzing the complexity of optimization problems, particularly those arising in combinatorics" [**19**]. Its appeal comes from the fact that it solves problems for convex bodies, not just polytopes. Further, has a very strong theoretical base, which makes it useful to mathematicians for reasons that go beyond the application of the algorithm itself; see Chapter 3. Therefore, a proof of a theoretical tool such as the Ellipsoid Algorithm is incredibly useful, hence, the motivation of my thesis. My goal is to present a thorough and complete proof of the Ellipsoid Algorithm, based on the original proof given by Khachiyan.

1.4. Outline

The following is a general outline of the paper:

(1) In Chapter 1, we will begin with the definitions that will be useful throughout the rest of the paper.
(2) In Chapter 2, we will review the basics of ellipsoids and present the simplified Ellipsoid Algorithm, along with a complete proof.
(3) We will establish several theorems as consequences of the proof in the final sections of Chapter 2.
(4) We will conclude with examples, applications and developments in Chapter 3.

1.5. Definitions

From basic geometry, one may recall the formula for an ellipse:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

This ellipse is a 2-dimensional ellipsoid. Ellipsoids will be the fundamental geometric object of our investigation. Before we move into higher dimensions, we need to review several definitions that we will refer to frequently.

The following review of concepts and definitions are found in the book [**2**]:

The *norm* of $\mathbf{x} \in \mathbb{R}^n$ is

$$\|\mathbf{x}\| = \left(\sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}}.$$

Note the following useful properties of the norm:

(1) $\|\mathbf{x}\| \geq 0$ and $\|\mathbf{x}\| = 0 \Leftrightarrow \mathbf{x} = 0$.
(2) $\|\lambda\mathbf{x}\| = \|\lambda\|\|\mathbf{x}\|$ for all $\lambda \in \mathbb{R}, \mathbf{x} \in \mathbb{R}^n$.
(3) $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$.

Recall that the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_k$ are *linearly independent* if

$$\sum_{i=1}^{k} \lambda_i \mathbf{x}_i = 0 \text{ for } \lambda_1, \ldots, \lambda_k \in \mathbb{R} \Rightarrow \lambda_1 = \ldots = \lambda_k = 0.$$

Otherwise, they are said to be *linearly dependent*.

Also recall the idea of open and closed sets:

(1) A set $S \subseteq \mathbb{R}^n$ is said to be an *open set* if and only if for each $\mathbf{x} \in S$ there exists some ball centered at $\mathbf{x}$ completely contained in S.
(2) A set S is said to be a *closed set* if and only if $S^C = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} \notin S\}$, the complement of S, is open.

A set S is said to be *bounded* if and only if it is contained in some ball.

Definition 1. A set $K \subset \mathbb{R}^n$ is *convex* if and only if whenever $\mathbf{x}_1, \mathbf{x}_2 \in K$ then $(1 - \lambda)\mathbf{x}_1 + \lambda\mathbf{x}_2 \in K$ for all $0 \leq \lambda \leq 1$.

Following from the above definition, the *convex hull* of $A \subset \mathbb{R}^n$ is defined as

$$\text{conv}(A) = \{\lambda_1\mathbf{x}_1 + \ldots + \lambda_k\mathbf{x}_k \mid k \text{ is a positive integer, } \mathbf{x}_1, \ldots, \mathbf{x}_k \in A, \sum_{i=1}^{k} \lambda_i = 1 \text{ and } \lambda_i \geq 0 \text{ for } i = 1, \ldots, k\}.$$

Another useful definition stemming from convexity is the notion of a *convex polytope*, which is the convex hull of a finite set of points. In $\mathbb{R}^2$, a convex polytope is called a *convex polygon*.

DEFINITION 2. Let $\mathbf{x}_0 \in \mathbb{R}^n$ and $\|\mathbf{u}\| = 1$. Then the set

$$H = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x} - \mathbf{x}_0, \mathbf{u} \rangle = 0\}$$

is a *hyperplane* passing through $\mathbf{x}_0$ and having unit normal $\mathbf{u}$.

We can use the definition of the hyperplane to define open and closed halfspaces:

DEFINITION 3. The *closed halfspaces* defined by the hyperplane H in Definition 2 are

$$H^+ = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x} - \mathbf{x}_0, \mathbf{u} \rangle \geq 0\}$$
$$H^- = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x} - \mathbf{x}_0, \mathbf{u} \rangle \leq 0\}.$$

The *open halfspaces* are

$$H^+ = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x} - \mathbf{x}_0, \mathbf{u} \rangle > 0\}$$
$$H^- = \{\mathbf{x} \in \mathbb{R}^n \mid \langle \mathbf{x} - \mathbf{x}_0, \mathbf{u} \rangle < 0\}.$$

We can also use the definition of a hyperplane to define a polyhedron and a polytope, found in book [**11**]:

DEFINITION 4. A *polyhedron* is the intersection of finitely many halfspaces. A bounded, nonempty polyhedron is called a *polytope*.

The following definitions are found in the book [**18**]:

DEFINITION 5. A matrix M is *positive semidefinite* if $\mathbf{x}M\mathbf{x}^T \geq 0$ for all $\mathbf{x} \in \mathbb{R}^n$.

For our purposes, a positive semidefinite matrix M will also be *symmetric*, that is, $M = M^T$.

DEFINITION 6. A *vector space* S in $\mathbb{R}^n$ is a nonempty subset of $\mathbb{R}^n$ closed under vector addition and scalar multiplication. The *dimension* $\dim(S)$ of a vector space S is the maximum number of linearly independent vectors in S.

Now that we have presented the necessary foundation, we are ready to examine the Ellipsoid Algorithm.

CHAPTER 2

The Ellipsoid Algorithm

2.1. Ellipsoids

First, we will define a general dimension ellipsoid.

DEFINITION 7. Let M be a (symmetric) positive semidefinite $n \times n$ matrix and let $\mathbf{z} \in \mathbb{R}^n$. Then

$$E_{M,\mathbf{z}} := \{\mathbf{x} \mid (\mathbf{x}-\mathbf{z})^T M(\mathbf{x}-\mathbf{z}) \leq 1\}$$

denotes an ellipsoid centered at $\mathbf{z}$.

Note that M is invertible and acts as the "stretch" that turns $B(0,1)$, the unit sphere centered at the origin, into an ellipsoid. Also, note that

$$\mathbf{x} \in E_{M,\mathbf{z}} \iff \|M^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\| \leq 1 \text{ (by the Cholesky Factorization)}$$

where $M^{\frac{1}{2}}$ is a lower triangular matrix with positive diagonal elements. Recall from linear algebra that the Cholesky Factorization is the decomposition of a symmetric, positive semidefinite matrix into a lower triangular matrix and its conjugate transpose [**16**]. We use $M^{\frac{1}{2}}$ since M is invertible and positive semidefinite, and so that we can perform the following operation, using properties of linear algebra:

$$\begin{aligned}(\mathbf{x}-\mathbf{z})^T M(\mathbf{x}-\mathbf{z}) &\implies (\mathbf{x}-\mathbf{z})^T (M^{\frac{1}{2}})^T M^{\frac{1}{2}}(\mathbf{x}-\mathbf{z}) \\ &\implies ((\mathbf{x}-\mathbf{z})M^{\frac{1}{2}})^T M^{\frac{1}{2}}(\mathbf{x}-\mathbf{z}) \\ &\implies \|M^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\|.\end{aligned}$$

Now we let $\mathbf{u} = M^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})$, and we multiply both sides of the equation by the inverse of $M^{\frac{1}{2}}$, which, by abuse of notation, we will denote by $M^{-\frac{1}{2}}$:

$$\begin{aligned}(M^{-\frac{1}{2}})\mathbf{u} &= (M^{-\frac{1}{2}})M^{\frac{1}{2}}(\mathbf{x}-\mathbf{z}) \\ (M^{-\frac{1}{2}})\mathbf{u} &= \mathbf{x}-\mathbf{z} \\ \mathbf{x} &= \mathbf{z} + M^{-\frac{1}{2}}\mathbf{u},\end{aligned}$$

for all $\mathbf{u} \in B(0,1)$ where $\|\mathbf{u}\| \leq 1$.

Therefore

$$E_{M,\mathbf{z}} = \{\mathbf{x} = \mathbf{z} + M^{-\frac{1}{2}}\mathbf{u} \mid \mathbf{u}^T\mathbf{u} \leq 1\}. \tag{2.1}$$

Thus, $E_{M,\mathbf{z}} = \mathbf{z} + M^{-\frac{1}{2}}B(0,1)$. In words, this equation tells us that an ellipsoid is the image of a ball under a linear map ($M^{\frac{1}{2}}$) plus a translation ($\mathbf{z}$).

The volume of $B(0,1)$ is given by

$$v(n) = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)},$$

as seen in calculus, and since

$$\det(M^{-\frac{1}{2}}) = \frac{1}{\det(M^{\frac{1}{2}})} = \frac{1}{\sqrt{\det(M)}}$$

by the Jacobian identity for volumes, the volume of $E_{M,\mathbf{z}}$ is given by

$$\text{volume}(E_{M,\mathbf{z}}) = \frac{v(n)}{\sqrt{\det(M)}}. \tag{2.2}$$

Hence,

$$\ln(\text{volume}(E_{M,\mathbf{z}})) = \ln(v(n)) - \frac{1}{2}\ln(\det(M)).$$

2.2. Ellipsoid Algorithm

We will now introduce the formal statement of the Ellipsoid Algorithm. In our presentation of the algorithm, we have simplified the steps to make the formal statement more precise.

Algorithm 1 Ellipsoid Algorithm

Require: A set S with volume$(S) > 0$ is bounded and convex with a separation oracle, and $E_{M,\mathbf{z}}$ is given such that $S \subseteq E_{M,\mathbf{z}}$.

Ensure: $s \in S$ or S is empty.

