The ellipsoid method

We have learned that the Markowitz mean-variance optimization problem is a convex programming problem. The good news is that there are efficient methods to solve such convex programming problems and in particular quadratic programming problems in practice. In this lecture we briefly sketch a theoretical result, which yields an approximate polynomial time algorithm for convex programming problems.

Our goal is to solve a convex optimization problem

$$\begin{aligned}&\min f_0(x)\\ &f_i(x) \leqslant b_i,\ i = 1, \ldots, m.\end{aligned}$$

We reduce the optimization problem to the decision problem as follows. We are trying to find a $\beta^* \in \mathbb{R}$ such that $f_0(x) \leqslant \beta^*, f_1(x) \leqslant b_1, \ldots, f_m(x) \leqslant b_m$ is feasible, while $f_0(x) \leqslant \beta^* - \varepsilon, f_1(x) \leqslant b_1, \ldots, f_m(x) \leqslant b_m$ is infeasible. Suppose we know numbers $L \leqslant \beta^* - \varepsilon$ and $U \geqslant \beta^*$. We now test whether $f_0(x) \leqslant (L+U)/2, f_1(x) \leqslant b_1, \ldots, f_m(x) \leqslant b_m$ is feasible. If yes, we set $U = (L+U)/2$ and if no, we set $L = (L+U)/2$. After $O(\log(U-L) - \log(\varepsilon))$ many steps, this procedure terminates. This approximates the optimum value of the convex program.

This leaves us with the problem to decide whether a convex body is nonempty or not. Let $K \subseteq \mathbb{R}^n$ be a compact convex set with volume $\mathrm{vol}(K)$. Initially, the *ellipsoid method* can be used to determine a point $x^* \in K$ or to assert that the volume of K is less than a certain lower bound L.

The *unit ball* is the set $B = \{x \in \mathbb{R}^n \mid \|x\| \leqslant 1\}$ and an *ellipsoid* $E(A, b)$ is the image of the unit ball under a linear map $t : \mathbb{R}^n \to \mathbb{R}^n$ with $t(x) = Ax + b$, where $A \in \mathbb{R}^{n \times n}$ is an invertible matrix and $b \in \mathbb{R}^n$ is a vector. Clearly

$$E(A, b) = \{x \in \mathbb{R}^n \mid \|A^{-1}x - A^{-1}b\| \leqslant 1\}. \tag{1.1}$$

Exercise 1. Consider the mapping $t(x) = \left(\begin{smallmatrix} 1 & 3 \\ 2 & 5 \end{smallmatrix}\right)\left(\begin{smallmatrix} x(1) \\ x(2) \end{smallmatrix}\right)$. Draw the ellipsoid which is defined by t. What are the axes of the ellipsoid?

The *volume* of the unit ball is denoted by V_n, where $V_n \sim \frac{1}{\pi n}\left(\frac{2e\pi}{n}\right)^{n/2}$. It follows that the volume of the ellipsoid $E(A, b)$ is equal to $|\det(A)| \cdot V_n$. The next lemma is the key to the development of the ellipsoid method.

Lemma 1 (Half-Ball Lemma). *The half-ball* $H = \{x \in \mathbb{R}^n \mid \|x\| \leqslant 1, x(1) \geqslant 0\}$ *is contained in the ellipsoid*

$$E = \left\{ x \in \mathbb{R}^n \mid \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2} \sum_{i=2}^{n} x(i)^2 \leqslant 1 \right\} \quad (1.2)$$

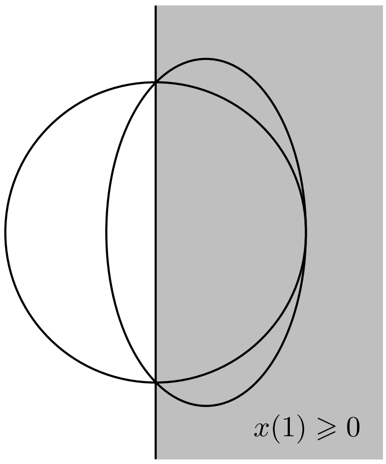

Figure 1.1: Half-ball lemma.

