Elipsoidová metoda - poznámky k přednášce

Petr Kolman

Říjen 2009

1 Náčrt algoritmu

Zadání: Pro daný mnohostěn $P = \{x \mid Ax \leq b\}$ najít $x \in P$, pokud existuje, a v opačném případě rozpoznat, že P je prázdný.

V tomto textu popíšeme tzv. elipsoidovou metodu, což je algoritmus, který daný problém řeší v polynomiálním čase vzhledem k velikosti zadání (podrobnosti níže).

Pro zjednodušení popisu algoritmu budeme prozatím o mnohostěnu P předpokládat:

P1 P je omezený (tj. celý P se vejde do koule o dostatečně velkém průměru),

P2 Je-li P neprázdný, pak je plné dimenze (tj. pro dostatečně malé $\epsilon > 0$ se do P vejde celá koule s průměrem ϵ).

Hrubý náčrt algoritmu: Najdeme dostatečně velký elipsoid E_0 takový, aby obsahoval celý mnohostěn P (předpoklad P1 zaručuje, že takový elipsoid existuje) a opakovaně provádíme následující. Pokud střed z_k elipsoidu E_k leží uvnitř P, našli jsme požadované řešení. V opačném případě víme, že z_k porušuje nějakou nerovnost ze systému $Ax \leq b$. Vezmeme poloprostor odpovídající porušené nerovnosti a posuneme ho tak, aby jeho hranice procházela bodem z_k; označme H_k tento posunutý poloprostor. Pak celý mnohostěn P leží v průniku elipsoidu E_k s poloprostorem H_k. Najdeme nový (menší) elipsoid E_{k+1} obsahující $E_k \cap H_k$ a krok opakujeme.

Jak poznáme, že je P prázdný a že můžeme přestat s konstrukcí nových elipsoidů? Využijeme náš druhý předpoklad P2. Je-li P neprázdný, je možno na základě A a b spočítat dolní odhad na objem P. Pokud zajistíme, že objem elipsoidu E_{k+1} je vždy výrazně menší než objem elipsoidu E_k, pak po dostatečném počtu kroků budeme vědět, že neprázdný P by se již díky svému objemu do elipsoidu E_l, pro dostatečně velké l, nevešel a tudíž P musí být prázdný.

Abychom dostatečně popsali elipsoidovou metodu (za výše uvedených předpokladů P1 a P2), potřebujeme zodpovědět tyto otázky:

1. Jak na počátku volit elipsoid E_0 tak, aby $P \subseteq E_0$?
2. Jak ze starého elipsoidu E_k spočítat nový E_{k+1}, neboli jak volit parametry nového, aby obklopoval, co má, a přitom byl co do objemu podstatně menší?
3. Kolik iterací je třeba provést k nalezení $x \in P$ nebo k rozpoznání, že P je prázdné?

Dále bude třeba ukázat, jak se předpokladů P1 a P2 zbavit. Než se ale těmto otázkám budeme věnovat, zavedeme a připomeneme některé základní potřebné pojmy a skutečnosti.

2 Terminologie a opakovaní z lineární algebry

Opakovaně budeme pracovat s vektory $\mathbf{0} = (0, 0, \ldots, 0)^T$ a $e_1 = (1, 0, \ldots, 0)^T$. Porovnání vektorů (případně matic) provádíme po složkách: pro vektory $x, y \in \mathbb{R}^n$ píšeme $x \leq y$, pokud $x_i \leq y_i$ pro $i = 1, \ldots, n$. Jednotkovou matici značíme I.

Definice 1 *Symetrickou matici $A \in \mathbb{R}^{n\times n}$ nazýváme positivně definitní, jestliže $\forall x \neq 0$ platí $x^T Ax > 0$.*

Tvrzení 2 *Pro pozitivně definitní matici A platí:*

- *inverzní matice A^{-1} je také pozitivně definitní,*
- *existuje právě jedna pozitivně definitní matice Q taková, že $A = Q^T \cdot Q$; takovou matici Q značíme $A^{1/2}$.*

Pro nás bude důležitá poslední vlastnost.

Definice 3 *Množinu*

$$E(a, A) = \{x \in \mathbb{R}^n : (x - a)^T A^{-1}(x - a) \leq 1\} \ ,$$

kde A je pozitivně definitní matice, budeme nazývat elipsoidem se středem v a a určeným maticí A.