1: **for** $k = 0$; $M^k = M$; $\mathbf{z}^k = \mathbf{z}$ **do**
2: If $\mathbf{z}^k \in S$, **STOP**; otherwise
3: Find a nonzero vector $\mathbf{a}$ such that $\mathbf{a}^T\mathbf{x} \leq \mathbf{a}^T\mathbf{z}^k$, for all $\mathbf{x} \in S$ (separating hyperplane);
4: Construct the smaller volume ellipsoid that contains

$$E_{M,\mathbf{z}} \cap \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{a}^T(\mathbf{x} - \mathbf{z}^k) \leq 0\}.$$

Let this ellipsoid have matrix M^{k+1} and center $\mathbf{z}^{k+1}$.
5: $k = k + 1$;
6: Go back to Step 2.
7: **end for**

For a visual representation of the Ellipsoid Algorithm in dimension two, see Figure 1 on the following page. Note that each quadrant of the figure represents another iteration of the algorithm, and the progression within Figure 1 moves clockwise, starting with the image on the top left.

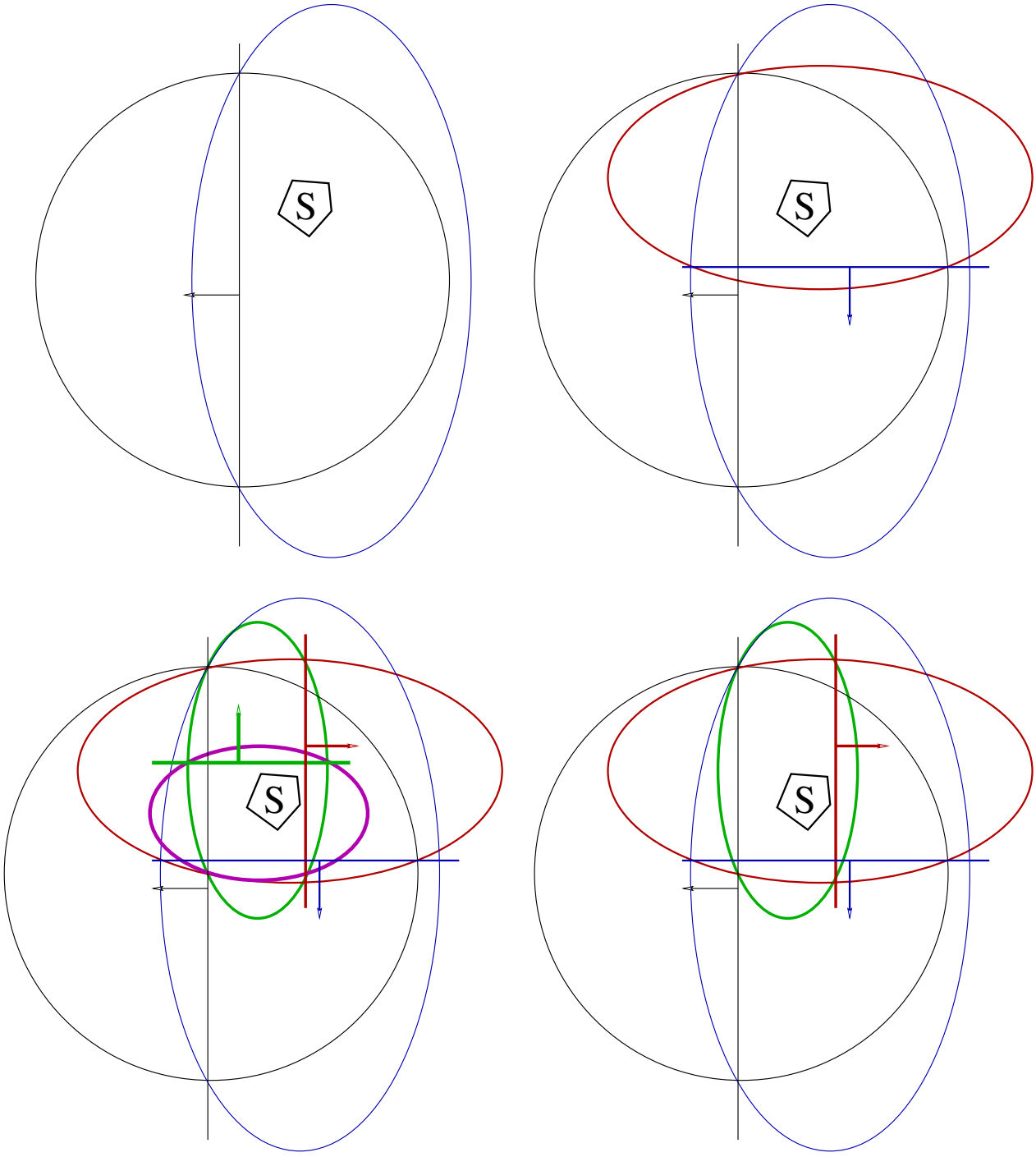

FIGURE 1. Four iterations of the Ellipsoid Algorithm for $n = 2$.

2.3. Basic Construction (1)

We will first discuss the special case of the Ellipsoid Algorithm where the ellipsoid is conveniently $B(0,1)$ and the separating hyperplane is $x_1 \geq 0$. We will prove that the Ellipsoid Algorithm works for this special case in the following three sections, Basic Construction (1) through Basic Construction (3). This special case will give us a better understanding of the algorithm and how it works mathematically. Then, we will generalize it to make the algorithm applicable to any ellipsoid.

We wish to find $\mathbf{m} = (z, 0, \ldots, 0)$, $M = \text{diag}(a_1, a_2, \ldots, a_n)$, such that the ellipsoid

$$E_{M,\mathbf{m}} = \{\mathbf{x} \in \mathbb{R}^n \mid (\mathbf{x} - \mathbf{m})^T M(\mathbf{x} - \mathbf{m}) \leq 1\}$$

contains $B(0,1) \cap \{\mathbf{x} \mid x_1 \geq 0\}$ and has minimal volume. Note that

$$(\mathbf{x} - \mathbf{m})^T M(\mathbf{x} - \mathbf{m}) = a_1(x_1 - z)^2 + \sum_{i=2}^{n} a_i x_i^2,$$

which follows directly from the matrix M.

The unit vectors $\mathbf{e}_1, \pm\mathbf{e}_2, \ldots, \pm\mathbf{e}_n$ are on the boundary of $B(0,1) \cap \{\mathbf{x} \mid x_1 \geq 1\}$.

We require them to lie on the boundary of the ellipsoid. This gives

$$\begin{aligned} a_1(1-z)^2 &= 1 \\ a_1 z^2 + a_i &= 1, \end{aligned}$$

for $2 \leq i \leq n$. From this we obtain

$$\begin{aligned} a_1 &= \frac{1}{(1-z)^2}, \\ a_i &= 1 - a_1 z^2 = 1 - \frac{z^2}{(1-z)^2} = \frac{1-2z}{(1-z)^2},\ i \geq 2. \end{aligned}$$

Recall from Equation 2.2 that $\text{volume}(E_{M,z})$ is minimal if $\det(M)$ is maximal. Since

$$\det(M) = \det(a_1 \cdot a_2 \cdots a_n) = \frac{1}{(1-z)^2} \cdot \underbrace{\frac{1-2z}{(1-z)^2} \cdots \frac{1-2z}{(1-z)^2}}_{n-1 \text{ times}} = \frac{(1-2z)^{n-1}}{(1-z)^{2n}},$$

which is obtained using calculus, we will verify that this occurs if $z = \frac{1}{n+1}$. To do so, we will take the derivative of $\det(M) = \frac{(1-2z)^{n-1}}{(1-z)^{2n}}$ and show that when $z = \frac{1}{n+1} \implies \frac{d}{dz}(\det(M)) = 0$.

$$\begin{aligned}\frac{d}{dz}(\det(M)) &= \frac{d}{dz}\left(\frac{(1-2z)^{n-1}}{(1-z)^{2n}}\right)\\ &= \left(\frac{-2(n-1)(1-z)^{2n}(1-2z)^{n-2}-(-1)(2n)(1-2z)^{n-1}(1-z)^{2n-1}}{[(1-z)^{2n}]^2}\right)\\ &= \left(\frac{(-2n+2)(1-z)^{2n}(1-2z)^{n-2}+2n(1-2z)^{n-1}(1-z)^{2n-1}}{(1-z)^{4n}}\right)\\ &= \left(\frac{(1-z)^{2n-1}(1-2z)^{n-2}\left[(-2n+2)(1-z)+2n(1-2z)\right]}{(1-z)^{4n}}\right)\end{aligned}$$

Now, we will plug in $z=\frac{1}{n+1}$:

$$\begin{aligned}\frac{d(\det(M))}{dz}\left(\frac{1}{n+1}\right) &= \left(\frac{\left(1-\frac{1}{n+1}\right)^{2n-1}\left(1-2\frac{1}{n+1}\right)^{n-2}\left[(-2n+2)\left(1-\frac{1}{n+1}\right)+2n\left(1-2\frac{1}{n+1}\right)\right]}{\left(1-\frac{1}{n+1}\right)^{4n}}\right)\\ &= \left(\frac{\left(\frac{n+1-1}{n+1}\right)^{2n-1}\left(\frac{n+1-2}{n+1}\right)^{n-2}\left[(-2n+2)\left(\frac{n+1-1}{n+1}\right)+2n\left(\frac{n+1-2}{n+1}\right)\right]}{\left(\frac{n+1-1}{n+1}\right)^{4n}}\right)\\ &= \left(\frac{\left(\frac{n}{n+1}\right)^{2n-1}\left(\frac{n-1}{n+1}\right)^{n-2}\left[(-2n+2)\left(\frac{n}{n+1}\right)+2n\left(\frac{n-1}{n+1}\right)\right]}{\left(\frac{n}{n+1}\right)^{4n}}\right)\\ &= \left(\frac{\left(\frac{n}{n+1}\right)^{2n-1}\left(\frac{n-1}{n+1}\right)^{n-2}\left[\left(\frac{-2n^2+2n}{n+1}\right)+\left(\frac{2n^2-2n}{n+1}\right)\right]}{\left(\frac{n}{n+1}\right)^{4n}}\right)\\ &= \left(\frac{\left(\frac{n}{n+1}\right)^{2n-1}\left(\frac{n-1}{n+1}\right)^{n-2}[0]}{\left(\frac{n}{n+1}\right)^{4n}}\right)\\ &= 0.\end{aligned}$$

