Lemma (Halb-Ellipsoid-Lemma)

Sei $E = p + \{x \in \mathbb{R}^n \mid x^t Q^{-1} x \leq 1\}$ ein Ellipsoid und $a \in \mathbb{R}^n$ mit $a^t Q a = 1$. Dann gilt

$$E \cap \{x \in \mathbb{R}^n \mid a^t x \geq a^t p\} \subseteq E'$$

mit

$$E' = p + \frac{1}{n+1} Q a + \left\{ x \in \mathbb{R}^n \mid \frac{n^2-1}{n^2} x^t \left(Q^{-1} + \frac{2}{n-1} a a^t \right) x \leq 1 \right\}.$$

Und: $\frac{\mathrm{vol}(E')}{\mathrm{vol}(E)} \leq e^{-\frac{1}{2(n+1)}}$.

E' heißt Löwner-John-Ellipsoid.

Beweis:
Sei M eine reguläre $n \times n$-Matrix mit $Q = MM^t$. O.B.d.A: $a^t M = e_1^t$ und somit $Qa = MM^t a = M(a^t M)^t = Me_1$ (sonst multipliziere M mit einer Rotationsmatrix, die $a^t M$ auf e_1 abbildet). Dann:

$$
\begin{aligned}
& E \cap \{x \in \mathbb{R}^n \mid a^t x \geq a^t p\} \\
= \;& (p + MB^n) \cap \{x \in \mathbb{R}^n \mid a^t x \geq a^t p\} \\
= \;& p + (MB^n \cap \{x \in \mathbb{R}^n \mid a^t (x + p) \geq a^t p\}) \\
= \;& p + (MB^n \cap \{x \in \mathbb{R}^n \mid a^t x \geq 0\}) \\
= \;& p + M(B^n \cap M^{-1}\{x \in \mathbb{R}^n \mid a^t x \geq 0\}) \\
= \;& p + M(B^n \cap \{x \in \mathbb{R}^n \mid a^t Mx \geq 0\}) \\
= \;& p + M(B^n \cap \{x \in \mathbb{R}^n \mid e_1^t x \geq 0\}) \\
\subseteq \;& p + \frac{1}{n+1} Me_1 + M \left\{ x \in \mathbb{R}^n \mid \frac{n^2 - 1}{n^2} x^t \left(I_n + \frac{2}{n-1} e_1 e_1^t \right) x \leq 1 \right\} \\
= \;& p + \frac{1}{n+1} Me_1 + \left\{ x \in \mathbb{R}^n \mid \frac{n^2 - 1}{n^2} (M^{-1}x)^t \left(I_n + \frac{2}{n-1} e_1 e_1^t \right) M^{-1} x \leq 1 \right\} \\
= \;& p + \frac{1}{n+1} Qa + \left\{ x \in \mathbb{R}^n \mid \frac{n^2 - 1}{n^2} x^t \left(Q^{-1} + \frac{2}{n-1} aa^t \right) x \leq 1 \right\}
\end{aligned}
$$

Beweis (Fortsetzung):

Wir können E' in Standardform schreiben als

$$E' = p + \frac{1}{n+1} Qa + \left\{ x \in \mathbb{R}^n \mid x^t \tilde{Q}^{-1} x \leq 1 \right\}$$

mit

$$\tilde{Q} = \frac{n^2}{n^2-1}\left(Q - \frac{2}{n+1} Qaa^tQ^t \right).$$

Denn:

$$\begin{aligned} & \frac{n^2-1}{n^2}\left(Q^{-1} + \frac{2}{n-1} aa^t \right) \overbrace{\frac{n^2}{n^2-1}\left(Q - \frac{2}{n+1} Qaa^tQ^t \right)}^{\tilde{Q}} \\ = \quad & I_n - \frac{2}{n+1} aa^tQ^t + \frac{2}{n-1} aa^tQ - \frac{4}{n^2-1} a \underbrace{a^tQa}_{=1} a^tQ^t \\ = \quad & I_n. \end{aligned}$$