Příklad 4 $E(\boldsymbol{0}, I) = \{x \in \mathbb{R}^n \mid x^T x \leq 1\}$ *- jednotková koule se středem v počátku.*

Definice 5 *Zobrazení $T : \mathbb{R}^n \to \mathbb{R}^n$ nazýváme* afinní zobrazení, *pokud je dáno předpisem $T(x) = Qx + s$, kde $Q \in \mathbb{R}^{n\times n}$ je matice a $s \in \mathbb{R}^n$ je vektor (tj. T je složením lineárního zobrazení a posunutí).*

Tvrzení 6 *Každý elipsoid je afinním obrazem jednotkové koule: $E(a, A) = A^{1/2} \cdot E(\boldsymbol{0}, I) + a$.*

Důkaz. $E(a, A) = \{x \in \mathbb{R}^n : (x - a)^T A^{-1}(x - a) \leq 1\} = \{x \in \mathbb{R}^n : (x - a)^T \cdot {A^{-1/2}}^T \cdot A^{-1/2} \cdot (x - a) \leq 1\}$. Označme $y = A^{-1/2} \cdot (x - a)$. Potom $A^{1/2}y + a = x$. Dosadíme-li do formule popisující elipsoid, získáme (uvědomme si, že $A^{-1/2}$ je také positivně definitní matice, tudíž je symetrická a $A^{-1/2} = {A^{-1/2}}^T$):

$$E(a, A) = \{(A^{1/2}y + a) \in \mathbb{R}^n : y^T y \leq 1\} = A^{1/2} \cdot E(\mathbf{0}, I) + a \ .$$

□

Pro $T \subseteq \mathbb{R}^n$ budeme $vol(T)$ označovat objem množiny T.

Tvrzení 7 *Pro afinní zobrazení $T : \mathbb{R}^n \to \mathbb{R}^n$ dané předpisem $T(x) = Qx + t$ a množinu $X \subseteq \mathbb{R}^n$ platí:*

$$vol(T(X)) = |det(Q)| \cdot vol(X).$$

V případě elipsoidů:

$$vol(E(a, A)) = |det(A^{1/2})| \cdot vol(E(\mathbf{0}, I)).$$

Pozorování 8 *Pro objem elipsoidu $E(a, A)$ platí:*

$$|det(A^{1/2})| \cdot n^{-n} \leq \ vol(E(a, A)) \leq |det(A^{1/2})| \cdot 2^n \ .$$

Odhady se opírají o objem krychle vepsané resp. opsané.

Definice 9 Velikost zápisu. *Pro celé číslo k značíme $\langle k\rangle = 1 + \lceil \log_2(|k| + 1)\rceil$, což je počet bitů potřebných pro zápis k včetně znaménka. Podobně pro racionální číslo $r = \frac{p}{q}$, kde p a q jsou nesoudělná, značíme $\langle r\rangle = \langle p\rangle + \langle q\rangle$. Pro racionální vektor $v \in \mathbb{Q}^n$ značíme $\langle v\rangle = \sum_{i=1}^{n} \langle v_i\rangle$ a pro matici $A \in \mathbb{Q}^{m\times n}$ obdobně $\langle A\rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} \langle a_{i,j}\rangle$.*

3 Počáteční elipsoid

Lemma 10 *Je-li $P = \{x \mid Cx \leq d\} \subseteq \mathbb{Q}^n$ omezený mnohostěn a C a d jsou celočíselné, pak všechny vrcholy P jsou obsaženy v kouli se středem v počátku a poloměrem $R = \sqrt{n} \cdot 2^{\langle C,d\rangle + n\log n}$.*

Důkaz. Uvažme libovolný vrchol $\mathbf{v}$ polytopu P. Z teorie mnohostěnů víme (např. [1]), že pak existuje podsystém nerovností $C'x \leq d'$ (vybraný ze systému nerovností $Cx \leq d$) takový, že $\mathbf{v}$ je jediným řešením $C'x = d'$. Z Cramerova pravidla dostáváme: $v_i = \frac{\det(C'_i)}{\det(C')}$, kde C'_i je matice vzniklá z C' nahrazením i-tého sloupce vektorem d'. Protože matice C' je celočíselná a regulární, máme $|det(C')| \geq 1$. Pro horní odhad velikosti v_i užijeme následující horní odhad velikosti determinantu.

Pozorování 11 *Nechť C je celočíselná matice $n \times n$. Pak $|det\ (C)| \leq 2^{\langle C\rangle + n\log n}$*

Důkaz. $|\det C| \leq \sum_{\pi\in S_n} |\prod_{i=1}^{n} c_{i,\pi(i)}| \leq \sum_{\pi\in S_n} \prod_{i=1}^{n} 2^{\langle c_{i,\pi(i)}\rangle} \leq \sum_{\pi\in S_n} 2^{\langle C\rangle} \leq n! 2^{\langle C\rangle} \leq 2^{\langle C\rangle + n\log n}$.