Thus, we have verified that there is an inflection point at $z=\frac{1}{n+1}$. Now we must check that the second derivative,

$$\frac{d^2}{dz^2}(\det(M)) = \frac{d^2}{dz^2}\left(\frac{(1-z)^{2n-1}(1-2z)^{n-2}\left[(-2n+2)(1-z)+2n(1-2z)\right]}{(1-z)^{4n}}\right),$$

is negative in order to verify that $\det(M)$ is maximal at $z=\frac{1}{n+1}$. Using the quotient rule $\left(\frac{BT'-TB'}{B^2}\right)$, we will examine the second derivative in pieces:

$$\begin{aligned}
BT' &= (1-z)^{4n}\left((2n-1)(1-z)^{2n-2}(n-2)(1-2z)^{n-3}\left[(-2n+2)(-1)+2n(-2)\right]\right)\\
&= (2n-1)(n-2)(1-z)^{6n-2}(1-2z)^{n-3}\left[(2n-2)-4n\right]\\
&= (2n-1)(n-2)(-2n-2)(1-z)^{6n-2}(1-2z)^{n-3}\\
&= (2n^2-5n+2)(-2n-2)(1-z)^{6n-2}(1-2z)^{n-3}\\
&= (-4n^3+6n^2+6n-4)(1-z)^{6n-2}(1-2z)^{n-3}.
\end{aligned}$$

$$\begin{aligned}
TB' &= 4n(1-z)^{4n-1}\left((1-z)^{2n-1}(1-2z)^{n-2}\left[(-2n+2)(1-z)+2n(1-2z)\right]\right)\\
&= 4n(1-z)^{6n-2}(1-2z)^{n-2}\left[(-2n+2)(1-z)+2n(1-2z)\right]\\
&= (1-z)^{6n-2}(1-2z)^{n-2}\left[4n(-2n+2)(1-z)+8n^2(1-2z)\right].
\end{aligned}$$

$$B^2 = \left[(1-z)^{4n}\right]^2 = (1-z)^{8n}.$$

Putting the numerator $(BT' - TB')$ back together, we obtain:

$$\begin{aligned}
BT' - TB' &= (-4n^3+6n^2+6n-4)(1-z)^{6n-2}(1-2z)^{n-3}\\
&\qquad -4n(1-z)^{6n-2}(1-2z)^{n-2}\left[(-2n+2)(1-z)+2n(1-2z)\right]\\
&= (1-z)^{6n-2}(1-2z)^{n-3}\left[(-4n^3+6n^2+6n-4)\right.\\
&\qquad \left.-4n(1-2z)\left[(-2n+2)(1-z)+2n(1-2z)\right]\right]\\
&= (1-z)^{6n-2}(1-2z)^{n-3}\left[(-4n^3+6n^2+6n-4)\right.\\
&\qquad \left.-\left[4n(-2n+2)(1-z)(1-2z)+8n^2(1-2z)^2\right]\right]\\
&= (1-z)^{6n-2}(1-2z)^{n-3}\left[(-4n^3+6n^2+6n-4)\right.\\
&\qquad \left.-\left[(-8n^2+8)(1-z)(1-2z)+8n^2(1-2z)^2\right]\right].
\end{aligned}$$

We will now plug in $z = \frac{1}{n+1}$:

$$
\begin{aligned}
BT' - TB'\big|_{\frac{1}{n+1}} &= \left(1-\frac{1}{n+1}\right)^{6n-2}\left(1-\frac{2}{n+1}\right)^{n-3}\Bigg[(-4n^3+6n^2+6n-4)\\
&\qquad -\left[(-8n^2+8)\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)+8n^2\left(1-\frac{2}{n+1}\right)^2\right]\Bigg]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\Bigg[(-4n^3+6n^2+6n-4)\\
&\qquad -\left[(-8n^2+8)\left(\frac{n}{n+1}\right)\left(\frac{n-1}{n+1}\right)+8n^2\left(\frac{n-1}{n+1}\right)^2\right]\Bigg]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\Bigg[(-4n^3+6n^2+6n-4)\\
&\qquad -\left[\left(\frac{(-8n^2+8)(n)(n-1)}{(n+1)^2}\right)+\left(\frac{8n^2(n-1)^2}{(n+1)^2}\right)\right]\Bigg]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\Bigg[(-4n^3+6n^2+6n-4)\\
&\qquad -\left[\left(\frac{(-8n^3+8n)(n-1)}{(n+1)^2}\right)+\left(\frac{(8n^3-8n^2)(n-1)}{(n+1)^2}\right)\right]\Bigg]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\Bigg[(-4n^3+6n^2+6n-4)\\
&\qquad -\left(\frac{(-8n^3+8n)(n-1)+(8n^3-8n^2)(n-1)}{(n+1)^2}\right)\Bigg]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\Bigg[(-4n^3+6n^2+6n-4)\\
&\qquad -\left(\frac{(n-1)[-8n^3+8n+8n^3-8n^2]}{(n+1)^2}\right)\Bigg]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left[(-4n^3+6n^2+6n-4)-\left(\frac{(n-1)[8n-8n^2]}{(n+1)^2}\right)\right]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left[(-4n^3+6n^2+6n-4)-\left(\frac{(n-1)(-8n)(n+1)}{(n+1)^2}\right)\right]\\
&= \left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left[(-4n^3+6n^2+6n-4)-\left(\frac{(n-1)(-8n)}{n+1}\right)\right].
\end{aligned}
$$

We can find a common denominator:

$$\begin{aligned}
&\left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left[\frac{(-4n^3+6n^2+6n-4)(n+1)}{n+1}-\frac{-8n^2+8n}{n+1}\right]\\
&=\left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left[\frac{-4n^4+2n^3+12n^2+10n+4}{n+1}-\frac{-8n^2+8n}{n+1}\right]\\
&=\left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left[\frac{-4n^4+2n^3+20n^2+2n+4}{n+1}\right]\\
&=\left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left(\frac{1}{n+1}\right)\left[-4n^4+2n^3+20n^2+2n+4\right].
\end{aligned}$$

Thus, we can put the fraction together:

$$\begin{aligned}
\frac{d^2(\det(M))}{dz^2}\left(\frac{1}{n+1}\right)&=\frac{\left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left(\frac{1}{n+1}\right)\left[-4n^4+2n^3+20n^2+2n+4\right]}{(1-z)^{8n}}\\
&=\frac{\left(\frac{n}{n+1}\right)^{6n-2}\left(\frac{n-1}{n+1}\right)^{n-3}\left(\frac{1}{n+1}\right)\left[-4n^4+2n^3+20n^2+2n+4\right]}{\left(\frac{n}{n+1}\right)^{8n}}\\
&=\frac{\left(\frac{n-1}{n+1}\right)^{n-3}\left(\frac{1}{n+1}\right)\left[-4n^4+2n^3+20n^2+2n+4\right]}{\left(\frac{n}{n+1}\right)^{2n+2}}.\\
&=\frac{\left(\frac{n-1}{n+1}\right)^{n-3}\left(\frac{1}{n+1}\right)\left[-2(n+2)(2n^3-5n^2-1)\right]}{\left(\frac{n}{n+1}\right)^{2n+2}}.
\end{aligned}$$

Since we know $2<n\in\mathbb{N}$, the polynomial $2n^3-5n^2-1$ will always be positive, and because we are multiplying this polynomial by $-2(n+2)$, we know that $-2(n+2)(2n^3-5n^2-1)$ will always be negative. By Descartes' Rule of Signs, there is only one root of $2n^3-5n^2-1$ from zero to infinity, and using a Sturm sequence, we know that this root lies between 0 and 2.6. That means for $2<n$, the second derivative will always be negative. Thus, we have verified that when $z=\frac{1}{n+1}$, $\det(M)$ is maximal. This means we

can substitute $z = \frac{1}{n+1}$ into our equations for a_1 and a_i and simplify to obtain:

$$a_1 = \frac{1}{(1-z)^2} = \frac{1}{\left(1-\frac{1}{n+1}\right)^2} = \frac{1}{\left(\frac{n+1-1}{n+1}\right)^2} = \frac{1}{\left(\frac{n}{n+1}\right)^2} = \left(\frac{n+1}{n}\right)^2$$

$$a_i = \frac{1-2z}{(1-z)^2} = \frac{1-2\left(\frac{1}{n+1}\right)}{\left(1-\frac{1}{n+1}\right)^2} = \frac{\frac{n+1-2}{n+1}}{\left(\frac{n+1-1}{n+1}\right)^2} = \frac{\frac{n-1}{n+1}}{\left(\frac{n}{n+1}\right)^2} = \frac{(n-1)(n+1)^2}{(n+1)(n^2)}$$

$$= \frac{(n-1)(n+1)}{n^2} = \frac{n^2-1}{n^2} \text{ for } i \geq 2.$$

Now we know the coordinates of the ellipsoid that contains half of the ball. In the next section, we will see all desired properties are true for this special case.

2.4. Basic Construction (2)

We let

$$a_1 := \frac{(n+1)^2}{n^2}, \quad a_i := \frac{n^2-1}{n^2} \text{ for } i \geq 2, \quad B := \{\mathbf{y} \mid \mathbf{y}^T\mathbf{y} \leq 1\}, \quad H := \{\mathbf{y} \mid y_1 \geq 0\},$$

$$\bar{M} := \frac{n^2-1}{n^2}\left(I + \frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right), \ \bar{\mathbf{z}} := \frac{1}{n+1}\mathbf{e}_1, \quad E := E_{\bar{M},\bar{\mathbf{z}}}.$$

THEOREM 1. $(B \cap H) \subseteq E$.

PROOF. One has $\mathbf{y} \in E$ if and only if

$$(\mathbf{y}-\bar{\mathbf{z}})^T\bar{M}(\mathbf{y}-\bar{\mathbf{z}}) = \left(\mathbf{y} - \frac{1}{n+1}\mathbf{e}_1\right)^T\left(\frac{n^2-1}{n^2}\left(I + \frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)\right)\left(\mathbf{y} - \frac{1}{n+1}\mathbf{e}_1\right) \leq 1.$$

This is equivalent to

$$\frac{n^2-1}{n^2}\sum_{i=1}^{n} y_i^2 + \frac{1}{n^2} + y_1(y_1-1)\left(\frac{2n+2}{n^2}\right) \leq 1.$$

Now let $\mathbf{y} \in B \cap H$. Then $0 \leq y_1 \leq 1$ implies that $y_1(y_1-1) \leq 0$. We also know that $\sum_{i=1}^{n} y_i^2 \leq 1$ because $y \in B$. Since

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

we obtain $\mathbf{y} \in E$.