Beweis (Fortsetzung):

$$\Rightarrow \frac{\mathrm{vol}(E')}{\mathrm{vol}(E)} = \sqrt{\frac{\det(\tilde{Q})}{\det(Q)}}. \qquad \tilde{Q} = Q \cdot (*)$$

Es gilt

$$\begin{aligned}
\frac{\det(\tilde{Q})}{\det(Q)} &= \det\left(\overbrace{\frac{n^2}{n^2-1}\left(I_n - \frac{2}{n+1}aa^tQ^t\right)}^{(*)}\right) \\
&= \left(\frac{n^2}{n^2-1}\right)^n \det\left(I_n - \frac{2}{n+1}aa^tQ^t\right) \\
&= \left(\frac{n^2}{n^2-1}\right)^n \left(1 - \frac{2}{n+1}\right).
\end{aligned}$$

Eigenwerte von $I_n - \frac{2}{n+1} aa^tQ^t$

$1 - \frac{2}{n+1}$ (zum Eigenvektor a) und 1

Determinante ist Produkt der Eigenwerte

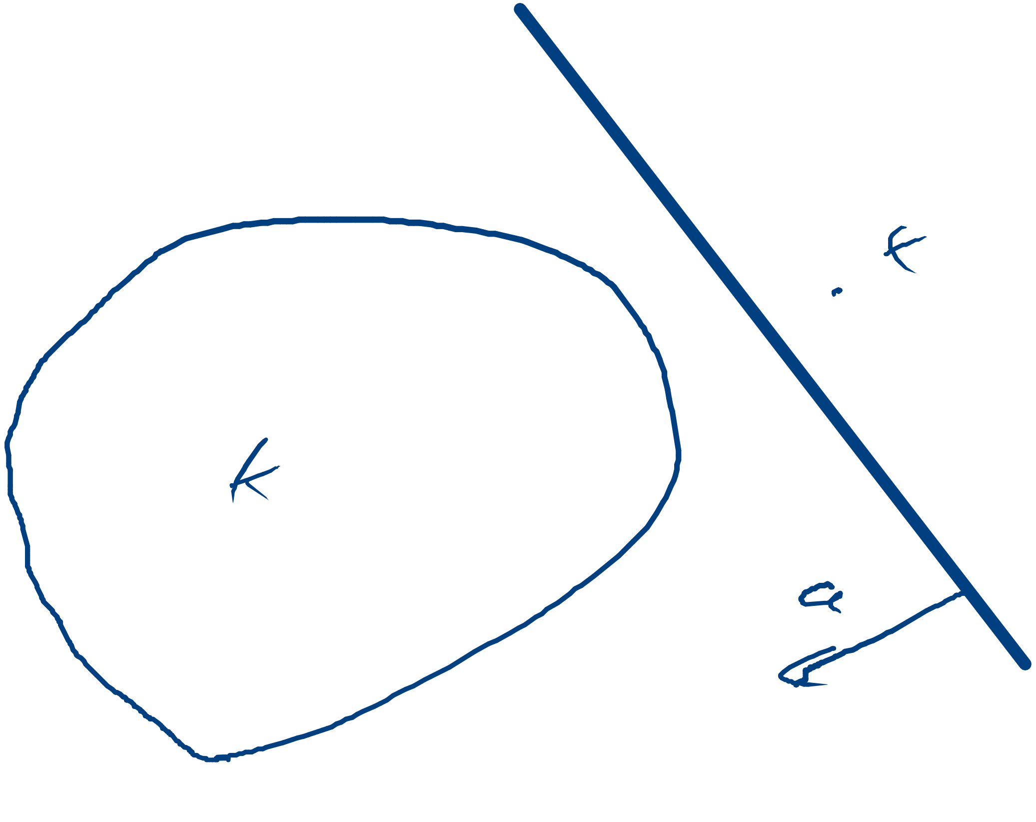
$$\Rightarrow \sqrt{\frac{\det(\tilde{Q})}{\det(Q)}} \le \left(\frac{n^2}{n^2-1}\right)^{\frac{n}{2}} \left(1 - \frac{2}{n+1}\right)^{\frac{1}{2}} = \frac{n}{n+1}\left(\frac{n^2}{n^2-1}\right)^{\frac{n-1}{2}} \le e^{-\frac{1}{2(n+1)}} \qquad \square$$

wie beim Halbkugel-Lemma

Definition:

