Chapter 7
The ellipsoid method

The simplex algorithm is not an algorithm which runs in polynomial time. It was long open, whether there exists a polynomial time algorithm for linear programming until Khachiyan \cite{2} showed that the ellipsoid method\cite{5,3} can solve linear programs in polynomial time. The remarkable fact is that the algorithm is polynomial in the binary encoding length of the linear program. In other words, if the input consists of the problem max\{c^T x: x ∈ R^n, A x ≤ b\}, where $A ∈ Q^{m×n}$ and $b ∈ Q^m$, then the algorithm runs in polynomial time in $m + n + s$, where $s$ is the largest binary encoding length of a rational number appearing in $A$ or $b$.

The question, whether there exists an algorithm which runs in time polynomial in $m + n$ and performs arithmetic operations on numbers, whose binary encoding length remains polynomial in $m + n + s$ is one of the most prominent open problems in theoretical computer science and discrete optimization.

Initially, the ellipsoid method can be used to solve the following problem.

Given a matrix $A ∈ Z^{m×n}$ and a vector $b ∈ Z^m$, determine a feasible point $x^*$ in the polyhedron $P = \{x ∈ R^n | A x ≤ b\}$ or assert that $P$ is not full-dimensional or $P$ is unbounded.

After we understand how the ellipsoid method solves this problem in polynomial time, we discuss why linear programming can be solved in polynomial time.

Clearly, we can assume that $A$ has full column rank. Otherwise, we can find with Gaussian elimination an invertible matrix $U ∈ R^{n×n}$ with $A·U = [A’|0]$ where $A’$ has full column rank. The system $A’x ≤ b$ is then feasible if and only if $Ax ≤ b$ is feasible.

**Exercise 1.** Let $x’$ be a feasible solution of $A’x ≤ b$ and suppose that $U$ from above is given. Show how to compute a feasible solution $x$ of $Ax ≤ b$. Also vice versa, show how to compute $x’$, if $x$ is given.

The unit ball is the set $B = \{x ∈ R^n | ∥x∥ ≤ 1\}$ and an ellipsoid $E(A, b)$ is the image of the unit ball under a linear map $t : R^n → R^n$ with $t(x) = Ax + b$, where $A ∈ R^{n×n}$ is an invertible matrix and $b ∈ R^n$ is a vector. Clearly

$$E(A, b) = \{x ∈ R^n | ∥A^{-1}x - A^{-1}b∥ ≤ 1\}. \quad (7.1)$$
Exercise 2. Consider the mapping $t(x) = \left(\frac{1}{2}, \frac{3}{2}\right)\left(\frac{x(1)}{x(2)}\right)$. 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 $V_n = \frac{1}{\pi n} (\frac{2e\pi}{n})^{n/2}$. 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 $H = \{x \in \mathbb{R}^n \mid \|x\| \leq 1, x(1) \geq 0\}$ is contained in the ellipsoid

$$E = \left\{ x \in \mathbb{R}^n \mid \left(\frac{n+1}{n}\right)^2 x(1) - \frac{1}{n+1} \right\}^2 + \frac{n^2-1}{n^2} \sum_{i=2}^{n} x(i)^2 \leq 1 \right\} \quad (7.2)$$

Fig. 7.1 Half-ball lemma.

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

$$\left(\frac{n+1}{n}\right)^2 x(1) - \frac{1}{n+1} \right\}^2 + \frac{n^2-1}{n^2} \sum_{i=2}^{n} x(i)^2 \leq 1 \quad (7.3)$$

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

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

$$\leq \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2} (1 - x(1)^2) \quad (7.4)$$
This shows that (7.3) holds if $x$ is contained in the half-ball and $x(1) = 0$ or $x(1) = 1$. Now consider the right-hand-side of (7.4) as a function of $x(1)$, i.e., consider

$$f(x(1)) = \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right)^2 + \frac{n^2-1}{n^2} (1-x(1)^2). \tag{7.5}$$

The first derivative is

$$f'(x(1)) = 2 \left(\frac{n+1}{n}\right)^2 \left(x(1) - \frac{1}{n+1}\right) - 2 \cdot \frac{n^2-1}{n^2} x(1). \tag{7.6}$$

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

In terms of a matrix $A$ and a vector $b$, the ellipsoid $E$ is described as

$$E = \{ x \in \mathbb{R}^n \mid \| A^{-1} x - A^{-1} b \| \leq 1 \},$$

where $A$ is the diagonal matrix with diagonal entries

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

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

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

which is bounded by

$$e^{-1/(n+1)} e^{(n-1)/(2(n^2-1))} = e^{-\frac{1}{2(n+1)}}. \tag{7.7}$$

We can conclude the following theorem.