Proof. Let x be contained in the unit ball, i.e., $\|x\| \leqslant 1$ and suppose further that $0 \leqslant x(1)$ holds. We need to show that

$$\left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2} \sum_{i=2}^{n} x(i)^2 \leqslant 1 \quad (1.3)$$

holds. Since $\sum_{i=2}^{n} x(i)^2 \leqslant 1 - x(1)^2$ holds we have

$$\begin{aligned} &\left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2} \sum_{i=2}^{n} x(i)^2 \\ &\qquad \leqslant \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2}(1 - x(1)^2) \end{aligned} \quad (1.4)$$

This shows that (1.3) holds if x is contained in the half-ball and $x(1) = 0$ or $x(1) = 1$. Now consider the right-hand-side of (1.4) as a function of $x(1)$, i.e., consider

$$f(x(1)) = \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2}(1 - x(1)^2). \quad (1.5)$$

The first derivative is

$$f'(x(1)) = 2 \cdot \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right) - 2 \cdot \frac{n^2-1}{n^2} x(1). \tag{1.6}$$

We have $f'(0) < 0$ and since both $f(0) = 1$ and $f(1) = 1$, we have $f(x(1)) \leqslant 1$ for all $0 \leqslant x(1) \leqslant 1$ and the assertion follows. $\square$

In terms of a matrix A and a vector b, the ellipsoid E is described as $E = \{x \in \mathbb{R}^n \mid \|A^{-1}x - A^{-1}b\| \leqslant 1\}$, where A is the diagonal matrix with diagonal entries

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

and b is the vector $b = (1/(n+1), 0, \ldots, 0)$. Our ellipsoid E is thus the image of the unit sphere under the linear transformation $t(x) = Ax + b$. The determinant of A is thus $\frac{n}{n+1}\left(\frac{n^2}{n^2-1}\right)^{(n-1)/2}$. Using the inequality $1 + x \leqslant e^x$ we see that this is bounded by

$$e^{-1/(n+1)} e^{(n-1)/(2\cdot(n^2-1))} = e^{-\frac{1}{2(n+1)}}. \tag{1.7}$$

We can conclude the following theorem.

Theorem 2. *The half-ball $\{x \in \mathbb{R}^n \mid x(1) \geqslant 0, \|x\| \leqslant 1\}$ is contained in an ellipsoid E, whose volume is bounded by $e^{-\frac{1}{2(n+1)}} \cdot V_n$.*

Recall the following notion from linear algebra. A symmetric matrix $A \in \mathbb{R}^{n\times n}$ is called positive definite if all its eigenvalues are positive. Recall the following theorem.

Theorem 3. *Let $A \in \mathbb{R}^{n\times n}$ be a symmetric matrix. The following are equivalent.*

i) A is positive definite.

ii) $A = L^T L$, where $L \in \mathbb{R}^{n\times n}$ is a uniquely determined upper triangular matrix.

iii) $x^T A x > 0$ for each $x \in \mathbb{R}^n \setminus \{0\}$.

iv) $A = Q^T diag(\lambda_1, \ldots, \lambda_n) Q$, where $Q \in \mathbb{R}^{n\times n}$ is an orthogonal matrix and $\lambda_i \in \mathbb{R}_{>0}$ for $i = 1, \ldots, n$.

It is now convenient to switch to a different representation of an ellipsoid. An ellipsoid $\mathscr{E}(A, a)$ is the set $\mathscr{E}(A, a) = \{x \in \mathbb{R}^n \mid (x - a)^T A^{-1}(x - a) \leqslant 1\}$, where $A \in \mathbb{R}^{n\times n}$ is a symmetric positive definite matrix and $a \in \mathbb{R}^n$ is a vector. Consider the half-ellipsoid $\mathscr{E}(A, a) \cap (c^T x \leqslant c^T a)$.

Our goal is a similar lemma as the half-ball-lemma for ellipsoids. Geometrically it is clear that each half-ellipsoid $\mathscr{E}(A, a) \cap (c^T x \leqslant c^T a)$ must be contained in another ellipsoid $\mathscr{E}(A', b')$ with $\mathrm{vol}(\mathscr{E}(A', a'))/\mathrm{vol}(\mathscr{E}(A, a)) \leqslant e^{-1/(2n)}$. More precisely this follows from the fact that the half-ellipsoid is the image of the half-ball under a linear transformation. Therefore the image of the ellipsoid E under the same transformation contains the half-ellipsoid. Also, the volume-ratio of the two ellipsoids is invariant under a linear transformation.

We now record the formula for the ellipsoid $\mathscr{E}'(A', a')$. It is defined by

$$a' = a - \frac{1}{n+1} b \tag{1.8}$$

$$A' = \frac{n^2}{n^2-1}\left(A - \frac{2}{n+1} b\, b^T\right), \tag{1.9}$$

where b is the vector $b = A\,c/\sqrt{c^T A\,c}$. The proof of the correctness of this formula can be found in [1].