Ein **Separationsorakel** für eine konvexe Menge $K \subseteq \mathbb{R}^n$ ist ein Black-Box-Algorithmus, der zu gegebenem $x \in \mathbb{R}^n$ entweder einen Vektor $a \in \mathbb{R}^n$ mit $a^t y > a^t x$ für alle $y \in K$ zurückgibt oder ausgibt, dass $x \in K$ gilt.

Beobachtung: Zu gegebenem $A \in \mathbb{Q}^{m \times n}$ und $b \in \mathbb{Q}^m$, kann ein Separationsorakel für $\{x \in \mathbb{R}^n \mid Ax \leq b\}$ in $O(mn)$ arithmetischen Operationen implementiert werden.



Algorithm 6: Idealized Ellipsoid Algorithm

Input: A separation oracle for a closed convex set $K \subseteq \mathbb{R}^n$, a number $R > 0$ with $K \subseteq \{x \in \mathbb{R}^n \mid x^t x \leq R^2\}$, and a number $\epsilon > 0$.

Output: An $x \in K$ or the message "$\mathrm{vol}(K) < \epsilon$".

$p_0 := 0$, $A_0 := R^2 I_n$;

for $k = 0, \ldots, N(R, \epsilon) := \lfloor 2(n+1)(n \ln(2R) + \ln(\frac{1}{\epsilon})) \rfloor$ **do**

  if $p_k \in K$ **then**

    return p_k;

  Let $\bar{a} \in \mathbb{R}^n$ be a vector with $\bar{a}^t y > \bar{a}^t p_k$ for all $y \in K$;

  $b_k := \frac{A_k \bar{a}}{\sqrt{\bar{a}^t A_k \bar{a}}}$;

  $p_{k+1} := p_k + \frac{1}{n+1} b_k$;

  $A_{k+1} := \frac{n^2}{n^2-1}(A_k - \frac{2}{n+1} b_k b_k^t)$;

return "$\mathrm{vol}(K) < \epsilon$";

$a := \frac{\bar{a}}{\sqrt{\bar{a}^t A_k \bar{a}}}$

$a^t A_k a = 1$

Theorem

Zu einem durch eine Separationsorakel gegebenem $K \subseteq \mathbb{R}^n$, $\epsilon > 0$, und R mit $K \subseteq \{x \in \mathbb{R}^n \mid x^t x \leq R^2\}$ kann man mit $O(n(n\ln(R) + \ln(\frac{1}{\epsilon})))$ Iterationen des IDEALISIERTEN ELLIPSOID-VERFAHRENS ein $x \in K$ berechnen oder (korrekterweise) “$\text{vol}(K) < \epsilon$” ausgeben. Jede Iteration benötigt einen Orakelaufruf, $O(n^2)$ arithmetische Standardoperationen und die Berechnung einer Quadratwurzel von einer reellen Zahl.

<u>Beweis:</u> Zeige: In jeder Iteration ist K enthalten in $P_k = \{x \in \mathbb{R}^n : x^t A_k^{-1} x \leq 1\}$

$k = 0$: trivial.