□

2.5. Basic Construction (3)

Recall the following variables from Basic Construction (2), Section 2.4:

$$\begin{aligned}
&\bar{M} := \frac{n^2-1}{n^2}\left(I + \frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right) \text{ where } \mathbf{e}_1\mathbf{e}_1^T \text{ is a diagonal matrix,}\\
&B := \{\mathbf{y} \mid \mathbf{y}^T\mathbf{y} \le 1\},\\
&E := E_{\bar{M},\bar{\mathbf{z}}}.
\end{aligned}$$

THEOREM 2. $\text{volume}(E) < \text{volume}(B)\, \mathrm{e}^{\frac{-1}{2(n+1)}}$.

PROOF. One has

$$\frac{\text{volume}(E)}{\text{volume}(B)} = \frac{\sqrt{\det(I)}}{\sqrt{\det(\bar{M})}} = \frac{1}{\sqrt{\det(\bar{M})}}.$$

Moreover,

$$\begin{aligned}
\det(\bar{M}) &= \left(\frac{n^2-1}{n^2}\right)^n \left(1 + \frac{2}{n-1}\right)\\
&= \left(\frac{n^2-1}{n^2}\right)^{n-1} \left(\frac{n^2-1}{n^2}\right)\left(\frac{n-1+2}{n-1}\right)\\
&= \left(\frac{n^2-1}{n^2}\right)^{n-1} \left(\frac{n^2-1}{n^2}\cdot\frac{n+1}{n-1}\right)\\
&= \left(\frac{n^2-1}{n^2}\right)^{n-1} \left(\frac{(n+1)(n-1)(n+1)}{n^2(n-1)}\right)\\
&= \left(\frac{n^2-1}{n^2}\right)^{n-1} \left(\frac{(n+1)^2}{n^2}\right)\\
&= \left(\frac{n^2-1}{n^2}\right)^{n-1} \left(\frac{n+1}{n}\right)^2.
\end{aligned}$$

Recall from calculus that $1 + x \le \mathrm{e}^x$. (To check this fact, write $0 \le \mathrm{e}^x - x - 1$ and take the first derivative to obtain $0 \le \mathrm{e}^x - 1 \implies \mathrm{e}^x = 1 \implies x = 0$, which satisfies $1 + x \le \mathrm{e}^x$, but we must make sure that $x = 0$ is a minimum in order for the claim to hold for all x. To do so, we take the second derivative and obtain $0 \le \mathrm{e}^x \implies x = 0$, so x is indeed a minimum. Therefore the claim holds for all x.)

Now, using $1 + x \leq \mathrm{e}^x$, we can compute

$$\begin{aligned}
\frac{1}{\det(\bar{M})} &= \frac{1}{(\frac{n^2-1}{n^2})^{n-1}(\frac{n+1}{n})^2} \\
&= \left(\frac{n^2}{n^2-1}\right)^{n-1}\left(\frac{n}{n+1}\right)^2 \\
&= \left(\frac{n^2}{n^2}+\frac{1}{n^2-1}\right)^{n-1}\left(\frac{n}{n}-\frac{1}{n+1}\right)^2 \\
&= \left(1+\frac{1}{n^2-1}\right)^{n-1}\left(1-\frac{1}{n+1}\right)^2 \\
&\leq \mathrm{e}^{\frac{1}{n^2-1}(n-1)}\,\mathrm{e}^{\frac{-1}{n+1}(2)} \\
&= \mathrm{e}^{\frac{n-1}{(n+1)(n-1)}}\,\mathrm{e}^{\frac{-2}{n+1}} \\
&= \mathrm{e}^{\frac{1}{n+1}}\,\mathrm{e}^{\frac{-2}{n+1}} = \mathrm{e}^{\frac{-1}{n+1}}\,.
\end{aligned}$$

Putting our equations together, we see that

$$\frac{\text{volume}(E)}{\text{volume}(B)} = \frac{1}{\sqrt{\det(\bar{M})}} \leq \sqrt{\mathrm{e}^{\frac{-1}{n+1}}} = \left(\mathrm{e}^{\frac{-1}{n+1}}\right)^{\frac{1}{2}} = \mathrm{e}^{\frac{-1}{2(n+1)}}$$

which can then be written

$$\text{volume}(E) \leq \text{volume}(B)\,\mathrm{e}^{\frac{-1}{2(n+1)}} \Longrightarrow \text{volume}(E) < \text{volume}(B)\,\mathrm{e}^{\frac{-1}{2(n+1)}}\,.$$

□

Thus, we have proved in Sections 2.3 - 2.5, Basic Construction (1) through Basic Construction (3), that the Ellipsoid Algorithm works for the special case when the ellipsoid is $B(0,1)$ and the supporting hyperplane is $x_1 \geq 0$. Next we will see that this is much more general.

2.6. Key Matrix Theory Lemmas

In this section, we will review some basic matrix manipulation that will be helpful for the rest of the chapter.

LEMMA 1. *Let U be such that $QU = R$. Then $I + S^TU$ is invertible.*

PROOF. Suppose $\mathbf{w} \in \mathbb{R}^k$ satisfies $(I + S^TU)\mathbf{w} = 0$. Then

$$\begin{aligned}
(Q + RS^T)U\mathbf{w} &= QU\mathbf{w} + RS^TU\mathbf{w} \\
&= (QU)\mathbf{w} + R(S^TU)\mathbf{w} \\
&= R\mathbf{w} + R(-\mathbf{w}) \\
&= R\mathbf{w} - R\mathbf{w} = 0.
\end{aligned}$$

$Q + RS^T$ being nonsingular gives $U\mathbf{w} = 0$. Since $\text{rank}(U) = k$, and U is a $n \times k$ matrix, that implies that k columns of U are linearly independent. Therefore, we must have $\mathbf{w} = 0$. Hence, $I + S^T U$ is invertible.

□

THEOREM 3. *If* $Q\mathbf{x}_0 = \mathbf{q}$ *and* $(I + S^T U)\mathbf{y} = S^T\mathbf{x}_0$ *then* $\mathbf{x} = \mathbf{x}_0 - U\mathbf{y}$ *satisfies* $(Q + RS^T)\mathbf{x} = \mathbf{q}$.

PROOF.

$$\begin{aligned}(Q + RS^T)\mathbf{x} &= (Q + RS^T)(\mathbf{x}_0 - U\mathbf{y}) \\ &= Q\mathbf{x}_0 + RS^T\mathbf{x}_0 - QU\mathbf{y} - RS^TU\mathbf{y} \\ &= \mathbf{q} + R(S^T\mathbf{x}_0) - (QU)\mathbf{y} - RS^TU\mathbf{y} \\ &= \mathbf{q} + R(I + S^TU)\mathbf{y} - R\mathbf{y} - RS^TU\mathbf{y} \\ &= \mathbf{q} + R(I\mathbf{y} + S^TU\mathbf{y}) - R\mathbf{y} - RS^TU\mathbf{y} \\ &= \mathbf{q} + R\mathbf{y} + RS^TU\mathbf{y} - R\mathbf{y} - RS^TU\mathbf{y} \\ &= \mathbf{q}.\end{aligned}$$

□

We now present the Sherman-Morrison Formula in the following theorem:

THEOREM 4. *Let* Q, R *and* S *be matrices such that* Q *and* $Q + RS^T$ *are nonsingular, and* R *and* S *are* $n \times k$ *matrices of* $\text{rank}(k) \leq n$. *Then*

$$(Q + RS^T)^{-1} = Q^{-1} - Q^{-1}R(I + S^TQ^{-1}R)^{-1}S^TQ^{-1}.$$

PROOF. Recall $Q\mathbf{x}_0 = \mathbf{q}$ and $(I + S^TU)\mathbf{y} = S^T\mathbf{x}_0$, as stated in Theorem 3, and $QU = R$, as stated in Lemma 1. Then, using the manipulations $\mathbf{x}_0 = Q^{-1}\mathbf{q}$, $U = Q^{-1}R$, and $\mathbf{y} = (I + S^TU)^{-1}S^T\mathbf{x}_0$, the solution $\mathbf{x}$ of $(Q + RS^T)\mathbf{x} = \mathbf{q}$ is given by

$$\begin{aligned}\mathbf{x} &= \mathbf{x}_0 - Uy \\ &= Q^{-1}\mathbf{q} - Q^{-1}R(I + S^TU)^{-1}S^T\mathbf{x}_0 \\ &= Q^{-1}\mathbf{q} - Q^{-1}R(I + S^TU)^{-1}S^T[Q^{-1}\mathbf{q}] \\ &= Q^{-1}\mathbf{q} - Q^{-1}R(I + S^T(Q^{-1}R))^{-1}S^TQ^{-1}\mathbf{q} \\ &= (Q^{-1} - Q^{-1}R(I + S^TQ^{-1}R)^{-1}S^TQ^{-1})\mathbf{q}.\end{aligned}$$

Since Theorem 3 holds for all $\mathbf{q} \in \mathbb{R}^n$ and by the uniqueness of inverses, that implies

$$(Q + RS^T)^{-1} = Q^{-1} - Q^{-1}R(I + S^TQ^{-1}R)^{-1}S^TQ^{-1}$$

(that is, the Sherman-Morrison Formula holds).

□

2.7. Prototypical Iteration for Arbitrary Ellipsoids

Before we continue with our more general case of the Ellipsoid Algorithm, note that in Sections 2.3 - 2.5, we use M and $\bar{M}$, which are different from, but correspond to, $\dot{M}$ and $\tilde{M}$, respectively, that will appear in the following sections. These new representations, $\dot{M}$ and $\tilde{M}$, are more general as well.

