CS 798 - Convexity and Optimization, Winter 2017, Waterloo

Lecture 6: John ellipsoids

John's theorem states that any symmetric convex body can be approximated by an ellipsoid with a factor of $O(\sqrt{n})$.

We will prove this theorem by writing a convex program and using the KKT optimality conditions.

We will also see some variants and some related problems such as the Dikin ellipsoid.

John's theorem

First we define the notion of approximation between two convex bodies (i.e. compact and non-empty interiors).

<u>Banach-Mazur distance</u> The distance $d(K,L)$ between convex bodies K and L is the least positive d for which there is an affine image $\tilde{L}$ of L such that $\tilde{L} \subset K \subset d(\tilde{L}-c)+c$ where c is some point in $\tilde{L}$.

For example, the cube $[-1,1]^n$ contains an Euclidean ball of radius 1, and is only contained in a ball of radius $\sqrt{n}$ as the corners are of distance $\sqrt{n}$ to the origin.

So, the distance between the cube and the ball is $\sqrt{n}$.

John's theorem shows that this is the worst case in some well-defined sense.

A convex body C is <u>symmetric</u> if $x \in C$ implies $-x \in C$.

<u>John's theorem</u> For any symmetric convex body $C \subseteq \mathbb{R}^n$, there is an ellipsoid $\mathcal{E}$ such that $\mathcal{E} \subseteq C \subseteq \sqrt{n}\,\mathcal{E}$.

For any (non-symmetric) convex body $C \subseteq \mathbb{R}^n$, there is an ellipsoid $\mathcal{E}$ such that $\mathcal{E} \subseteq C \subseteq n(\mathcal{E}-c)+c$, where c is the center of the ellipsoid $\mathcal{E}$.

We consider the case when C is a polytope. Intuitively, we do not lose much by considering this case as any convex body is the intersection of (possibly infinite) halfspaces. We will mention how to prove the general case.

We will prove the first part, and leave the second part as a homework problem.

The cube shows that the first part is tight.

It is more difficult to see that a simplex (e.g. $\mathrm{conv}\{0, e_1, \ldots, e_n\}$ where e_i is the i-th standard unit vector) is a tight example for the second part, see [BV exercise 8.13].

Maximum inscribed ellipsoid

Let the polytope be described as $P = \{ x \mid a_i^T x \le b_i \text{ for } 1 \le i \le m \}$ where $a_i \in \mathbb{R}^n$ and $b_i \in \mathbb{R}$.

The plan is quite natural: We first formulate the problem of finding a maximum inscribed ellipsoid (i.e. an ellipsoid $\mathcal{E} \subseteq P$ with maximum volume) as a convex optimization problem. Then we write down the KKT optimality conditions and deduce from them that $P \subseteq \sqrt{n}\,\mathcal{E}$ when P is symmetric.

Convex programming formulation

Since the polytope is symmetric, a maximum inscribed ellipsoid has the origin as its center.

Recall from L01 that an ellipsoid with center at origin can be represented as $\mathcal{E} := \{ x \mid x^T Q^{-1} x \le 1 \}$ where $Q \succ 0$.

This ellipsoid can also be written as $\{ Q^{\frac{1}{2}} u \mid \|u\|_2 \le 1 \}$ and its volume is $\det(Q^{\frac{1}{2}}) \cdot \mathrm{vol}(B_2^n)$.

Recall also from L02 that $\log\det(X)$ is a concave function in X.

So, to maximize the volume of the ellipsoid, we can use the objective function $\min -\log\det(Q^{\frac{1}{2}}) = -\frac{1}{2}\log\det(Q)$.

The constraints are $\sup\{ a_i^T x \le b_i \mid x \in \mathcal{E} \} = \sup\{ a_i^T (Q^{\frac{1}{2}} u) \le b_i \mid \|u\|_2 \le 1 \}$.

Note that $\sup\{ a_i^T Q^{\frac{1}{2}} u \mid \|u\|_2 \le 1 \} = \|Q^{\frac{1}{2}} a_i\|_2$, achieved at $u = Q^{\frac{1}{2}} a_i / \|Q^{\frac{1}{2}} a_i\|_2$.