Für den Induktionsschritt werde das Halb-Ellipsoid-Lemma auf $Q = A_k$ und $a = \frac{\bar{a}}{\sqrt{\bar{a}^t A_k \bar{a}}}$ an

Und: $\mathrm{vol}(\{x \in \mathbb{R}^n : x^t x \leq R\}) \leq \mathrm{vol}([-R,R]^n)$
$= 2^n \cdot R^n$

In jeder Iteration wird das Volumen von E_k (das durch p_k und A_k gegebene Ellipsoid) um mindestens den Faktor

$e^{-\frac{1}{2(n+1)}}$ verringert.

$$\Rightarrow \operatorname{vol}(E_k) \le e^{-\frac{k}{2(n+1)}} 2^n R^n$$

Betrachte kleinstes k mit

$$e^{-\frac{k}{2(n+1)}} 2^n R^n \le \varepsilon$$

$$\Leftrightarrow \frac{k}{2(n+1)} \ge \ln\left(\frac{2^n R^n}{\varepsilon}\right)$$

$$\Leftrightarrow k \ge 2(n+1)\left(n \cdot \ln(2R) + \ln\left(\frac{1}{\varepsilon}\right)\right) \qquad \square$$

Fehler-Analyse

Problem:

Wir können in $b_k := \frac{A_k \bar{a}}{\sqrt{\bar{a}^t A_k \bar{a}}}$ die Wurzel nicht exakt ausrechnen.

$\Rightarrow$ Wir müssen mit gerundeten Zwischenlösungen rechnen.

$\widetilde{p_k}$ und $\widetilde{A_k}$: exakte Werte
p_k und A_k: gerundete Werte

Aber: $\widetilde{p_k}$ und $\widetilde{A_k}$ werden aus den gerundeten Werten p_{k-1} und A_{k-1} berechnet.

$\widetilde{E_k}$ und E_k seien die zugehörigen Ellipsoide

Sei δ eine obere Schranke für den absoluten Rundungsfehler, also $\|p_k - \widetilde{p_k}\|_\infty \leq \delta$ und $\|A_k - \widetilde{A_k}\|_\infty \leq \delta$.

Beim Runden der Einträge in $\widetilde{A_k}$ sorgen wir dafür, dass die Matrix symmetrisch bleibt.

Let $\Gamma_k = A_k - \widetilde{A_k}$ and $\Delta_k = p_k - \widetilde{p_k}$.

Es sei $\|\cdot\|$ für Vektoren die Euklidische Norm und für Matrizen die induzierte Operator-Norm.

Können annehmen:

Für jedes $x \in K$ gilt $(x - \widetilde{p}_k)^t \widetilde{A_k}^{-1} (x - \widetilde{p}_k) \leq 1$

Für p_k und A_k muss das aber nicht gelten.

$\Rightarrow$ Vergrößere das Ellipsoid in jeder Iteration leicht durch Skalierung von $\widetilde{A_k}$ um den Faktor $\mu = 1 + \frac{1}{2n(n+1)}$.

$\Rightarrow$ Ersetze $\widetilde{A_k}$ durch $\mu \widetilde{A_k}$ (und nenne das Ergebnis wieder $\widetilde{A_k}$!).

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

Dann: für $x \in K$:

$$(x - \widetilde{p}_k)^t \widetilde{A_k}^{-1} (x - \widetilde{p}_k) \leq \frac{1}{1 + \frac{1}{2n(n+1)}} = \frac{2n^2 + 2n}{2n^2 + 2n + 1} < 1 - \frac{1}{4n^2}.$$

Es gilt für $x \in \mathcal{E}_k$:

$$
\begin{aligned}
(x-p_k)^t A_k^{-1}(x-p_k) \quad = \quad & (x-p_k)^t \widetilde{A_k}^{-1}(x-p_k) + \\
& (x-p_k)^t (A_k^{-1} - \widetilde{A_k}^{-1})(x-p_k).
\end{aligned}
$$