We let $\dot{M}$ be an arbitrary positive semidefinite matrix,

$$E_{\dot{M},\mathbf{z}} := \{\mathbf{x} \mid (\mathbf{x}-\mathbf{z})^T \dot{M}(\mathbf{x}-\mathbf{z}) \leq 1\} = \mathbf{z} + \dot{M}^{-\frac{1}{2}} B(0,1),$$

since we now wish to work with arbitrary ellipsoids. We know $\dot{M}, \mathbf{z}$ and a nonzero vector $\mathbf{a}$ (a separating hyperplane). Define

$$\tilde{M} := \frac{n^2-1}{n^2}\left(\dot{M} + \frac{2}{n-1}\frac{\mathbf{a}\mathbf{a}^T}{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right) \quad \text{and} \quad \bar{\mathbf{z}} := \mathbf{z} + \frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}. \tag{2.3}$$

Using the Sherman-Morrison Formula from Theorem 4, we have that

$$\begin{aligned}
&\tilde{M}^{-1} \\
&= \left(\frac{n^2-1}{n^2}\right)^{-1}\left(\dot{M}^{-1} - \dot{M}^{-1}\frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\mathbf{a}\left(1+\mathbf{a}^T\dot{M}^{-1}\frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\mathbf{a}\right)^{-1}\mathbf{a}^T\dot{M}^{-1}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\dot{M}^{-1}\mathbf{a}\left(1+\frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\mathbf{a}^T\dot{M}^{-1}\mathbf{a}\right)^{-1}\mathbf{a}^T\dot{M}^{-1}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\dot{M}^{-1}\mathbf{a}\left(1+\frac{2}{n-1}\right)^{-1}\mathbf{a}^T\dot{M}^{-1}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\dot{M}^{-1}\mathbf{a}\left(\frac{n+1}{n-1}\right)^{-1}\mathbf{a}^T\dot{M}^{-1}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2}{(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\left(\frac{n-1}{n+1}\right)\dot{M}^{-1}\mathbf{a}\mathbf{a}^T\dot{M}^{-1}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2(n-1)\dot{M}^{-1}\mathbf{a}\mathbf{a}^T\dot{M}^{-1}}{(n+1)(n-1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2\dot{M}^{-1}\mathbf{a}\mathbf{a}^T\dot{M}^{-1}}{(n+1)\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right) \\
&= \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2}{n+1}\frac{\dot{M}^{-1}\mathbf{a}\mathbf{a}^T\dot{M}^{-1}}{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right).
\end{aligned}$$

Therefore, we have shown that

$$\tilde{M}^{-1} = \frac{n^2}{n^2-1}\left(\dot{M}^{-1} - \frac{2}{n+1}\frac{\dot{M}^{-1}\mathbf{a}\mathbf{a}^T\dot{M}^{-1}}{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right). \tag{2.4}$$

Thus, by using Equation 2.3 and Equation 2.4, we obtain a direct formula for a new ellipsoid that will follow $\tilde{M}$ right after we find a separating hyperplane. Note that this is also related to Equation 2.1.

2.8. Two Important Theorems

The following two theorems are almost duplicates to Theorems 1 and Theorem 2, but are valid for arbitrary configurations.

THEOREM 5. $E_{\dot{M},\mathbf{z}} \cap \{\mathbf{x} \mid \mathbf{a}^T\mathbf{x} \leq \mathbf{a}^T\mathbf{z}\} \subseteq E_{\tilde{M},\bar{\mathbf{z}}}$.

PROOF. Let $\mathbf{u} := \dot{M}^{-\frac{1}{2}}\mathbf{a}$, $\mathbf{b} := \|\mathbf{u}\|\mathbf{e}_1$, and $R := \frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I$. Then we have that $R^T = R$, $R\mathbf{u} = \mathbf{b}$, and $R^2 = I$. Before we use these three properties, we will check that they hold:

(1) $R^T = R$.

$$\begin{aligned}
R^T &= \left(\frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I\right)^T \\
&= \frac{2((\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T)^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I^T \\
&= \frac{2((\mathbf{u}+\mathbf{b})^T)^T(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I \\
&= \frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I \\
&= R.
\end{aligned}$$

(2) $R\mathbf{u} = \mathbf{b}$. First we check that $\|R\mathbf{u}\| = \|\mathbf{u}\|$.

$$\begin{aligned} R\mathbf{u} &= \left(\frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I\right)\mathbf{u} \\ &= \frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2} - \mathbf{u} \\ &= \frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2} - \frac{\|\mathbf{u}+\mathbf{b}\|^2\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2} \\ &= \frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - \|\mathbf{u}+\mathbf{b}\|^2\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2} \\ &= \frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2}. \end{aligned}$$

We want $\|R\mathbf{u}\|$, so we take the norm of this fraction, which we will do in two separate pieces.

(a) First, the numerator:

$$\begin{aligned} &\|2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}\|^2 \\ &= \left[2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}\right]^T \left[2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}\right] \\ &= \left[(2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u})^T - ((\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u})^T\right] \left[2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}\right] \\ &= \left[2\mathbf{u}^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T - \mathbf{u}^T(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\right] \left[2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}\right] \\ &= 4\mathbf{u}^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - 2\mathbf{u}^T(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} \\ &\quad - 2\mathbf{u}^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u} + \mathbf{u}^T(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u} \\ &= 4\|\mathbf{u}+\mathbf{b}\|^2\mathbf{u}^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - 2\|\mathbf{u}+\mathbf{b}\|^2\mathbf{u}^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} \\ &\quad - 2\|\mathbf{u}+\mathbf{b}\|^2\mathbf{u}^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} + \|\mathbf{u}+\mathbf{b}\|^4\|\mathbf{u}\|^2 \\ &= \|\mathbf{u}+\mathbf{b}\|^4\|\mathbf{u}\|^2. \end{aligned}$$

(b) And now, the denominator:

$$\left(\|\mathbf{u}+\mathbf{b}\|^2\right)^2 = \|\mathbf{u}+\mathbf{b}\|^4.$$

Putting the numerator and denominator back together, we obtain:

$$\begin{aligned} \|R\mathbf{u}\|^2 = \frac{\|\mathbf{u}+\mathbf{b}\|^4\|\mathbf{u}\|^2}{\|\mathbf{u}+\mathbf{b}\|^4} &= \|\mathbf{u}\|^2 \\ \implies \|R\mathbf{u}\| &= \|\mathbf{u}\|, \text{ as desired.} \end{aligned}$$

Now we claim that $\frac{R\mathbf{u}}{\|\mathbf{u}\|} = \mathbf{e}_1$. If this claim holds, then $\mathbf{e}_1^T \left(\frac{R\mathbf{u}}{\|\mathbf{u}\|}\right) = \mathbf{e}_1^T\mathbf{e}_1 = 1$. We can check by plugging the equation we found for $R\mathbf{u}$ into $\mathbf{e}_1^T \left(\frac{R\mathbf{u}}{\|\mathbf{u}\|}\right)$:

$$\mathbf{e}_1^T \left(\frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T\mathbf{u} - (\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})\mathbf{u}}{\|\mathbf{u}\|\|\mathbf{u}+\mathbf{b}\|^2} \right).$$

We will simplify the numerator using $\mathbf{b} = \|\mathbf{u}\|\mathbf{e}_1$:

$$\begin{aligned}
&\mathbf{e}_1^T \left[2\left(\mathbf{u}+\mathbf{b}\right)\left(\mathbf{u}+\mathbf{b}\right)^T\mathbf{u} - \left(\mathbf{u}+\mathbf{b}\right)^T\left(\mathbf{u}+\mathbf{b}\right)\mathbf{u} \right] \\
&= \mathbf{e}_1^T \left[2\left(\mathbf{u}+\mathbf{b}\right)\left(\mathbf{u}^T+\mathbf{b}^T\right)\mathbf{u} - \left(\mathbf{u}^T+\mathbf{b}^T\right)\left(\mathbf{u}+\mathbf{b}\right)\mathbf{u} \right] \\
&= \mathbf{e}_1^T \left[2\left(\mathbf{u}\mathbf{u}^T+\mathbf{b}\mathbf{u}^T+\mathbf{u}\mathbf{b}^T+\mathbf{b}\mathbf{b}^T\right)\mathbf{u} - \left(\mathbf{u}^T\mathbf{u}+\mathbf{b}^T\mathbf{u}+\mathbf{u}^T\mathbf{b}+\mathbf{b}^T\mathbf{b}\right)\mathbf{u} \right] \\
&= \mathbf{e}_1^T \left[2\left(\mathbf{u}\mathbf{u}^T\mathbf{u}+\mathbf{b}\mathbf{u}^T\mathbf{u}+\mathbf{u}\mathbf{b}^T\mathbf{u}+\mathbf{b}\mathbf{b}^T\mathbf{u}\right) - \left(\mathbf{u}^T\mathbf{u}\mathbf{u}+\mathbf{b}^T\mathbf{u}\mathbf{u}+\mathbf{u}^T\mathbf{b}\mathbf{u}+\mathbf{b}^T\mathbf{b}\mathbf{u}\right) \right] \\
&= \mathbf{e}_1^T \left[2\mathbf{u}\mathbf{u}^T\mathbf{u}+2\mathbf{b}\mathbf{u}^T\mathbf{u}+2\mathbf{u}\mathbf{b}^T\mathbf{u}+2\mathbf{b}\mathbf{b}^T\mathbf{u} - \mathbf{u}^T\mathbf{u}\mathbf{u} - \mathbf{b}\mathbf{u}^T\mathbf{u} - \mathbf{u}^T\mathbf{b}\mathbf{u} - \mathbf{b}^T\mathbf{b}\mathbf{u} \right] \\
&= 2\mathbf{e}_1^T\mathbf{u}\mathbf{u}^T\mathbf{u} + 2\mathbf{e}_1^T\mathbf{b}\mathbf{u}^T\mathbf{u} + 2\mathbf{e}_1^T\mathbf{u}\mathbf{b}^T\mathbf{u} + 2\mathbf{e}_1^T\mathbf{b}\mathbf{b}^T\mathbf{u} - \mathbf{e}_1^T\mathbf{u}^T\mathbf{u}\mathbf{u} - \mathbf{e}_1^T\mathbf{b}^T\mathbf{u}\mathbf{u} \\
&\quad - \mathbf{e}_1^T\mathbf{u}^T\mathbf{b}\mathbf{u} - \mathbf{e}_1^T\mathbf{b}^T\mathbf{b}\mathbf{u} \\
&= 2\mathbf{e}_1^T\mathbf{u}\left(\|\mathbf{u}\|^2\right) + 2\mathbf{e}_1^T\left(\|\mathbf{u}\|\mathbf{e}_1\right)\left(\|\mathbf{u}\|^2\right) + 2\mathbf{e}_1^T\mathbf{u}\left(\|\mathbf{u}\|\mathbf{e}_1^T\right)\mathbf{u} + 2\mathbf{e}_1^T\left(\|\mathbf{u}\|\mathbf{e}_1\right)\left(\|\mathbf{u}\|\mathbf{e}_1^T\right)\mathbf{u} \\
&\quad - \mathbf{e}_1^T\left(\|\mathbf{u}\|^2\right)\mathbf{u} - \mathbf{e}_1^T\left(\|\mathbf{u}\|\mathbf{e}_1^T\right)\mathbf{u}\mathbf{u} - \mathbf{e}_1^T\left(\mathbf{b}^T\mathbf{u}\right)\mathbf{u} - \mathbf{e}_1^T\left(\|\mathbf{u}\|\mathbf{e}_1^T\right)\left(\|\mathbf{u}\|\mathbf{e}_1\right)\mathbf{u} \\
&= 2\|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u} + 2\|\mathbf{u}\|^3\left(\mathbf{e}_1^T\mathbf{e}_1\right) + 2\|\mathbf{u}\|(\mathbf{e}_1^T\mathbf{u})^2 + 2\|\mathbf{u}\|^2\left(\mathbf{e}_1^T\mathbf{e}_1\right)\left(\mathbf{e}_1^T\mathbf{u}\right) - \|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u} \\
&\quad - \|\mathbf{u}\|(\mathbf{e}_1^T\mathbf{u})^2 - \mathbf{e}_1^T\left(\|\mathbf{u}\|\mathbf{e}_1^T\mathbf{u}\right)\mathbf{u} - \|\mathbf{u}\|^2\mathbf{e}_1^T\left(\mathbf{e}_1^T\mathbf{e}_1\right)\mathbf{u} \\
&= 2\|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u} + 2\|\mathbf{u}\|^3 + 2\|\mathbf{u}\|(\mathbf{e}_1^T\mathbf{u})^2 + 2\|\mathbf{u}\|^2\left(\mathbf{e}_1^T\mathbf{u}\right) - \|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u} - \|\mathbf{u}\|(\mathbf{e}_1^T\mathbf{u})^2 \\
&\quad - \|\mathbf{u}\|(\mathbf{e}_1^T\mathbf{u})^2 - \|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u} \\
&= 2\|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u} + 2\|\mathbf{u}\|^3.
\end{aligned}$$