To summarize, the maximum inscribed ellipsoid can be formulated as the following convex program:

$$\begin{aligned} \min \quad & -\tfrac{1}{2}\log\det Q \\ & \|Q^{\frac{1}{2}} a_i\|_2 \le b_i \quad \text{for } 1 \le i \le m \end{aligned}$$

By squaring the inequalities and ignoring the factor $\frac{1}{2}$ in the objective, it is equivalent to

$$\begin{aligned} \min \quad & -\log\det Q \\ & \frac{a_i^T Q a_i}{b_i^2} \le 1 \quad \text{for } 1 \le i \le m, \end{aligned}$$

where the domain of the objective function is S_{++}^n (i.e. define $-\log\det X = \infty$ when $X \not\succ 0$)

Optimality conditions

Since the program is convex with only linear constraints, Slater's condition is satisfied.

Hence, the KKT optimality conditions are necessary and sufficient of the optimal solutions.

The Lagrangian of the program is $L(Q,\lambda) = -\log\det Q + \sum_{i=1}^m \lambda_i \left(\frac{a_i^T Q a_i}{b_i^2} - 1 \right) = -\log\det Q + \sum_{i=1}^m \left\langle Q, \frac{\lambda_i a_i a_i^T}{b_i^2} \right\rangle - \sum_{i=1}^m \lambda_i$.

The KKT conditions include:

(primal feasibility)	$\frac{a_i^T Q a_i}{b_i^2} \le 1$	for $1 \le i \le m$
(dual feasibility)	$\lambda_i \ge 0$	for $1 \le i \le m$
(complementary slackness)	$\lambda_i \left(\frac{a_i^T Q a_i}{b_i^2} - 1 \right) = 0$	for $1 \le i \le m$
(Lagrangian optimality)	$0 = \nabla_Q L(Q,\lambda) = -(Q^{-1})^T + \sum_{i=1}^m \frac{\lambda_i a_i a_i^T}{b_i^2} \Rightarrow Q^{-1} = \sum_{i=1}^m \frac{\lambda_i a_i a_i^T}{b_i^2}$.	

To see that $\nabla_Q(\log\det Q) = (Q^{-1})^T$, note that $\frac{\partial}{\partial Q_{ij}} \log\det Q = \frac{1}{\det Q}\frac{\partial}{\partial Q_{ij}}\det Q = \frac{(-1)^{i+j} M_{ij}}{\det Q} = \frac{\mathrm{adj}(Q)_{ji}}{\det Q}$

where M_{ij} is the determinant of the $(n-1)\times(n-1)$ matrix by deleting the i-th row and j-th column of Q.

Using the fact that $Q\cdot \mathrm{adj}(Q) = \det(Q)\cdot I$, we have $\frac{\mathrm{adj}(Q)}{\det(Q)} = Q^{-1}$ and thus $\nabla_Q \log\det Q = (Q^{-1})^T$.

Proof of John's theorem (in the symmetric polytope case):

The proof follows quite quickly from the KKT conditions.

We would like to prove that $x\in P$ implies that $x\in \sqrt{n}\,\mathcal{E}$, or equivalently $x^TQ^{-1}x \le n$.

The assumption that the polytope is symmetric means that if the constraint $a_i^Tx\le b_i$ is valid,

then the constraint $-a_i^Tx\le b_i$ is also valid, and this implies that $\langle a_i, x\rangle^2 \le b_i^2$.

So, $x^TQ^{-1}x = x^T\left(\sum_{i=1}^m \frac{\lambda_i a_i a_i^T}{b_i^2}\right)x = \sum_{i=1}^m \lambda_i \langle a_i, x\rangle^2/b_i^2 \le \sum_{i=1}^m \lambda_i$.

It remains to bound $\sum_{i=1}^m \lambda_i$.

From the Lagrangian optimality condition $Q^{-1} = \frac{\sum \lambda_i a_i a_i^T}{b_i^2}$, by taking inner product with Q on both sides,

we get $n = \mathrm{Tr}(QQ^{-1}) = \langle Q, Q^{-1}\rangle = \langle Q, \frac{\sum \lambda_i a_i a_i^T}{b_i^2}\rangle = \sum_{i=1}^m \frac{\lambda_i a_i^T Q a_i}{b_i^2} = \sum_{i=1}^m \lambda_i$,

where the final equality follows from the complementary slackness condition.

This completes the proof. □

Remark: The non-symmetric case is a little harder to prove, mainly because the primal program and the dual program are harder to construct, because the center is also a variable.

But when the optimality conditions are successfully written down, the proof is similar to the above.

We leave it as a harder exercise to work out.

Discussions

Geometric interpretation: We can try to understand the optimality conditions geometrically.

By a linear transformation, we can assume that the maximum inscribed ellipsoid is the Euclidean ball, $Q=I$.