**Theorem 1.** The half-ball $\{ x \in \mathbb{R}^n \mid x(1) \geq 0, \| x \| \leq 1 \}$ 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 2.** 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) $A = Q^T \text{diag}(\lambda_1, \ldots, \lambda_n) Q$, 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 $\mathcal{E}(A, a)$ is the set $\mathcal{E}(A, a) = \{ x \in \mathbb{R}^n \mid (x-a)^T A^{-1} (x-a) \leq 1 \}$, 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 $\mathcal{E}(A, a) \cap \{ c^T x \leq c^T a \}$.

Our goal is a similar lemma as the half-ball-lemma for ellipsoids. Geometrically it is clear that each half-ellipsoid $\mathcal{E}(A, a) \cap \{ c^T x \leq c^T a \}$ must be contained
in another ellipsoid $\mathcal{E}(A', b')$ with $\text{vol}(\mathcal{E}(A', a'))/\text{vol}(\mathcal{E}(A, a)) \leq e^{-1/(2n)}$. 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 $\mathcal{E}'(A', a')$. It is defined by

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

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

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

**The method**

Suppose we know the following things of our polyhedron $P$.

I) We have a number $L$ such that $\text{vol}(P) \geq L$ if $P$ is full-dimensional.

II) We have an ellipsoid $\mathcal{E}_{\text{init}}$ which contains $P$ if $P$ is bounded.

The ellipsoid method is now easily described.

Algorithm 1 (Ellipsoid method exact version).

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

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

c) If $\text{vol}(\mathcal{E}) < L$, then assert that $P$ is unbounded or $P$ is not full-dimensional

d) Otherwise, compute an inequality $c^T x \leq \beta$ which is valid for $P$ and satisfies $c^T a > \beta$ and replace $\mathcal{E}(A, a)$ by $\mathcal{E}(A', a)$ computed with formula (7.8) and goto step 5.

**Theorem 3.** The ellipsoid method computes a point in the polyhedron $P$ or asserts that $P$ is unbounded or not full-dimensional. The number of iterations is bounded by $2 \cdot n \ln(\text{vol}(\mathcal{E}_{\text{init}})/L)$.

**Proof.** Unless $P$ is unbounded, we start with an ellipsoid which contains $P$. This then holds for all the subsequently computed ellipsoids. After $i$ iterations one has

$$\text{vol}(\mathcal{E})/\text{vol}(\mathcal{E}_{\text{init}}) \leq e^{-\frac{i}{2n}}.$$  \hspace{1cm} (7.10)

Since we stop when $\text{vol}(\mathcal{E}) < L$, we stop at least after $2 \cdot n \ln(\text{vol}(\mathcal{E}_{\text{init}})/L)$ iterations. This shows the claim.
The separation problem

At this point we can already notice a very important fact. Inspect step d of the algorithm. What is required here? An inequality which is valid for \( P \) but not for the center \( a \) of \( \mathcal{C}(A,a) \). Such an inequality is readily at hand if we have the complete inequality description of \( P \) in terms of a system \( Cx \leq d \). Just pick an inequality which is violated by \( a \). Sometimes however, it is not possible to describe the polyhedron of a combinatorial optimization problem with an inequality system efficiently, simply because the number of inequalities is too large. An example of such a polyhedron is the matching polytope, see Theorem 7.

The great power of the ellipsoid method lies in the fact that we do not have to write down the polyhedron entirely. We only have to solve the so-called separation problem for the polyhedron, which is defined as follows.

**Separation Problem**

Given a point \( a \in \mathbb{R}^n \) determine, whether \( a \in P \) and if not, compute an inequality \( c^T x \leq \beta \) which is valid for \( P \) with \( c^T a > \beta \).

**Exercise 3.** We are given an undirected graph \( G = (V,E) \). A spanning tree \( T \) is a subset \( T \subseteq E \) of the edges such that \( T \) does not contain a cycle and \( T \) connects all the vertices \( V \). Consider the following spanning tree polytope \( P_{\text{span}} \)

\[
\sum_{e \in E} x(e) = n - 1 \quad (7.11)
\]

\[
\sum_{e \in \partial(U)} x(e) \geq 1 \quad \forall \emptyset \subset U \subset V \quad (7.12)
\]

\[
x(e) \leq 1 \quad \forall e \in E \quad (7.13)
\]

\[
x(e) \geq 0 \quad \forall e \in E \quad (7.14)
\]

Let \( x \) be an integral solution of \( P_{\text{span}} \) and define \( T = \{ e \in E \mid x(e) = 1 \} \). The inequality (7.11) ensures that exactly \( n - 1 \) edges are picked. The inequalities (7.12) ensure that \( T \) connects the vertices of \( G \). Thus \( T \) must be a spanning tree. Clearly, there are exponentially many inequalities of type (7.12). Nevertheless, a fractional solution of this polytope can be computed using the ellipsoid method.