Lemma 4 (Half-Ellipsoid-Theorem)**.** *The half-ellipsoid $\mathscr{E}(A, b) \cap (c^T x \leqslant c^T a)$ is contained in the ellipsoid $\mathscr{E}'(A', a')$ and one has $\mathrm{vol}(\mathscr{E}')/\mathrm{vol}(\mathscr{E}) \leqslant e^{-1/(2n)}$.*

The method

Suppose we know an ellipsoid $\mathscr{E}_{init}$ which contains K. The ellipsoid method is described as follows. The input to the ellipsoid method is $\mathscr{E}_{init}$ and a positive number L. The mothod either

i) asserts that $\mathrm{vol}(K) < L$ or

ii) finds a point $x^* \in K$.

Algorithm (Ellipsoid method exact version)**.**

a) (Initialize): Set $\mathscr{E}(A, a) := \mathscr{E}_{init}$

b) If $a \in K$, then assert $K \neq \emptyset$ and stop

c) If $\mathrm{vol}(\mathscr{E}) < L$, then assert that $\mathrm{vol}(K) < L$.

d) Otherwise, compute an inequality $c^T x \leqslant \beta$ which is valid for K and satisfies $c^T a > \beta$ and replace $\mathscr{E}(A, a)$ by $\mathscr{E}(A', a)$ computed with formula (1.8) and goto step b).

Theorem 5. *The ellipsoid method computes a point in K or asserts that $\mathrm{vol}(K) < L$. The number of iterations is bounded by $2 \cdot n \ln(\mathrm{vol}(\mathscr{E}_{init})/L)$.*

Proof. After i iterations one has

$$\mathrm{vol}(\mathscr{E})/\mathrm{vol}(\mathscr{E}_{init}) \leqslant e^{-\frac{i}{2n}}. \tag{1.10}$$

Since we stop when $\mathrm{vol}(\mathscr{E}) < L$, we stop at least after $2 \cdot n \ln(\mathrm{vol}(\mathscr{E}_{init})/L)$ iterations. This shows the claim. □

1.1 Linear programming

In this section we discuss how the ellipsoid method can solve a linear program in polynomial time. This result was shown by Khachiyan [2] in 1979 and solved a longstanding open problem at that time.

Feasibility versus optimization

We first show that it is enough to have an algorithm for the *feasibility problem* of linear inequalities.

> Given $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$ defining a polyhedron $P = \{x \in \mathbb{R}^n \colon Ax \leqslant b\}$, compute a point $x^* \in P$ or assert that P is empty.

That this is enough is easily seen by linear programming duality. A point $x^* \in \mathbb{R}^n$ is an optimal solution of the linear program $\max\{c^T x \colon x \in \mathbb{R}^n,\, Ax \leqslant b\}$ if and only if there exists a $y^* \in \mathbb{R}^m$ such that $\binom{x^*}{y^*}$ is contained in the polyhedron $\{\binom{x}{y} \in \mathbb{R}^{n+m} \colon c^T x = b^T y,\, Ax \leqslant b,\, A^T y = c,\, y \geqslant 0\}$.

Our goal is therefore to show that the ellipsoid method can solve the feasibility problem in a polynomial number of iterations. More precisely, we are showing the following theorem.

Theorem 6. *Let $Ax \leqslant b$ be an inequality system with $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$ and let $U \in \mathbb{N}$ be the largest absolute value of a coefficient of A and b. There exist constants $k_1, k_2 \in \mathbb{N}$ such that the ellipsoid method requires $O(n^{k_1}(\log B)^{k_2})$ iterations to solve the feasibility problem for A and b.*

Notice that this polynomial $n^{k_1}(\log B)^{k_2}$ does not only depend on the dimension n but also on the *binary encoding length* of the numbers describing A and b. But since the input length is lower bounded by $\Omega(n + \log B)$ this is polynomial in the input length and shows that the Ellipsoid method is efficient in theory.

Bounded and full-dimensional polyhedra

We first analyze the Ellipsoid method under the assumption that P is full-dimensional and bounded. Later we will see that this assumtion can be made without loss of generality.

Lemma 7. *Suppose that $P = \{x \in \mathbb{R}^n \mid Ax \leqslant b\}$ is full-dimensional and bounded with $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$. Let B be the largest absolute value of a component of A and b.*

i) The vertices of P are in the box $\{x \in \mathbb{R}^n \mid -n^{n/2}B^n \leqslant x \leqslant n^{n/2}B^n\}$. Thus P is contained in the ball around 0 with radius $n^n B^n$.

ii) The volume of P is bounded from below by $1/(n \cdot B)^{3n^2}$.