Then the optimality conditions become $\frac{a_i^Ta_i}{b_i^2}\le 1$ $\forall i$ (primal), $\lambda_i \ge 0$ $\forall i$ (dual),

$\lambda_i\left(\frac{a_i^Ta_i}{b_i^2} - 1\right) = 0$ $\forall i$ (complementary slackness), and $I = \sum_{i=1}^m \frac{\lambda_i a_i a_i^T}{b_i^2}$ (Lagrangian optimality).

The complementary slackness condition implies that if $\lambda_i > 0$, then $\frac{a_i^Ta_i}{b_i^2} - 1 = 0 \Leftrightarrow a_i^T\left(\frac{a_i}{b_i}\right) = b_i$.

Notice that those $\frac{a_i}{b_i}$ with $\lambda_i>0$ are on the boundary of both the polytope and the Euclidean ball (the maximum inscribed ellipsoid), as $\left\|\frac{a_i}{b_i}\right\|_2^2 = \frac{a_i^Ta_i}{b_i^2} = 1$ and $a_i^T\left(\frac{a_i}{b_i}\right) = b_i$.

ball (the maximum inscribed ellipsoid), as $\|\frac{a_i}{b_i}\|_2^2 = \frac{a_i^T a_i}{b_i^2} = 1$ and $a_i^T(\frac{a_i}{b_i}) = b_i$.

We call these <u>contact points</u> $u_1, \dots, u_{m^+}$ of the polytope and the ball.

The Lagrangian optimality condition says that $\sum_{i=1}^{m^+} \lambda_i u_i u_i^T = I$.

These contact points behave like an orthonormal basis in the sense that $\sum_{i=1}^{m^+} \lambda_i \langle u_i, x \rangle u_i = x$ for any $x \in \mathbb{R}^n$, by multiplying both sides of the Lagrangian optimality condition by x.

This guarantees that the contact points are spread out in all directions, e.g. the u_i do not all lie close to a proper subspace, as otherwise we could shrink the ball a little in this subspace and expand it in the orthogonal direction to obtain a larger ellipsoid.

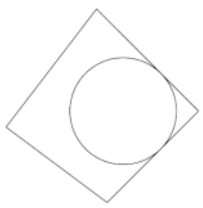


Figure 13. An ellipsoid where all contacts are on one side can grow.

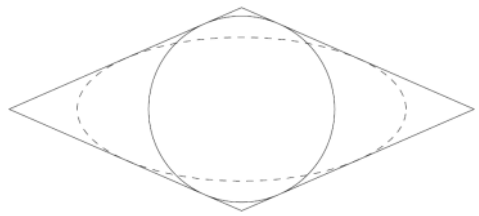


Figure 14. An ellipsoid (solid circle) whose contact points are all near one plane can grow.

pictures from Ball's survey

These are necessary and sufficient conditions for a ball to be the maximum inscribed ellipsoid of a polytope.

<u>Uniqueness</u> From the convex program, we can also derive that the maximum inscribed ellipsoid is unique, as the objective function is strictly convex on the set of positive definite matrices.

(See the proof that logdet is strictly concave on positive definite matrices from L02.)

<u>Norm approximation</u>: Given a norm, recall that the norm ball $B = \{x \mid \|x\| \le 1\}$ is convex.

By using John's theorem, since norm balls are symmetric, there is an ellipsoid $\mathcal{E} = \{x \mid x^T Q x \le 1\}$ such that $\mathcal{E} \subseteq B \subseteq \sqrt{n}\,\mathcal{E}$.

This implies that the quadratic norm $\|x\|_Q$ satisfies $\|x\|_Q \le \|x\| \le \sqrt{n}\,\|x\|_Q$, a basic result in functional analysis.

<u>Proof ideas for general convex body</u>:

There are a few approaches to prove John's theorem.

① The first approach is to generalize the convex programming approach to "semi-infinite" programming, in which there are a finite number of variables but possibly an infinite number of constraints.

Informally, under some technical conditions (e.g. the constraint set is compact), the KKT conditions are still necessary and sufficient for the optimal solutions

Then, following a similar line of reasoning, it can be proved that $\mathcal{E} \subseteq C \subseteq \sqrt{n}\,\mathcal{E}$.

This is the approach taken by Fritz John: see [Güler].

② Another approach is to write down the optimality conditions, and prove directly using separating hyperplane theorem that the optimal solution must satisfy them.

See [Ball]'s survey for a proof. The statement is as follows:

<u>John's theorem</u>: Each convex body K contains an ellipsoid of maximal volume.