Show that the separation problem for \( P_{\text{span}} \) can be solved in polynomial time.

**Hint:** To verify whether a vector \( x \in \mathbb{R}^{\left| E \right|} \) fulfills inequalities of type (7.12), it is a good idea to recall the MinCut or MaxFlow problem.

Via binary search even an optimal solution can be computed in polynomial time (in the input length) if we introduce edge costs (you don’t have to show that). In the next semester you will see that any optimal basis solution is integral and hence defines an optimal spanning tree w.r.t. the edge costs.

**Exercise 4.** Consider the triangle defined by
\[-x(1) - x(2) \leq -2
3x(1) \leq 4
-2x(1) + 2x(2) \leq 3.\]

Draw the triangle and simulate the ellipsoid method with starting ellipsoid being the ball of radius 6 around 0. Draw each of the computed ellipsoids with your favorite program (pstrics, maple …). How many iterations does the ellipsoid method take?

Ignore the occurring rounding errors!

**How to start and when to stop**

In our description of the ellipsoid method, we did not explain yet what the initial ellipsoid is and when we can stop with asserting that $P$ is either not full-dimensional or unbounded.

Suppose therefore that $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ 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 $b$. In this section we will show the following things.

i) The vertices of $P$ are in the box $\{x \in \mathbb{R}^n \mid -\frac{n}{2}B \leq x \leq \frac{n}{2}B\}$. Thus $P$ is contained in the ball around 0 with radius $nB$. Observe that the encoding length of this radius is size $(nB) = O(n \log n + n \text{size}(B))$ which is polynomial in the dimension $n$ and the largest encoding length of a coefficient of $A$ and $b$.

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

The following lemma is proved in any linear algebra course.

**Lemma 3 (Inverse formula and Cramer’s rule).** Let $C \in \mathbb{R}^{n \times n}$ be a nonsingular matrix. Then

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

where $C_{\bar{i}, \bar{j}}$ 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 $\frac{\det(\bar{C})}{\det(C)}$, where $\bar{C}$ arises from $C$ by replacing the $j$-th column with $d$.

We now define the size of a rational number $r = p/q$ with $p$ and $q$ relatively prime integers, a vector $c \in \mathbb{Q}^n$ and a matrix $A \in \mathbb{Q}^{m \times n}$:

- $\text{size}(r) = 1 + \lceil \log(|p| + 1) \rceil + \lceil \log(|q| + 1) \rceil$
- $\text{size}(c) = n + \sum_{i=1}^{n} \text{size}(c(i))$
- $\text{size}(A) = m \cdot n + \sum_{i=1}^{n} \sum_{j=1}^{m} \text{size}(A(i, j))$

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

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

(7.15)
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

\[
|\det(A)| \leq n^{n/2} B^n. \tag{7.16}
\]

Now let us inspect the vertices of a polyhedron \( P = \{ x \in \mathbb{R}^n \mid A x \leq b \} \), 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 \( A'x \leq b' \) is a subsystem of \( Ax \leq b \) and \( A' \) is invertible. Using Cramer’s rule and our observation (7.16) we see that the vertices of \( P \) lie in the box \( \{ x \in \mathbb{R}^n \mid -n^{n/2} B^n \leq x \leq n^{n/2} B^n \} \). 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 \( v_0, \ldots, v_n \) of \( P \) which span a simplex in \( \mathbb{R}^n \). The volume of this simplex is determined by the formula

\[
\frac{1}{n!} \left| \det \begin{pmatrix} 1 & \cdots & 1 \\ v_0 & \cdots & v_n \end{pmatrix} \right|. \tag{7.17}
\]

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 (7.17) is bounded by

\[
1/ \left( n^n (n^2 B^n)^{n+1} \right) \geq 1/ \left( n^{3n^2} B^{2n^2} \right) \geq 1/(n \cdot B)^{3 \cdot n^2}, \tag{7.18}
\]

which shows ii).

Now we plug these values into our analysis in Theorem 3. Our initial volume \( \text{vol}(E_{\text{init}}) \) is bounded by the volume of the box with side-lengths \( 2(n \cdot B)^n \). Thus

\[
\text{vol}(E_{\text{init}}) \leq (2 \cdot n \cdot B)^n. \tag{7.19}
\]

Above we have shown that

\[
L \geq 1/(n \cdot B)^{3n^2}. \tag{7.20}
\]

Clearly

\[
\text{vol}(E_{\text{init}})/L \leq (n \cdot B)^{4 \cdot n^2}. \tag{7.21}
\]

By Theorem 3 the ellipsoid method performs

\[
O\left(2 \cdot n \cdot \ln \left( (n \cdot B)^{4 \cdot n^2} \right) \right) \tag{7.22}
\]

iterations. This is bounded by

\[
O(n^3 \cdot \ln(n \cdot B)). \tag{7.23}
\]

Now recall that \( \log B \) is the number of \textit{bits} which are needed to encode the coefficient with the largest absolute value of the constraint system \( Ax \leq b \) and that \( n \) is the number of variables of this system. Therefore the expression (7.23) is poly-
nomial in the binary input encoding of the system $Ax \leq b$. We conclude the following theorem.