Úpravy se ubírají takto: Při první nerovnosti zanedbáme znaménka permutací π z definice determinantu. Druhá nerovnost využívá definice délky zápisu čísla: $|a| \leq 2^{\langle a\rangle}$. V další nerovnosti využijeme pravidel pro počítání s exponenty a navíc součet délek zápisu n prvků matice (hrubě) shora odhadneme součtem délek zápisu všech prvků matice. Počet permutací n-prvkové množiny je $n!$, což (hrubě) shora odhadneme $n! \leq n^n \leq 2^{n\log n}$. □

K dokončení důkazu Lemmatu 10 si všimneme, že $\langle C'_i\rangle \leq \langle C, d\rangle$. Zbývá upočítat délku vektoru o všech složkách velikosti nejvýše $2^{\langle C,d\rangle + n\log n}$: $||\mathbf{v}|| \leq \sqrt{\sum_{i=1}^{n} (2^{\langle C,d\rangle + n\log n})^2} = \sqrt{n} \cdot 2^{\langle C,d\rangle + n\log n}$, což je hledaný poloměr R. □

Jako počáteční elipsoid E_1 použijeme tedy kouli $E(0, R \cdot I)$.

4 Iterační krok: výpočet E_{k+1} z E_k

4.1 Snadný případ: $E_k = E(\mathbf{0}, I)$ a $H_k = \{x \mid x_1 \leq 0\}$

V této části předpokládáme, že $E_k = E(\mathbf{0}, I)$ a $H_k = \{x \mid x_1 \leq 0\}$. Pro zjednodušení zápisu (ušetření indexů) budeme používat značení B místo E_k (jedná se o jednotkovou kouli kolem počátku) a H místo H_k. Máme tedy $B = \{x \in \mathbb{R}^n | x^T x \leq 1\}$, $H = \{x \in \mathbb{R}^n | e_1^T x \leq 0\}$ a označme $B^- = B \cap H$ "zápornou" polovinu jednotkové koule se středem v počátku, to jest

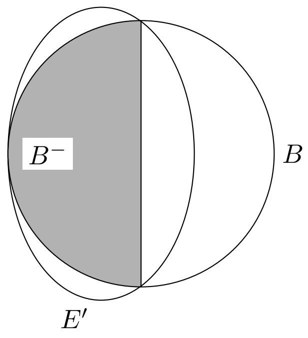
$$B^- = \{x \in \mathbb{R}^n | x^T x \leq 1, x_1 \leq 0\}.$$

Hledáme elipsoid E' obsahující B^-, který bude "malý". Přesněji, chceme, aby $\mathrm{vol}(E') \leq q \cdot \mathrm{vol}(E)$ pro nějakou konstantu $q < 1$. Protože množina B^- je symetrická kolem osy x_1, budeme hledat E' ve tvaru

$$E' = \{x \in \mathbb{R}^n | (x - z)^T Z^{-1} (x - z) \leq 1\},$$

kde $z = t \cdot e_1$ pro $t \in \mathbb{R}^-$ a Z je diagonální matice. Uvažme jednotkovou matici I. Pokud prvek $I_{1,1}$ zmenšíme, získáme matici zobrazení smršťujícího v první souřadnici. Naopak pokud prvek $I_{1,1}$ zvětšíme, zobrazení bude v tomto směru „roztahovat". Podobně pro ostatní $I_{i,i}$. Vezměme tedy $0 < p < 1$ a $d > 1$ a diagonální matici Z takovou, že

$$Z^{-1} = \begin{pmatrix} \frac{1}{p^2} & & & & \\ & \frac{1}{d^2} & & & \\ & & \frac{1}{d^2} & & \\ & & & \ddots & \\ & & & & \frac{1}{d^2} \end{pmatrix}.$$



Obrázek 1: Hledané E'.