Now placing the simplified numerator back into the fraction:

$$\frac{2\|\mathbf{u}\|^3 + 2\|\mathbf{u}\|^2\mathbf{e}_1^T\mathbf{u}}{\|\mathbf{u}\|\|\mathbf{u}+\mathbf{b}\|^2} = \frac{2\|\mathbf{u}\|^2 + 2\|\mathbf{u}\|\mathbf{e}_1^T\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2} = \frac{2\mathbf{u}^T\mathbf{u} + 2\mathbf{b}^T\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2} = \frac{2(\mathbf{u}^T+\mathbf{b}^T)\mathbf{u}}{\|\mathbf{u}+\mathbf{b}\|^2}.$$

We want to show that this fraction is equal to 1. Using Laws of Cosines (see Figure 2), we can rewrite this fraction as:

$$\frac{2\|\mathbf{u}+\mathbf{b}\|\|\mathbf{u}\|\cos(\mathbf{u}+\mathbf{b},\mathbf{u})}{\|\mathbf{u}+\mathbf{b}\|^2} = \frac{2\|\mathbf{u}\|\cos(\mathbf{u}+\mathbf{b},\mathbf{u})}{\|\mathbf{u}+\mathbf{b}\|} = \frac{2\|\mathbf{u}\|}{\|\mathbf{u}+\mathbf{b}\|}\frac{\|\mathbf{u}+\mathbf{b}\|}{2\|\mathbf{u}\|} = 1.$$

Thus, we have shown that $R\mathbf{u} = \mathbf{b}$.

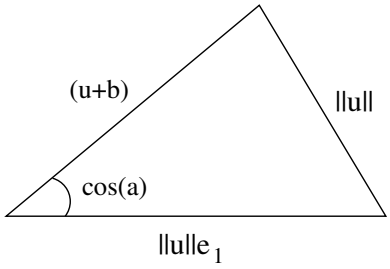

FIGURE 2. The Law of Cosines for the Proof of Theorem 5.

(3) $R^2 = I$.

$$\begin{aligned}
R^2 &= \left(\frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I\right)^2 \\
&= \left(\frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I\right)\left(\frac{2(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - I\right) \\
&= \frac{4(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2\|\mathbf{u}+\mathbf{b}\|^2} - \frac{4(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} + I \\
&= \frac{4(\mathbf{u}+\mathbf{b})\|\mathbf{u}+\mathbf{b}\|^2(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2\|\mathbf{u}+\mathbf{b}\|^2} - \frac{4(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} + I \\
&= \frac{4(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} - \frac{4(\mathbf{u}+\mathbf{b})(\mathbf{u}+\mathbf{b})^T}{\|\mathbf{u}+\mathbf{b}\|^2} + I \\
&= I.
\end{aligned}$$

Now we can use $R^T = R,\ R\mathbf{u} = \mathbf{b}$, and $R^2 = I$ to prove the stated theorem!

Suppose $(\mathbf{x}-\mathbf{z})^T\dot{M}(\mathbf{x}-\mathbf{z}) \leq 1$ and $\mathbf{a}^T\mathbf{x} \geq \mathbf{a}^T\mathbf{z}$.
Recall $\mathbf{u} := \dot{M}^{-\frac{1}{2}}\mathbf{a},\ R\mathbf{u} = \mathbf{b} = \|\mathbf{u}\|\mathbf{e}_1,\ \mathbf{y} := R\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})$. Then

$$\begin{aligned}
\mathbf{y}^T\mathbf{y} &= \left(R\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\right)^T\left(R\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\right) \\
&= \left((\mathbf{x}-\mathbf{z})^T\dot{M}^{\frac{1}{2}}R^T\right)\left(R\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\right) \\
&= (\mathbf{x}-\mathbf{z})^T\dot{M}^{\frac{1}{2}}R^TR\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z}) \\
&= (\mathbf{x}-\mathbf{z})^T\dot{M}^{\frac{1}{2}}R^2\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z}) \\
&= (\mathbf{x}-\mathbf{z})^T\dot{M}(\mathbf{x}-\mathbf{z}) \\
&\leq 1.
\end{aligned}$$

Moreover,

$$\begin{aligned}\|\mathbf{u}\|y_1 = \|\mathbf{u}\|\mathbf{e}_1^T\mathbf{y} = \mathbf{b}^T\mathbf{y} = \mathbf{u}^T R\mathbf{y} &= \left(\mathbf{a}^T\dot{M}^{-\frac{1}{2}}\right) R\left(R\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\right)\\ &= \mathbf{a}^T\dot{M}^{-\frac{1}{2}}RR\dot{M}^{\frac{1}{2}}(\mathbf{x}-\mathbf{z})\\ &= \mathbf{a}^T(\mathbf{x}-\mathbf{z})\\ &\geq 0.\end{aligned}$$

Now we will show

$$\begin{aligned}&(\mathbf{x}-\bar{\mathbf{z}})^T\tilde{M}(\mathbf{x}-\bar{\mathbf{z}})\\ &= \left(\mathbf{x}-\left[\mathbf{z}+\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right]\right)^T\tilde{M}\left(\mathbf{x}-\left[\mathbf{z}+\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right]\right)\\ &= \left(\mathbf{x}-\mathbf{z}-\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right)^T\tilde{M}^{\frac{1}{2}}\tilde{M}^{\frac{1}{2}}\left(\mathbf{x}-\mathbf{z}-\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right)\\ &= \left((\mathbf{x}-\mathbf{z})-\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right)^T\dot{M}^{\frac{1}{2}}R\bar{M}R\dot{M}^{\frac{1}{2}}\left((\mathbf{x}-\mathbf{z})-\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right)\end{aligned}$$

Recall that $\bar{M} := \frac{n^2-1}{n^2}\left(I+\frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)$. We can substitute this value into our equation and simplify:

$$\begin{aligned}&\left(\mathbf{y}-\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right)^T\dot{M}^{\frac{1}{2}}R\left(\frac{n^2-1}{n^2}\right)\left(I+\frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)\\ &\qquad R\dot{M}^{\frac{1}{2}}\left(\mathbf{y}-\frac{1}{n+1}\frac{\dot{M}^{-1}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}}\right)\\ &= \left(\mathbf{y}-\frac{1}{n+1}\frac{\dot{M}^{-\frac{1}{2}}\dot{M}^{-\frac{1}{2}}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-\frac{1}{2}}\dot{M}^{-\frac{1}{2}}\mathbf{a}}}\right)^T\dot{M}^{\frac{1}{2}}R\left(\frac{n^2-1}{n^2}\right)\left(I+\frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)\\ &\qquad R\dot{M}^{\frac{1}{2}}\left(\mathbf{y}-\frac{1}{n+1}\frac{\dot{M}^{-\frac{1}{2}}\dot{M}^{-\frac{1}{2}}\mathbf{a}}{\sqrt{\mathbf{a}^T\dot{M}^{-\frac{1}{2}}\dot{M}^{-\frac{1}{2}}\mathbf{a}}}\right)\\ &= \left(\mathbf{y}-\frac{1}{n+1}\frac{\dot{M}^{-\frac{1}{2}}\mathbf{u}}{\sqrt{\mathbf{u}^T\mathbf{u}}}\right)^T\dot{M}^{\frac{1}{2}}R\left(\frac{n^2-1}{n^2}\right)\left(I+\frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)R\dot{M}^{\frac{1}{2}}\left(\mathbf{y}-\frac{1}{n+1}\frac{\dot{M}^{-\frac{1}{2}}\mathbf{u}}{\sqrt{\mathbf{u}^T\mathbf{u}}}\right)\\ &\leq \left(\mathbf{y}-\frac{1}{n+1}\frac{\|\mathbf{u}\|\mathbf{e}_1}{\|\mathbf{u}\|}\right)^T\left(I+\frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)\left(\mathbf{y}-\frac{1}{n+1}\frac{\|\mathbf{u}\|\mathbf{e}_1}{\|\mathbf{u}\|}\right)\\ &\leq 1.\end{aligned}$$

The inequality follows just as in the proof of Theorem 1, since $\mathbf{y}^T\mathbf{y} \leq 1$ and $y_1 \geq 0$.