**Theorem 4.** The ellipsoid method (exact version) performs a polynomial number of iterations.

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 $P = \{x \in \mathbb{R}^n | Ax \leq b\}$ or assert that $P = \emptyset$.

**Boundedness**

We have argued that the matrix $A \in \mathbb{Z}^{m \times n}$ can be assumed to have full column rank. So, if $P$ is not empty, then $P$ does have at least one vertex. The vertices are contained in the box $\{x \in \mathbb{R}^n | -\frac{n}{2}B^n \leq x \leq \frac{n}{2}B^n\}$. Therefore, we can append the inequalities $-\frac{n}{2}B^n \leq x \leq \frac{n}{2}B^n$ to $Ax \leq b$ 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 5.** Let $P = \{x \in \mathbb{R}^n | Ax \leq b\}$ be a polyhedron and $\epsilon > 0$ be a real number. Show that $P_\epsilon = \{x \in \mathbb{R}^n | Ax \leq b + \epsilon \cdot 1\}$ is full-dimensional if $P \neq \emptyset$.

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

Recall Farkas’ Lemma (Theorem 2.9 of chapter 2) and Exercise 10 of chapter 2.

**Theorem 5.** The system $Ax \leq b$ does not have a solution if and only if there exists a nonnegative vector $\lambda \in \mathbb{R}^m_{\geq 0}$ 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 $Ax \leq b$ is not feasible, then there exists a $\lambda \geq 0$ such that $\lambda^T (A|b) = (0|1)$. We want to estimate the largest absolute value of a coefficient of $\lambda$ with Cramer’s rule and the Hadamard inequality. We can choose $\lambda$ such that the nonzero coefficients of $\lambda$ 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 \( \lambda \) such that \( |\lambda(i)| \leq (n \cdot B)^n \).

Now let \( \epsilon = 1/((n + 1) \cdot (n \cdot B)^n) \). Then \( |\lambda^T \cdot \epsilon| < 1 \) and thus

\[ A^T (b + \epsilon \cdot 1) < 0. \] (7.24)

Consequently the system \( Ax \leq b + \epsilon \cdot 1 \) is infeasible if and only if \( Ax \leq b \) is infeasible. Notice again that the encoding length of \( \epsilon \) is polynomial in the encoding length of \( Ax \leq b \) and we conclude with the main theorem of this section.

**Theorem 6.** The ellipsoid method can be used to decide whether a system of inequalities \( Ax \leq b \) 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 \( b \).

**The ellipsoid method for optimization**

Suppose that you want to solve a linear program

\[ \max \{ c^T x \mid x \in \mathbb{R}^n, \ Ax \leq b \} \] (7.25)

and recall that if \( (7.25) \) is bounded and feasible, then so is its dual and the two objective values are equal. Thus, we can use the ellipsoid method to find a point \((x, y)\) with \( c^T x = b^T y, \ Ax \leq b \) and \( A^T y = c, y \geq 0 \).

However, we mentioned that the strength of the ellipsoid method lies in the fact that we do not need to write the system \( Ax \leq b \) down explicitly. The only thing which has to be solvable is the separation problem. This is to be exploited in the next exercise.

**Exercise 6.** Show how to solve the optimization problem \( \max \{ c^T x \mid Ax \leq b \} \) with a polynomial number of calls to an algorithm which solves the separation problem for \( Ax \leq b \). You may assume that \( A \) has full column rank and the polynomial bound on the number of calls to the algorithm to solve the separation problem can depend on \( n \) and the largest size of a component of \( A, b \) and \( c \).

**Numerical issues**

We did not discuss the numerical details on how to implement the ellipsoid method such that it runs in polynomial time. One issue is crucial.

We only want to compute with a precision which is polynomial in the input encoding!
In the formula (7.8) the vector $b$ is defined by taking a square root. The question thus rises on how to round the numbers in the intermediate ellipsoids such that they can be handled on a machine. Also one has to analyze the growth of the numbers in the course of the algorithm. All these issues can be overcome but we do not discuss them in this course. I would like to refer you to the book of Alexander Schrijver \[4\] for further details. They are not difficult, but a little technical.

References