Chceme, aby se náš nový elipsoid E' toho původního $E = B$ dotýkal v bodech $-e_1$ a e_2 (viz. obr. 1) a ze všech takových chceme ten s nejmenším objemem. Z první podmínky na dotek dostáváme následující omezení:

$$(-1-t)e_1^T \begin{pmatrix} \frac{1}{p^2} & & & & \\ & \frac{1}{d^2} & & & \\ & & \frac{1}{d^2} & & \\ & & & \ddots & \\ & & & & \frac{1}{d^2} \end{pmatrix} (-1-t)e_1 = 1$$

a tedy:

$$\frac{(1+t)^2}{p^2} = 1 \ .$$

Ze druhé podmínky na dotek dostáváme:

$$(-t, 1, 0, ..., 0) \begin{pmatrix} \frac{1}{p^2} & & & & \\ & \frac{1}{d^2} & & & \\ & & \frac{1}{d^2} & & \\ & & & \ddots & \\ & & & & \frac{1}{d^2} \end{pmatrix} \begin{pmatrix} -t \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 1 \ ,$$

tedy

$$\frac{t^2}{p^2} + \frac{1}{d^2} = 1 \ .$$

Z výše uvedených výrazů vyjádříme $1/p^2$ a $1/d^2$ jako funkce proměnné t:

$$\frac{1}{p^2} = \frac{1}{(1+t)^2}, \quad \frac{1}{d^2} = \frac{1+2t}{(1+t)^2} \quad .$$

Nyní máme dvě podmínky na tři proměnné. Třetí podmínku získáme z požadavku na minimální objem elipsoidu E', pro který podle Tvrzení 7 platí $vol(E') = \sqrt{|det(Z)|}vol(B)$, což je rovno

$$vol(E') = pd^{n-1}vol(B) = \frac{(1+t)^n}{\sqrt{(1+2t)^{n-1}}}vol(B) \ .$$

Snadno ověříme, že $vol(E')$ jako funkce proměnné t nabývá svého minima pro

$$t = \frac{-1}{n+1} \ .$$

Dosazením za p, d a t dostáváme, že hledaný elipsoid E' je tvaru

$$E' = \left\{ x \in \mathbb{R}^2 \mid (x + \frac{1}{n+1}e_1)^T \begin{pmatrix} \frac{(n+1)^2}{n^2} & 0 & \dots & 0 \\ 0 & \frac{n^2-1}{n^2} & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & \frac{n^2-1}{n^2} \end{pmatrix} (x + \frac{1}{n+1}e_1) \leq 1 \right\} .$$

Pro kontrolu ověříme, že elipsoid E' vskutku obsahuje celou "zápornou polovinu" koule B, tedy že $B^- \subseteq E'$. Víme, že pro $x \in B^-$ platí $x^T x \leq 1$, $x_1 \leq 0$. Rozepsáním podmínky v zápisu E' dostaneme

$$\left(\frac{n+1}{n}\right)^2 (x_1 + \frac{1}{1+n})^2 + \left(\frac{n^2-1}{n^2}\right) \sum_{i=2}^{n} x_i^2 \leq 1 .$$

Podle předpokladů $\sum_{i=1}^{n} x_i^2 \leq 1$ a proto také

$$\left(\frac{n^2-1}{n^2}\right) \sum_{i=2}^{n} x_i^2 \leq \frac{n^2-1}{n^2}(1 - x_1^2) .$$

Levá straně nápadně připomíná omezení v zápisu elipsoidu E'. Všimneme si dále, že

$$\left(\frac{n+1}{n}\right)^2 \left(x_1 + \frac{1}{n+1}\right)^2 = \left(\frac{n+1}{n}\right)^2 x_1^2 + 2\frac{n+1}{n^2}x_1 + \frac{1}{n^2} .$$

Poslední dvě nerovnosti (resp. nerovnost a rovnost) sečteme. S užitím $x_1^2 + x_1 \leq 0$ pro $-1 \leq x_1 \leq 0$ dostaneme kýžené $(x + \frac{1}{n+1})^T Z^{-1} (x + \frac{1}{n+1})^T \leq 1$.

Zbývá ukázat, že nový elipsoid bude mít objem výrazně menší, než elipsoid původní.

Lemma 12

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

Důkaz. Připomeňme, že $vol(E') = \sqrt{detZ} vol(B)$. Proto

$$\frac{\mathrm{vol}(E')}{\mathrm{vol}(B)} = \sqrt{\det(Z)} = \sqrt{\frac{n^2}{(n+1)^2}} \cdot \sqrt{\left(\frac{n^2}{n^2-1}\right)^{n-1}} = \frac{n}{n+1} \cdot \left(\frac{n^2}{n^2-1}\right)^{\frac{n-1}{2}} =$$