Before we prove this theorem, we understand its consequences in terms of number of iterations of the ellipsoid method. If we plug these values into our analysis in Theorem 5. Our initial volume $\mathrm{vol}(\mathscr{E}_{init})$ is bounded by the volume of the box with side-lengths $2(n \cdot B)^n$. Thus

$$\mathrm{vol}(\mathscr{E}_{init}) \leqslant (2 \cdot n \cdot B)^{n^2}. \tag{1.11}$$

We can set L to

$$L = 1/(n \cdot B)^{3n^2}. \tag{1.12}$$

Clearly

$$\mathrm{vol}(\mathscr{E}_{init})/L \leqslant (2 \cdot n \cdot B)^{4 \cdot n^2}. \tag{1.13}$$

By Theorem 5 the ellipsoid method thus performs

$$O\left(2 \cdot n \cdot \ln\left((n \cdot B)^{4 \cdot n^2}\right)\right) \tag{1.14}$$

iterations. This is bounded by

$$O(n^3 \cdot \ln(n \cdot B)). \tag{1.15}$$

Theorem 8. *The ellipsoid method requires $O(n^3 \cdot \ln(n \cdot B))$ iterations to find a feasible point in a bounded and full-dimensioinal polyhedron $P = \{x \in \mathbb{R}^n \colon Ax \leqslant b\}$, where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$ and B is an upper bound on the coefficients of A and b.*

To prove lemma 7, we recall the following lemma that is proved in every linear algebra course.

Lemma 9 (Inverse formula and Cramer's rule)**.** *Let $C \in \mathbb{R}^{n \times n}$ be a nonsingular matrix. Then*

$$C^{-1}(j,i) = (-1)^{i+j} \det(C_{ij}) / \det(C),$$

where C_{ij} is the matrix arising from C by the deletion of the i-th row and j-th column. If $d \in \mathbb{R}^n$ is a vector then the j-th component of $C^{-1}d$ is given by $\det(\widetilde{C})/det(C)$, where $\widetilde{C}$ arises from C be replacing the j-th column with d.

We recall the Hadamard inequality which states that for $A \in \mathbb{R}^{n \times n}$ one has

$$|\det(A)| \leqslant \prod_{i=1}^{n} \|a_i\|, \tag{1.16}$$

where a_i denotes the i-th column of A. In particular, if B is the largest absolute value of an entry in A, then

$$|\det(A)| \leqslant n^{n/2} B^n. \tag{1.17}$$

Now let us inspect the vertices of a polyhedron $P = \{x \in \mathbb{R}^n \colon Ax \leqslant b\}$, where A and b are integral and the largest absolute value of any entry in A and b is bounded by B. A vertex is determined as the unique solution of a linear system $A'x = b'$, where $A'x \leqslant b'$ is a subsystem of $Ax \leqslant b$ and A' is invertible. Using Cramer's rule and our observation (1.17) we see that the vertices of P lie in the box $\{x \in \mathbb{R}^n \mid -n^{n/2}B^n \leqslant x \leqslant n^{n/2}B^n\}$. This shows i).

Now let us consider a lower bound on the volume of P. Since P is full-dimensional, there exist $n+1$ affinely independent vertices $v_0, \dots, v_n$ of P which span a *simplex* in $\mathbb{R}^n$. The volume of this simplex is determined by the formula

$$\frac{1}{n!} \cdot \left| \det \begin{pmatrix} 1 & \cdots & 1 \\ v_0 & \dots & v_n \end{pmatrix} \right|. \tag{1.18}$$

By Cramer's rule and the Hadamard inequality, the common denominator of each component of v_i can be bounded by $n^{n/2}B^n$. Thus (1.18) is bounded by

$$1/\left(n^n (n^{\frac{n}{2}} \cdot B^n)^{n+1}\right) \geqslant 1/\left(n^{3n^2} B^{2n^2}\right) \geqslant 1/(n \cdot B)^{3 \cdot n^2}, \tag{1.19}$$

which shows ii).

The boundedness and full-dimensionality condition

In this section we want to show how the ellipsoid method can be used to solve the following problem.

> Given a matrix $A \in \mathbb{Z}^{m \times n}$ and a vector $b \in \mathbb{Z}^m$, determine a feasible point x^* in the polyhedron $P = \{x \in \mathbb{R}^n \mid Ax \leqslant b\}$ or assert that $P = \emptyset$.