□

THEOREM 6. $\text{volume}(E_{\tilde{M},\bar{\mathbf{z}}}) < \text{volume}(E_{\dot{M},\mathbf{z}})\, \mathrm{e}^{\frac{-1}{2(n+1)}}$.

PROOF.

$$\begin{aligned}
\tilde{M} &= \frac{n^2-1}{n^2}\left(\dot{M} + \frac{2}{n-1}\frac{\mathbf{a}\mathbf{a}^T}{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right) \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}\left(I + \frac{2}{n-1}\frac{\dot{M}^{-\frac{1}{2}}\mathbf{a}\mathbf{a}^T\dot{M}^{-\frac{1}{2}}}{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right)\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{R\dot{M}^{-\frac{1}{2}}\mathbf{a}\mathbf{a}^T\dot{M}^{-\frac{1}{2}}R}{\mathbf{a}^T\dot{M}^{-1}\mathbf{a}}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{R\dot{M}^{-\frac{1}{2}}\mathbf{a}\mathbf{a}^T\dot{M}^{-\frac{1}{2}}R}{\mathbf{a}^T\dot{M}^{-\frac{1}{2}}RR\dot{M}^{-\frac{1}{2}}\mathbf{a}}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{R\left[\dot{M}^{-\frac{1}{2}}\mathbf{a}\right]\left[\mathbf{a}^T\dot{M}^{-\frac{1}{2}}\right]R}{\left[\mathbf{a}^T\dot{M}^{-\frac{1}{2}}\right]RR\left[\dot{M}^{-\frac{1}{2}}\mathbf{a}\right]}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{R\mathbf{u}\mathbf{u}^TR^T}{\mathbf{u}^TR^TR\mathbf{u}}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{R\mathbf{u}(R\mathbf{u})^T}{(R\mathbf{u})^TR\mathbf{u}}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{\|\mathbf{u}\|^2\mathbf{e}_1\mathbf{e}_1^T}{\|R\mathbf{u}\|^2}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\frac{\|\mathbf{u}\|^2\mathbf{e}_1\mathbf{e}_1^T}{\|\mathbf{u}\|^2}\right)R\dot{M}^{\frac{1}{2}} \\
&= \frac{n^2-1}{n^2}\dot{M}^{\frac{1}{2}}R\left(I + \frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right)R\dot{M}^{\frac{1}{2}}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\det(\tilde{M}) &= \left(\frac{n^2-1}{n^2}\right)^n \det(\dot{M})(\det(R))^2 \det\left(I + \frac{2}{n-1}\mathbf{e}_1\mathbf{e}_1^T\right) \\
&= \left(\frac{n^2-1}{n^2}\right)^n \left(1 + \frac{2}{n-1}\right)\det(\dot{M}),
\end{aligned}$$

which can be written

$$\frac{\det(\tilde{M})}{\det(\dot{M})} = \left(\frac{n^2-1}{n^2}\right)^n \left(1 + \frac{2}{n-1}\right) > \mathrm{e}^{\frac{1}{n+1}}.$$

Hence

$$\frac{\text{volume}(E_{\tilde{M},\bar{\mathbf{z}}})}{\text{volume}(E_{\dot{M},\mathbf{z}})} = \frac{\sqrt{\det(\dot{M})}}{\sqrt{\det(\tilde{M})}} < \mathrm{e}^{\frac{-1}{2(n+1)}} \Longrightarrow \text{volume}(E_{\tilde{M},\bar{\mathbf{z}}}) < \text{volume}(E_{\dot{M},\mathbf{z}})\,\mathrm{e}^{\frac{-1}{2(n+1)}}\,.$$

□

2.9. Conclusions and Consequences of the Ellipsoid Algorithm

In this section, we will consider several consequences of the Ellipsoid Algorithm. In particular, we will consider how long it will take the algorithm to terminate.

Theorems 7 and 8 discuss the results using the special case that we examined in Sections 2.3 - 2.5.

THEOREM 7. *Suppose we want to find a point in the set S, with $S \subseteq E_{M^0,\mathbf{z}^0}$ and* $\text{volume}(S) > 0$. *Then the algorithm will find a point in S after at most*

$$\left\lfloor 2(n+1)\ln\left(\frac{\text{volume}(E_{M^0,\mathbf{z}^0})}{\text{volume}(S)}\right)\right\rfloor$$

iterations.

PROOF. After k iterations, we have

$$\text{volume}(E_{M^k,\mathbf{z}^k}) \leq \text{volume}(E_{M^0,\mathbf{z}^0})\,\mathrm{e}^{\frac{-k}{2(n+1)}}\,.$$

Since $S \subseteq E_{M^k,\mathbf{z}^k}$ for each k we obtain $\text{volume}(S) \leq \text{volume}(E_{M^0,\mathbf{z}^0})\,\mathrm{e}^{\frac{-k}{2(n+1)}}$. Taking the natural logarithm of both sides,

$$\ln(\text{volume}(S)) \leq \ln(\text{volume}(E_{M^0,\mathbf{z}^0})) - \frac{k}{2(n+1)}.$$

By rearranging terms, $\frac{k}{2(n+1)} + \ln(\text{volume}(S)) \leq \ln(\text{volume}(E_{M^0,\mathbf{z}^0}))$, which implies $\frac{k}{2(n+1)} \leq \ln\left(\frac{\text{volume}(E_{M^0,\mathbf{z}^0})}{\text{volume}(S)}\right)$. Therefore

$$k \leq 2(n+1)\ln\left(\frac{\text{volume}(E_{M^0,\mathbf{z}^0})}{\text{volume}(S)}\right).$$

This proves the theorem.

□

Now let $B(c,\delta) := \{\mathbf{x} \mid \|\mathbf{x}-\mathbf{c}\| \leq \delta\}$.

THEOREM 8. *Suppose we know R such that $S \subseteq B(0,R)$ and that S contains a ball $B(\hat{x},r)$ for some $\hat{x}$ and $r > 0$. Then the algorithm will find a point in S after at most*

$$\left\lfloor 2n(n+1)\ln\left(\frac{R}{r}\right)\right\rfloor$$

iterations.

PROOF. After k iterations, we have

$$\text{volume}(B(\hat{x}, r)) \leq \text{volume}(S) \leq \text{volume}(B(0, R))\, \mathrm{e}^{\frac{-k}{2(n+1)}}.$$

Taking logarithms again we get

$$\ln(\text{volume}(B(\hat{x}, r))) \leq \ln(\text{volume}(B(0, R))) - \frac{k}{2(n+1)}.$$

By rearranging terms,

$$\frac{k}{2(n+1)} + \ln(\text{volume}(B(\hat{x}, r))) \leq \ln(\text{volume}(B(0, R))),$$

which implies

$$\frac{k}{2(n+1)} \leq \ln\left(\frac{\text{volume}(B(0, R))}{\text{volume}(B(\hat{x}, r))}\right).$$

Therefore

$$\begin{aligned} k \leq 2(n+1)\ln\left(\frac{\text{volume}(B(0, R))}{\text{volume}(B(\hat{x}, r))}\right) &= 2(n+1)\ln\left(\frac{v(n)R^n}{v(n)r^n}\right) \\ &= 2(n+1)\ln\left(\frac{R}{r}\right)^n \\ &= 2n(n+1)\ln\left(\frac{R}{r}\right), \end{aligned}$$

where $v(n)$ is the volume of $B(0, 1)$ as seen in Section 2.1. This proves the theorem. □

We can improve the previous two results a lot in terms of generality. The following two theorems, Theorem 9 and Theorem 10, are more general versions of Theorem 7 and Theorem 8, respectively. Notice that the proofs are almost identical to the special case described above, but with a much more general result.

THEOREM 9. *Suppose* $\text{volume}(S \cap E_{M^0, \mathbf{z}^0}) > 0$. *Then the algorithm will find a point in* S *after at most*

$$\left\lfloor 2(n+1)\ln\left(\frac{\text{volume}(E_{M^0, \mathbf{z}^0})}{\text{volume}(S \cap E_{M^0, \mathbf{z}^0})}\right)\right\rfloor$$

iterations.

PROOF. Similarly to the Proof of Theorem 7, after k iterations, we have

$$\text{volume}(S \cap E_{M^0, \mathbf{z}^0}) \leq \text{volume}(E_{M^0, \mathbf{z}^0})\, \mathrm{e}^{\frac{-k}{2(n+1)}}.$$

Taking logarithms again we get

$$\ln(\text{volume}(S \cap E_{M^0, \mathbf{z}^0})) \leq \ln(\text{volume}(E_{M^0, \mathbf{z}^0})) - \frac{k}{2(n+1)}.$$

By rearranging terms,

$$\frac{k}{2(n+1)} + \ln(\text{volume}(S \cap E_{M^0,\mathbf{z}^0})) \leq \ln(\text{volume}(E_{M^0,\mathbf{z}^0})),$$

which implies

$$\frac{k}{2(n+1)} \leq \ln\left(\frac{\text{volume}(E_{M^0,\mathbf{z}^0})}{\text{volume}(S \cap E_{M^0,\mathbf{z}^0})}\right).$$

Therefore

$$k \leq 2(n+1)\ln\left(\frac{\text{volume}(E_{M^0,\mathbf{z}^0})}{\text{volume}(S \cap E_{M^0,\mathbf{z}^0})}\right).$$

This proves the theorem.

□

THEOREM 10. *Suppose we know R and that $S \cap B(0,R)$ contains a ball $B(\hat{x},r)$ for some $\hat{x}$ and $r > 0$. Then the algorithm will find a point in S after at most*

$$\left\lfloor 2n(n+1)\ln\left(\frac{R}{r}\right)\right\rfloor$$

iterations.