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

Pro pořádek dodejme, že ve výpočtu jsme použili odhad $1 + x \leq e^x$. □

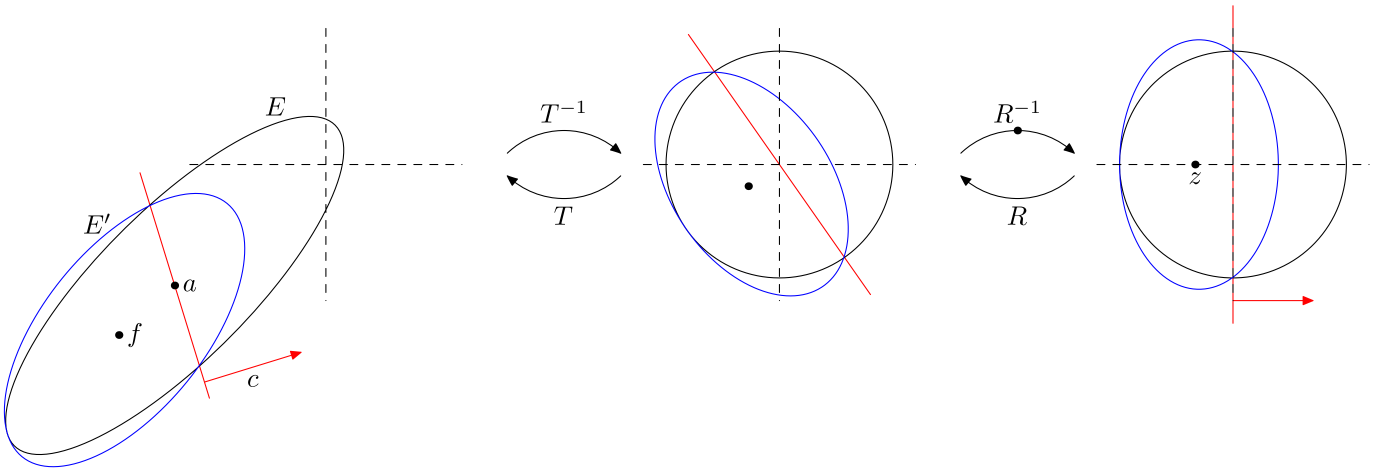
4.2 Obecný případ

Připomeňme si situaci. Je dán elipsoid E se středem v a určený pozitivně definitní maticí A. Dále je dán poloprostor H s normálovým vektorem c, jehož hranice prochází středem a elipsoidu E; poloprostor H odpovídá porušené nerovnosti. Víme, že všechna přípustná řešení se vyskytují v poloprostoru H. Označme $Q = A^{1/2}$. Formálně tedy:

$$E = E(a, A) = \{x \in \mathbb{R}^n | (x-a)^T A^{-1} (x-a) \leq 1\} = Q \cdot E(0, I) + a,$$

$$H = \{x \in \mathbb{R}^n | c^T x \leq c^T a\} = \{x \in \mathbb{R}^n | c^T (x-a) \leq 0\}$$

Hledáme elipsoid $E' = E(f, C) \supseteq E \cap H$ s co nejmenším objemem.



Obrázek 2: Obrázek demonstruje, jaká zobrazení použijeme.

Znovu využijeme skutečnosti, že každý elipsoid je afinním obrazem jednotkové koule. Pro daný elipsoid $E = E(a, A)$ označme T afinní zobrazení, které jednotkovou kouli se středem v počátku zobrazí na E; s pomocí T^{-1} zobrazíme naopak náš elipsoid E na jednotkovou kouli. Toto zobrazení T^{-1} aplikujeme také na poloprostor $H = \{x \mid c^T(x-1) \leq 0\}$. Všimněme si, že poloprostor $T^{-1}(H)$ typicky nebude totožný s poloprostorem $H_0 = \{x \in \mathbb{R}^n \,|x_1 \leq 0\}$, ale pro vhodnou rotaci R kolem počátku jistě $T^{-1}(H) = R(H_0)$. Abychom mohli použít výsledek z předešlé sekce, zobrazíme poloprostor $T^{-1}(H)$ pomocí R^{-1} na H_0 (viz obr. 2). Pak jistě

$$R^{-1}(T^{-1}(E)) \cap R^{-1}(T^{-1}(H)) \subseteq E(\frac{-1}{n+1}e_1, Z) \ ,$$

a tudíž elipsoid $T(R(E(\frac{-1}{n+1}e_1, Z)))$ obsahje $E \cap H$. Chceme proto spočítat zobrazení T a R.

V dalších výpočtech využijeme o zobrazení T následující vlastnosti:

- $T(y) = Q \cdot y + a$
- $T^{-1}(x) = Q^{-1} \cdot (x - a)$
- $T^{-1}(H) = \{T^{-1}(x) | c^T(x-a) \leq 0\} = \{y \in \mathbb{R}^n | c^T(T(y) - a) \leq 0\} = \{y | c^T Q y \leq 0\} = \{y | (Qc)^T y \leq 0\}$.