Boundedness

Consider the polyhedron $P = \{x \in \mathbb{R}^n \colon Ax \leqslant b\}$, and suppose that A' is a maximal sub-matrix of A consisting of linearly independent columns. Clearly $P = \{x \in \mathbb{R}^n \colon Ax \leqslant b\}$ is nonempty, if and only if $P' = \{x \in \mathbb{R}^n \colon A'x \leqslant b\}$ is nonempty and for each $x^* \in P'$ one has that $(x^*, 0) \in P$. Therefore, we can assume that the matrix A is of full-column rank.

If P is not empty, then P does have at least one vertex. The vertices are contained in the box $\{x \in \mathbb{R}^n \mid -n^{n/2}B^n \leqslant x \leqslant n^{n/2}B^n\}$. Therefore, we can append the inequalities $-n^{n/2}B^n \leqslant x \leqslant n^{n/2}B^n$ to $Ax \leqslant b$ without changing the status of $P \neq \emptyset$ or $P = \emptyset$. Notice that the *binary encoding length* of the new inequalities is polynomial in the binary encoding length of the old inequalities.

Full-dimensionality

Exercise 2. Let $P = \{x \in \mathbb{R}^n \mid Ax \leqslant b\}$ be a polyhedron and $\varepsilon > 0$ be a real number. Show that $P_\varepsilon = \{x \in \mathbb{R}^n \mid Ax \leqslant b + \varepsilon \cdot \mathbf{1}\}$ is full-dimensional if $P \neq \emptyset$.

The above exercise raises the following question. Is there an $\varepsilon > 0$ such that $P_\varepsilon = \emptyset$ if and only if $P = \emptyset$ and furthermore is the binary encoding length of this ε polynomial in the binary encoding length of A and b ?

Recall Farkas' Lemma.

Theorem 10. *The system $Ax \leqslant b$ does not have a solution if and only if there exists a nonnegative vector $\lambda \in \mathbb{R}^m_{\geqslant 0}$ such that $\lambda^T A = 0$ and $\lambda^T b = -1$.*

Let $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$ and let B be the largest absolute value of a coefficient of A and b. If $Ax \leqslant b$ is not feasible, then there exists a $\lambda \geqslant 0$ such that $\lambda^T(A|b) = (\mathbf{0}|1)$. We want to estimate the largest absolute value of a coefficient of λ with Cramer's rule and the Hadamard inequality. We can choose λ such that the nonzero coefficients of λ are the unique solution of a system of equations $Cx = d$, where each coefficient has absolute value at most B. By Cramer's rule and the Hadamard inequality we can thus choose λ such that $|\lambda(i)| \leqslant (n \cdot B)^n$. Now let $\varepsilon = 1/\left((n+1) \cdot (n \cdot B)^n\right)$. Then $|\lambda^T \mathbf{1} \cdot \varepsilon| < 1$ and thus

$$\lambda^T(b + \varepsilon \cdot \mathbf{1}) < 0. \tag{1.20}$$

Consequently the system $Ax \leqslant b + \varepsilon\mathbf{1}$ is infeasible if and only of $Ax \leqslant b$ is infeasible. Notice again that the encoding length of ε is polynomial in the encoding length of $Ax \leqslant b$ and we conclude with the main theorem of this section.

Theorem 11. *The ellipsoid method can be used to decide whether a system of inequalities $Ax \leqslant b$ contains a feasible point, where $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$. The number of iterations is bounded by a polynomial in n and $\log B$, where B is the largest absolute value of a coefficient of A and b.*

Solving linear programs

It finally follows from linear programming duality that the ellipsoid method can be used to solve a linear program of the form

$$\max\{c^T x \colon Ax \leqslant b,\, x \in \mathbb{R}^n\}$$

by finding a feasible point in the polyhedron

$$\{(x, y) \colon x \in \mathbb{R}^n,\, y \in \mathbb{R}^m,\, Ax \leqslant b,\, A^T y = c,\, c^T x = b^T y\}$$

The number of iterations is polynomial.

Theorem 12. *A linear program $\max\{c^T x \colon Ax \leqslant b\}$ can be solved in polynomial time in its binary encoding length.*

Warning

This short writeup serves only as a rough sketch of the ellipsoid method. We did not care about an important issue. The representation of the numbers in the intermediate steps of the algorithm (notice the square root in (1.8)) can be very large and need to be rounded to rational numbers with a polynomial encoding length. The details are not very difficult but tedious. They are very nicely described in the book [1].

Bibliography

[1] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer, 1988.

[2] L. Khachiyan. A polynomial algorithm in linear programming. *Doklady Akademii Nauk SSSR*, 244:1093–1097, 1979.