Beschränkung der Summanden: $x - p_k = (x - \widetilde{p_k}) + (\widetilde{p_k} - p_k)$

$$
\begin{aligned}
& (x-p_k)^t \widetilde{A_k}^{-1}(x-p_k) \\
= \quad & (x-\widetilde{p_k})^t \widetilde{A_k}^{-1}(x-\widetilde{p_k}) + |2\Delta_k^t \widetilde{A_k}^{-1}(x-\widetilde{p_k})| + \Delta_k^t \widetilde{A_k}^{-1}\Delta_k \\
\leq \quad & 1 - \frac{1}{4n^2} + 2\|\Delta_k\| \cdot \|\widetilde{A_k}^{-1}\| \; (R + \|\widetilde{p_k}\|) + \|\Delta_k\|^2 \cdot \|\widetilde{A_k}^{-1}\| \\
\leq \quad & 1 - \frac{1}{4n^2} + 2\sqrt{n}\delta \; \|\widetilde{A_k}^{-1}\| \; (R + \|\widetilde{p_k}\|) + n\delta^2 \|\widetilde{A_k}^{-1}\|.
\end{aligned}
$$

Und:

$$
\begin{aligned}
& (x-p_k)^t (A_k^{-1} - \widetilde{A_k}^{-1})(x-p_k) \\
\leq \quad & \|x-p_k\|^2 \cdot \|A_k^{-1} - \widetilde{A_k}^{-1}\| \\
\leq \quad & (R + \|p_k\|)^2 \; \|A_k^{-1}(A_k - \widetilde{A_k})\widetilde{A_k}^{-1}\| \\
\leq \quad & (R + \|p_k\|)^2 \; \|A_k^{-1}\| \cdot \|\widetilde{A_k}^{-1}\| \cdot \|\Gamma_k\| \\
\leq \quad & (R + \|p_k\|)^2 \; \|A_k^{-1}\| \cdot \|\widetilde{A_k}^{-1}\| \cdot n\delta
\end{aligned}
$$

Wunsch an δ

$$\begin{aligned}\frac{1}{4n^2} \geq\ & 2\sqrt{n}\delta\ \|\widetilde{A_k}^{-1}\|\ (R+\|\widetilde{p_k}\|) + n\delta^2\|\widetilde{A_k}^{-1}\| \\ & +(R+\|p_k\|)^2\ \|A_k^{-1}\|\cdot\|\widetilde{A_k}^{-1}\|n\delta\end{aligned}$$

Auswirkungen der Skalierung auf das Volumen

$\widetilde{E_{k+1}}$ gehöre zur skalierten Version von $\widetilde{A_k}$:

$$\frac{\mathrm{vol}(\widetilde{E_{k+1}})}{\mathrm{vol}(E_k)} \le e^{-\frac{1}{2(n+1)}} \Bigg(\underbrace{1 + \frac{1}{2n(n+1)}}\Bigg)^{\frac{n}{2}} \le e^{-\frac{1}{2(n+1)}} e^{\frac{1}{4(n+1)}} = e^{-\frac{1}{4(n+1)}}.$$

Dann

$$\frac{\mathrm{vol}(E_{k+1})}{\mathrm{vol}(E_k)} = \frac{\mathrm{vol}(\widetilde{E_{k+1}})}{\mathrm{vol}(E_k)} \frac{\mathrm{vol}(E_{k+1})}{\mathrm{vol}(\widetilde{E_{k+1}})} \le e^{-\frac{1}{4(n+1)}} \sqrt{\det(A_{k+1}\widetilde{A_{k+1}}^{-1})}$$

Es gilt

$$\begin{aligned}
\det(A_{k+1}\widetilde{A_{k+1}}^{-1}) &= \det\left(I_n + (A_{k+1} - \widetilde{A_{k+1}})\widetilde{A_{k+1}}^{-1}\right) \\
&\overset{(*)}{\le} \|I_n + (A_{k+1} - \widetilde{A_{k+1}})\widetilde{A_{k+1}}^{-1}\|^n \\
&\le (1 + \|\Gamma_{k+1}\| \cdot \|\widetilde{A_{k+1}}^{-1}\|)^n \\
&\le (1 + n\delta\|\widetilde{A_{k+1}}^{-1}\|)^n \\
&\le e^{n^2\delta\|\widetilde{A_{k+1}}^{-1}\|},
\end{aligned}$$

wobei Ungleichung $(*)$ daraus folgt, dass für eine $n \times n$-Matrix A mit Spalten $a_1, \dots, a_n$ gilt: $|\det(A)| \le \prod_{i=1}^{n} \|a_i\|$ (siehe Übungen).