Po rotaci R vyžadujeme jedině, aby $R^{-1}\left(\frac{Qc}{||Qc||}\right) = e_1$. Všimněme si, že v $\mathbb{R}^2$ je rotace R určena jednoznačně, ale v prostorech vyšších dimenzí už nikoli (což nám ovšem nevadí, jak za chvíli uvidíme). Nyní použijeme složení zobrazení T a R k popsání E' (pro jednoduchost požíváme R pro označení zobrazení i označení matice totoho zobrazení). Připomeňme si ještě z lineární algebry, že pro matici R rotace platí $RR^T = I$.

Střed f elipsoidu E':

$$f = T(R(z)) = T\left(\frac{-1}{n+1} \cdot \frac{Qc}{||Qc||}\right) = a - \frac{1}{n+1} \frac{Ac}{\sqrt{c^T A c}} \ .$$

Matici C elipsoidu E' nám pomůže určit Lemma 13; v jeho důkazu se nám bude hodit následující pomocný výpočet.

$$x - f = x - a + \frac{Q}{n+1} \frac{Qc}{\sqrt{c^T A c}} = x - a + \frac{QRe_1}{(n+1)} = x - a - QRz = QR(R^{-1}Q^{-1}(x-a) - z).$$

Lemma 13

$$C = (QRZ^{1/2})(QRZ^{1/2})^T$$

Důkaz.

$$
\begin{aligned}
E(f,C) &= \{T(Ry)|(y-z)^T Z^{-1}(y-z) \leq 1\} = \\
&= \{x|(R^{-1}T^{-1}(x)-z)^T Z^{-1}(R^{-1}T^{-1}(x)-z) \leq 1\} = \\
&= \{x|(R^{-1}Q^{-1}(x-a)-z)^T Z^{-1}(R^{-1}Q^{-1}(x-a)-z) \leq 1\} = \\
&= \{x|R^{-1}Q^{-1}(x-f))^T Z^{-1}(R^{-1}Q^{-1}(x-f)) \leq 1\} = \\
&= \{x|(x-f)^T {Q^{-1}}^T {R^{-1}}^T Z^{-1} R^{-1} Q^{-1}(x-f) \leq 1\} \ .
\end{aligned}
$$

□

S využitím předešlého lemmatu a znalosti $Z = \mathrm{diag}\left(\frac{n^2}{(n+1)^2}, \frac{n^2}{n^2-1}, ...\right)$) vyjádříme matici C pomocí matice A a vektoru a.

$$
\begin{aligned}
C &= Q \cdot R \cdot Z \cdot R^T \cdot Q^T = \\
&= \frac{n^2}{n^2-1} \cdot Q \cdot R \cdot \mathrm{diag}\left(\frac{n-1}{n+1}, 1, ...1\right) \cdot R^T \cdot Q^T = \\
&= \frac{n^2}{n^2-1} \cdot (QRIR^TQ^T - \frac{2}{n+1} \cdot QRe_1e_1^T R^T Q^T) = \\
&= \frac{n^2}{n^2-1} \cdot (A - \frac{2}{n+1} \cdot \frac{Ac}{\sqrt{c^TAc}} \cdot \frac{c^TA^T}{\sqrt{c^TAc}}) = \\
&= \frac{n^2}{n^2-1} \cdot (A - \frac{2}{n+1} \frac{Acc^TA^T}{c^TAc}) \ .
\end{aligned}
$$

Zbývá ověřit, že C je symetrická a pozitivně definitní matice (za úkol).

Z výsledků předešlé sekce a z výše uvedeného výpočtu plynou následující lemmata:

Lemma 14

$$E(a,A) \cap \{x|c^T(x-a) \leq 0\} \subseteq E(f,C).$$

Lemma 15

$$\frac{vol(E(f,C))}{vol(E(a,A))} \leq e^{\frac{-1}{2(n+1)}}.$$

5 Kdy skončit?

Lemma 16 *Je-li $P = \{x \mid Cx \leq d\}$ polytop plné dimenze, pak vol$(P) \geq 2^{-(n+1)\langle C\rangle + n^3}$.*

Důkaz. Pro jednoduchost dokážeme slabší odhad; pro náš hlavní cíl - ukázat, že existuje polynomiální algoritmus pro hledání přípustného řešení - to nehraje žádnou roli.