PROOF. Similarly to the Proof of Theorem 8, after k iterations, we have

$$\text{volume}(B(\hat{x},r)) \leq \text{volume}(S \cap B(0,R)) \leq \text{volume}(B(0,R))\,\mathrm{e}^{\frac{-k}{2(n+1)}}.$$

Taking logarithms again we get

$$\ln(\text{volume}(B(\hat{x},r))) \leq \ln(\text{volume}(B(0,R))) - \frac{k}{2(n+1)}.$$

By rearranging terms,

$$\frac{k}{2(n+1)} + \ln(\text{volume}(B(\hat{x},r))) \leq \ln(\text{volume}(B(0,R))),$$

which implies

$$\frac{k}{2(n+1)} \leq \ln\left(\frac{\text{volume}(B(0,R))}{\text{volume}(B(\hat{x},r))}\right).$$

Therefore

$$\begin{aligned} k \leq 2(n+1)\ln\left(\frac{\text{volume}(B(0,R))}{\text{volume}(B(\hat{x},r))}\right) &= 2(n+1)\ln\left(\frac{v(n)R^n}{v(n)r^n}\right) \\ &= 2(n+1)\ln\left(\frac{R}{r}\right)^n \\ &= 2n(n+1)\ln\left(\frac{R}{r}\right), \end{aligned}$$

where $v(n)$ is the volume of $B(0,1)$ as seen in Section 2.1. This proves the theorem.

□

CHAPTER 3

Recent Applications and Developments of the Ellipsoid Algorithm

There are many applications of the Ellipsoid Algorithm, and as more research surrounding the algorithm has been conducted, there have been many new developments since Khachiyan's development of the algorithm in 1979. Although there has been a decent amount of research surrounding the algorithm, but there is still much research left to be done. For our purposes, we will consider articles with applications and/or developments that took place after 1990, mostly due to the fact the serious research surrounding the Ellipsoid Algorithm took place from 1990 to the present. In particular, we will focus our attention on two specific examples.

EXAMPLE 1. **Design Problems obtained by Cost Minimization Problems**
Design problems are "the class of max-min and min-max optimization problems subject to a global budget constraint", as discussed in the paper [**3**]. Recent developments have shown that these problems are as easy to solve as their corresponding optimization problems, and that this holds for a large class of optimization problems. This is significant because optimization problems are a very important tool, and are relatively easy to solve. Specifically,

- The large class of optimization problems are:
  - minimization problems with concave objective functions, and
  - maximization problems with convex objective functions.
- For a minimization problem with a concave objective function, the corresponding design problem can be set up as a convex optimization problem.
- If the Ellipsoid Algorithm is used to solve the problem, then the problem can be solved in polynomial-time.
- Another way to solve the design problems is an algorithm developed by the authors that is based on the Ellipsoid Algorithm but is even more efficient. This is the main algorithmic result of the paper and an important development of the Ellipsoid Algorithm.

EXAMPLE 2. **The Classical Bin Packing Problem**
A recent application of the Ellipsoid Algorithm is in the Classical Bin Packing Problem, where n items of specified sizes need to be packed into the smallest number of unit-sized bins, and fragmentation of the items is allowed. Fragmentation can reduce the number of

bins required, but will increase overhead costs. The paper [**17**] considers two variants of this problem:

1. The first variant is "bin packing with size increasing fragmentation", where fragmenting an item increases the input size.
2. The second variant is "bin packing with size preserving fragmentation", where there is a bound on the total number of fragmented items.

These two variants cover a many practical scenarios, including "message transmission in community TV networks" and "preemptive scheduling on parallel machines with setup times/setup costs". The authors found that by applying the Ellipsoid Algorithm, they can solve the dual LP of this problem in polynomial-time.

There are many more applications of the Ellipsoid Algorithm, and many more developments. We briefly examine several other significant applications and developments that took place from 1990 to present.

3.1. Applications and Developments

(1) A simple algorithmic framework based on the Ellipsoid Algorithm is used to compute the approximation for a single-source buy-at-bulk problem with an unknown concave cost function. [**8**]
(2) An algorithm based on the ellipsoid method can be used to solve the windy postman problem. [**15**]
(3) The Ellipsoid Algorithm can be used to efficiently find a minimum cost k-partition for $k = 2$ of a set X with respect to the objective function, a problem that is NP-hard to solve exactly for the general case. [**21**]
(4) A variant of the Ellipsoid Algorithm is used to estimate the "distance to ill-posedness" of a conic linear system. The authors also present an analysis of the complexity of the ellipsoid algorithm. The main conclusion of the paper is that "the complexity of estimating the distance to ill-posedness of a particular conic system is roughly of the same order as the complexity of solving the conic system". [**6**]
(5) An algorithm that computes an allocation in the intersection of the prekernel and the least core of any cooperative game (in game theory) uses the Ellipsoid Algorithm as a subroutine. [**5**]
(6) The nucleolus flow of games has been shown to be polynomially solvable by the Ellipsoid Algorithm. [**12**]
(7) The Ellipsoid Algorithm is described by the authors as "easy to implement and [having] very good theoretical complexity". A modification of the algorithm, where the radii of the spheres they use are unknown, is an improvement on the author's previous work. [**7**]
(8) More efficient combinatorial algorithms that are based on the Ellipsoid Algorithm have been developed in recent years, as discussed in [**10**].

(9) The authors establish that Khachiyan's barycentric coordinate descent method is the polar of the deepest cut Ellipsoid Algorithm as they consider the classical problems of "computing a minimum-volume enclosing ellipsoid and an approximate rounding of the convex hull of the set". [**20**]
(10) The "best fit multiple ellipsoid" method has been explored for the use in classification (data mining) problems, where several ellipsoids are used in the separation of sets. [**4**]
(11) A large class of optimization problems, including directed edge augmentation problems (which fall into the class of covering supermodular functions over pairs of sets), can be solved using an algorithm that relies on the Ellipsoid Algorithm. [**1**]
(12) A survey found that an algorithm based on the Ellipsoid Algorithm is able to color the vertices of perfect graphs optimally and in polynomial time. [**14**]

It is important to note that although we have mentioned many applications and developments here, this list is far from complete. The Ellipsoid Algorithm has a far-reaching impact in mathematics and, since the development by Khachiyan in 1979, has broadened many aspects of the mathematical community and created new opportunities for research and further development. Since it is a fairly new addition to the family of linear programming algorithms, the Ellipsoid Algorithm has many years of research and development ahead, hopefully with the discovery of many more useful applications.

Bibliography

1. A. A. Benczúr, *Pushdown-reduce: an algorithm for connectivity augmentation and poset covering problems*, Discrete Appl. Math. **129** (2003), no. 2-3, 233–262. MR 1997351 (2004g:90089)
2. G. D. Chakerian and J. R. Sangwine-Yager, *Synopsis and exercises for the theory of convex sets*, 2009.
3. D. Chakrabarty, A. Mehta, and V. V. Vazirani, *Design is as easy as optimization*, SIAM J. Discrete Math. **24** (2010), no. 1, 270–286. MR 2630027 (2011b:90073)
4. A. V. Demyanov and M. Gaudioso, *An approach to classification based on separation of sets by means of several ellipsoids*, Optimization **54** (2005), no. 6, 579–593. MR 2190810 (2006g:90124)
5. U. Faigle, W. Kern, and J. Kuipers, *On the computation of the nucleolus of a cooperative game*, Internat. J. Game Theory **30** (2001), no. 1, 79–98. MR 1863715 (2002m:91008)
6. R. M. Freund and J. R. Vera, *On the complexity of computing estimates of condition measures of a conic linear system*, Math. Oper. Res. **28** (2003), no. 4, 625–648. MR 2015906 (2004j:90159)
7. ———, *Equivalence of convex problem geometry and computational complexity in the separation oracle model*, Math. Oper. Res. **34** (2009), no. 4, 869–879. MR 2573500 (2010m:90158)
8. A. Goel and I. Post, *An oblivious $O(1)$-approximation for single source buy-at-bulk*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), IEEE Computer Soc., Los Alamitos, CA, 2009, pp. 442–450. MR 2648425 (2011d:68196)
9. M. Grötschel, L. Lovász, and A. Schrijver, *Geometric algorithms and combinatorial optimization*, 2 ed., Algorithms and Combinatorics, Springer-Verlag, Germany, 1993.
10. S. Iwata, *Submodular function minimization*, Math. Program. **112** (2008), no. 1, Ser. B, 45–64. MR 2327001 (2008j:90103)
11. H. Karloff, *Linear programming*, Birkhäuser, 1991.
12. W. Kern and D. Paulusma, *On the core and f-nucleolus of flow games*, Math. Oper. Res. **34** (2009), no. 4, 981–991. MR 2573505 (2011e:91052)
13. L. G. Khachiyan, *A polynomial algorithm in linear programming*, Dokl. Akad. Nauk SSSR **244** (1979), no. 5, 1093–1096. MR 522052 (80g:90071)
14. F. Maffray, *On the coloration of perfect graphs*, Recent advances in algorithms and combinatorics, CMS Books Math./Ouvrages Math. SMC, vol. 11, Springer, New York, 2003, pp. 65–84. MR 1952983 (2003m:05073)
15. Z. Martínez and F. Javier, *Series-parallel graphs are windy postman perfect*, Discrete Math. **308** (2008), no. 8, 1366–1374. MR 2392053 (2009a:05200)
16. P. Olver and C. Shakiban, *Applied linear algebra*, Prentice-Hall, 2006.
17. H. Shachnai, T. Tamir, and O. Yehezkely, *Approximation schemes for packing with item fragmentation*, Theory Comput. Syst. **43** (2008), no. 1, 81–98. MR 2385695 (2009d:68188)
18. G. Strang, *Linear algebra and its applications*, Thomson, Brooks/Cole, 2006.
19. M. J. Todd, *The basic George B. Dantzig, by Richard W. Cottle*, Bulletin of the American Mathematical Society **48** (2011), no. 1, 123–129.
20. M. J. Todd and E. A. Yıldırım, *On Khachiyan's algorithm for the computation of minimum-volume enclosing ellipsoids*, Discrete Appl. Math. **155** (2007), no. 13, 1731–1744. MR 2348357 (2008h:90077)
21. L. Zhao, H. Nagamochi, and T. Ibaraki, *On generalized greedy splitting algorithms for multiway partition problems*, Discrete Appl. Math. **143** (2004), no. 1-3, 130–143. MR 2087875 (2005k:05025)