Daraus folgt:

$$\frac{\mathrm{vol}(E_{k+1})}{\mathrm{vol}(E_k)} \leq e^{-\frac{1}{4(n+1)}} \cdot e^{\frac{1}{2}n^2\delta\|\widetilde{A_{k+1}}^{-1}\|}.$$

$\Rightarrow$ Wenn $\frac{1}{2}\delta\|\widetilde{A_{k+1}}^{-1}\| < \frac{1}{8(n+1)^3}$ gilt, dann folgt $\frac{\mathrm{vol}(E_{k+1})}{\mathrm{vol}(E_k)} < e^{-\frac{1}{8(n+1)}}$.

$\Rightarrow$ Neuer Wunsch:

$\delta\|\widetilde{A_{k+1}}^{-1}\| \leq \frac{1}{4(n+1)^3}$

$\Rightarrow$ Unser Ziel ist δ so zu wählen, dass die folgenden Ungleichungen gelten:

- $2\sqrt{n}\delta \; \|\widetilde{A_k}^{-1}\| \; (R + \|\widetilde{p_k}\|) + n\delta^2 \|\widetilde{A_k}^{-1}\| + (R + \|p_k\|)^2 \; \|A_k^{-1}\| \cdot \|\widetilde{A_k}^{-1}\| n\delta \quad \leq \quad \frac{1}{4n^2}$
- $\delta \|\widetilde{A_{k+1}}^{-1}\| \quad \leq \quad \frac{1}{4(n+1)^3}$

Satz

Es sei in Iteration k der ELLIPSOID-METHODE $\delta \leq \frac{1}{12n4^k}$ gewählt. Dann gilt:

(a) A_k ist positiv definit.

(b) $\|p_k\| \leq R2^k$, $\|\widetilde{p_k}\| \leq R2^k$.

(c) $\|A_k\| \leq R^2 2^k$, $\|\widetilde{A_k}\| \leq R^2 2^k$.

(d) $\|A_k^{-1}\| \leq R^{-2} 4^k$, $\|\widetilde{A_k}^{-1}\| \leq R^{-2} 4^k$.

Beweis:

Es gilt

$$\widetilde{A_{k+1}}^{-1} = \frac{n^2-1}{n^2}\frac{1}{\mu}\left(\underbrace{A_k^{-1}}_{pos.\ def.} + \underbrace{\frac{2}{n-1}\frac{\bar{a}\bar{a}^t}{\bar{a}^t A_k \bar{a}}}_{pos.\ semidef.}\right).$$

$\Rightarrow \widetilde{A_{k+1}}^{-1}$ ist positiv definit.

$\Rightarrow \widetilde{A_{k+1}} = \frac{n^2}{n^2-1}\mu(A_k - \frac{2}{n+1}b_k b_k^t)$ ist positiv definit.

Zeige induktiv:

- A_k ist positiv definit und
- $\|{A_k}^{-1}\| \leq R^{-2}4^k$.

$$\|A_k^{-1}\| \geq \frac{1}{\|A_k\|} = \frac{1}{\max\{\frac{x^tAx}{x^tx} : x \neq 0\}}$$

Es gilt: $\|\frac{\bar{a}\bar{a}^t}{\bar{a}^t A_k \bar{a}}\| = \frac{\bar{a}^t\bar{a}}{\bar{a}^t A_k \bar{a}} \leq \left(\min\{x^t A_k x \mid \|x\| = 1\}\right)^{-1} \leq \|A_k^{-1}\|$.

Daher:

$$\|\widetilde{A_{k+1}}^{-1}\| \leq \frac{n^2-1}{n^2}\frac{1}{\mu}\left(\|A_k^{-1}\| + \frac{2}{n-1}\|\frac{\bar{a}\bar{a}^t}{\bar{a}^t A_k \bar{a}}\|\right) \leq 3\|{A_k}^{-1}\|$$