Protože P je plné dimenze, má P $n+1$ afinně nezávislých vrcholů $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n$ a platí:

$$\mathrm{vol}(\mathrm{conv}(\mathbf{v}_0, \ldots, \mathbf{v}_n)) \leq \mathrm{vol}(P) \ ,$$

kde conv$(\cdots)$ označuje konvexní obal dané množiny vrcholů.

Opět využijeme toho, že každý vrchol P je řešením vhodné soustavy rovnic odvozené z $Cx \leq d$: pro každé $\mathbf{v}_i$ existuje podsystém $C_ix \leq d_i$ systému $Cx \leq d$ takový, že $\mathbf{v}_i$ je jediným řešením soustavy $C_ix = d_i$. Podle Cramerova pravidla $v_{i,j} = \frac{detC_{i,j}}{detC_i}$, kde $C_{i,j}$ je matice vzniklá z C_i nahrazením j-tého sloupce vektorem d_i. S užitím věty o objemu simplexu daného vektory $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n$ a věty o rozvoji determinantu dostáváme (při značení $\mathbf{u}_i = detC_i \cdot \mathbf{v}_i$):

$$\begin{aligned}
\mathrm{vol}(\mathrm{conv}(v_0, \dots v_n)) &= \frac{1}{n!}\left|\det\begin{pmatrix} 1 & 1 & \dots & 1 \\ v_0 & v_1 & \dots & v_n \end{pmatrix}\right| = \\
&= \frac{1}{n!} \cdot \frac{1}{|\det C_0 \cdot \det C_1 \cdot \dots \cdot \det C_n|} \cdot \left|\det\begin{pmatrix} \det C_0 & \det C_0 & \dots & \det C_0 \\ u_0 & u_1 & \dots & u_n \end{pmatrix}\right| \geq \\
&\geq \frac{1}{n!} \cdot (2^{\frac{1}{\langle C\rangle + n\log n}})^{(n+1)} \geq \\
&\geq 2^{-n\log n} \cdot 2^{-(n+1)\cdot\langle C\rangle - n(n+1)\log n} .
\end{aligned}$$

□

Lemma 17 *Je-li P plnodimenzionální polytop, pak pro $k = 2 \cdot (n+1) \cdot (2(n+1)\langle C\rangle + n \cdot \langle d\rangle - n^3)$ platí: $vol(E_k) < vol(P)$.*

Důkaz. Víme: $\mathrm{vol}(E_0) \leq (2R)^n$ pro $R = \sqrt{n} \cdot 2^{\langle C|d\rangle + n\log n}$. □

Dopočítání je domácí úkol.

6 Jak se zbavit zjednodušujících předpokladů

6.1 Omezenost

Už víme, že je-li $\mathbf{v}$ libovolný vrchol mnohostěnu $P = \{\mathbf{x} \mid Ax \leq b\}$, pak pro jeho i-tou souřadnici v_i platí $|v_i| \leq 2^{\langle A,b\rangle + n\log n}$. Pokud tedy P nějaké vrcholy má, jejich konvexní obal se jistě vejde do koule se středem v počátku a průměrem $R = \sqrt{n}\cdot 2^{\langle C,d\rangle + n\log n}$. Algoritmus bude po celou dobu svého běhu zachovávat invariant, že konvexní obal vrcholů P leží uvnitř aktuálního elipsoidu, což zaručuje správné chování algoritmu i pro tento případ.

Pokud P žádné vrcholy nemá, uvažme průnik P s 2^n možnými ortanty. Je-li P neprázdný, pak jistě existuje ortant, který má s P neprázdný průnik. Tento průnik je opět mnohostěn, řekněme P', a jistě už má vrchol. Přitom velikost zápisu tohoto nového mnohostěnu P' je jen nepatrně větší než velikost zápisu P a tedy všechny vrcholy P' leží v kouli kolem středu a průměru $2R$. V předešlých úvahách, kde nám šlo o obemktnutí mnohostěnu P posloupností elipsoidů, můžeme P nahradit konvexním obalem vrcholů odvozeného mnohostěnu P'. Všimněme si, že P' ani konvexní obal jeho vrcholů neznáme, ale podobně jako v předešlém případě máme zaručeno, že konvexní obal vrcholů P' vždy leží uvnitř aktuálního elipsoidu. Musíme pouze maličko změnit podmínku na ukončení iterací: splňuje-li střed elispoidu E_k všechny původní nerovnosti $Ax \leq b$, skončíme (čímž se může stát, že máme vektor, který neleží v konvexním obalu vrcholů P', ale to ničemu nevadí; s P' pracujeme hlavně kvůli argumentům o počtu iterací).

6.2 Plná dimenze

Lemma 18 *Nechť A je celočíselná matice a b celočíselný vektor. Pak systém $Ax \leq b$ má řešení právě když systém $Ax \leq b + \mathbb{1} \cdot \varepsilon$ má řešení pro $\varepsilon = \frac{1}{2n2^{\langle A,b\rangle - n^2}}$.*

Důkaz. Implikace zleva doprava je triviální. Pro opačnou použijeme Farkasovo lemma a ukážame, že y z Farkasova lemmatu pro původní úlohu funguje i pro odvozenou. Podrobnosti za domácí úkol. □

Lemma 19 *Předpokládejme, že úloha „rozhodni, zda mnohostěn P je prázdný či neprázný" je řešitelná v polynomiálním čase. Pak i úloha „nalezni $x \in P$, nebo poznej, že P je prázdné", je řešitelná v polynomiálním čase.*

Důkaz. Uvědomme si, že řešení úlohy s uvolněnou pravou stranou nemusí být řešením původní úlohy (což je ta, která nás opravdu zajímá). Předeslé lemma nás ale ujišťuje, že má-li řešení uvolněná soustava, má řešení (ne nutně stejné) i úloha původní. Jde o to, jak tuto znalost využít k tomu, abychom řešení skutečně nalezli.

Idea: snižovat počet nerovností v původní soustavě. Dva způsoby: ubírání nadbytečných nerovností a přeměnou ostatních na rovnice. Systém tvořený pouze rovnicemi vyřešíme např. Gaussovou eliminací.

Přesněji: Předpokládejme, že naše soustava $Ax \leq b$ obsahuje k nerovností (a jedno kolik rovností - dvě opačné nerovnosti počítáme jako jednu rovnost). Vezmeme libovolnou nerovnost, nahradíme ji rovností a otestujeme, zda nová soustava má řešení (pomocí předešlého lemmatu). Má-li nová soustava řešení, ubyla nám jedna nerovnost a soustava má i nadále nějaké řešení. Nemá-li nová soustava řešení, pak vybraná nerovnost neodpovídá žáďné stěně mnohostěnu a můžeme ji proto vynechat jako nadbytečnou. □

6.3 Hledání optimálního řešení

Lemma 20 *Je-li rozhodovací verze LP řešitelná v polynomiálním čase (tj. umíme-li zodpovědět, zda* $\exists x : Ax \leq b$*), pak je i optimalizační verze řešitelná v polynomiálním čase.*

Důkaz. Úlohu $\max\{cx : Ax \leq b\}$ vyřešíme pomocí úlohy $\exists x : Cx \leq d$.

Ze silné duality víme: $\max\{cx : Ax \leq b\} = \min\{yb : yA = c, y \geq 0\}$ (jsou-li obě množiny neprázdné).

Postupovat tedy budeme takto:

1. Otestuj zda $\{x \in \mathbb{R}^n : Ax \leq b\} = \emptyset$. Pokud ano, pak řešení neexistuje.
2. Uvaž $P' = \{(x, y) \in \mathbb{R}^{n+m} : Ax \leq b, y \geq 0, yA \leq c, -yA \leq -c, cx \leq yb, -cx \leq -yb\}$. Pokud $P' = \emptyset$, pak P je neomezený a maximum cílové funkce je libovolně velké. Pokud P' není prázdný, pak existuje $x_0, y_0 \in P'$, přičemž snadno vidíme, že x_0 je přípustné řešení primární úlohy, y_0 je přípustné řešení duální úlohy a silná dualita nás ujišťuje, že obě jsou optimální.

□

6.4 Nedohodnocená těžkost

Iracionalita (odmocniny) ve výpočtech …

7 Shrnutí

Odhlédneme-li od problémů s odmocninami, dokázali jsme následující větu.

Věta 21 (Chačijan, 1979) *Existuje polynomiální algoritmus pro řešení úlohy lineárního programování.*

Poděkování Martinu Perglovi za výchozí verzi poznámek podle běhu přednášky v roce … .

Literatura

[1] W. J. Cook, W. H. Cunningham, W. R. Pulleyblank, and A. Schrijver. *Combinatorial Optimization.* John Wiley, New York, 1997.

[2] M. Groetschel, L. Lovasz, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization.* Springer, Berlin, 1988.

[3] R. Seidel. Skript zur Vorlesung Optimierung. Technical report, Universität des Saarlandes, Saarbrücken, 1996.