This ellipsoid is B_2^n if and only if the following conditions are satisfied:

$B_2^n \subset K$ and (for some m) there are Euclidean unit vectors $(u_i)_1^m$ on the boundary of K and positive numbers $(c_i)_1^m$ satisfying $\sum_{i=1}^m c_i u_i = 0$ and $\sum_{i=1}^m c_i \langle x, u_i\rangle^2 = \|x\|_2^2$ for all $x \in \mathbb{R}^n$.

(Note that the condition $\sum_{i=1}^m c_i u_i = 0$ didn't come up in the symmetric case as it is redundant.)

③ There is also a more elementary approach to prove John's theorem, without using separating hyperplanes.

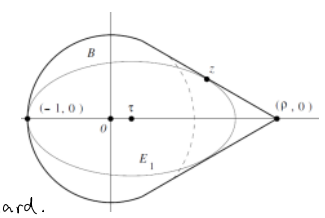
Suppose the Euclidean ball is a maximal inscribed ellipsoid, perhaps after an affine transformation.

Suppose, by contradiction that $C \not\subseteq nB$. This means that there is a point $p \in C$ with $\|p\|_2 = n$.

So, $\operatorname{conv}(B_2^n \cup \{p\}) \subseteq C$.

By an elementary calculation, there is an ellipsoid $\mathcal{E} \subseteq \operatorname{conv}(B_2^n \cup \{p\})$ with $\operatorname{vol}(\mathcal{E}) > \operatorname{vol}(B_2^n)$, contracting the maximality of B_2^n.

See [Barvinok] for a proof using this approach.



picture from [Barvinok].

<u>Hardness</u> In general, computing the John ellipsoid is computationally hard.

For example, given a set of points $\{x_1, \dots, x_n\}$, finding the maximum inscribed ellipsoid of $\operatorname{conv}\{x_1, \dots, x_n\}$ is hard (reference needed).

We will see later how to use the "ellipsoid method" to find an ellipsoid with "small distance" to a convex body.

<u>Minimum covering ellipsoid</u> [BV 8.4]

Intuitively, if $\mathcal{E}$ is a minimum volume ellipsoid that contains a convex body C, then you would expect the same result $\mathcal{E} \supseteq C \supseteq \frac{1}{\sqrt{n}}\mathcal{E}$ holds for a symmetric C and $\mathcal{E} \supseteq C \supseteq \frac{1}{n}\mathcal{E}$ for general C.

One approach is to follow use the above plan: first write a convex program, then write down the

optimality conditions, and then deduce the result.

This would work (see [BV 8.4]) and is a good exercise.

Another approach is to observe that the results about minimum covering ellipsoid follows from the results about maximum inscribed ellipsoid via duality; see homework 1.

Dikin ellipsoid [BV 8.5]

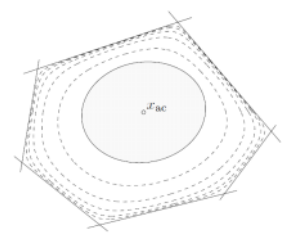
There is another way to define an ellipsoid that approximates a polytope.

The Dikin ellipsoids are useful in some optimization algorithms.

We are given a set of linear inequalities, $a_i^T x \le b_i$ for $1 \le i \le m$.

The <u>analytic center</u> of this set of linear inequalities is defined as $\min -\sum_{i=1}^m \log(b_i - a_i^T x)$.

Intuitively, a point is punished heavily if it is getting close to a hyperplane, and the analytic center denoted by x_{ac} is the point which is far away from any constraint.



The objective function is called the <u>logarithmic barrier function</u>, and it plays an important role in interior point algorithms.

As it is an unconstrained strictly convex optimization problem, we know that x_{ac} is the unique point when the gradient is zero, i.e. $\sum_{i=1}^m \frac{a_i}{b_i - a_i^T x_{ac}} = 0$

Interestingly, the Hessian of the logarithmic barrier function defines an inscribed and a covering ellipsoid.

The Hessian is $H = \sum_{i=1}^m \frac{a_i a_i^T}{(b_i - a_i^T x_{ac})^2}$.

Let $\mathcal{E}_{inner} = \{ x \mid (x - x_{ac})^T H (x - x_{ac}) \le 1 \}$ and $\mathcal{E}_{outer} = \{ x \mid (x - x_{ac})^T H (x - x_{ac}) \le m(m-1) \}$

<u>Theorem</u> $\mathcal{E}_{inner} \subseteq P \subseteq \mathcal{E}_{outer}$. A corollary is $\mathcal{E}_{inner} \subseteq P \subseteq m\,\mathcal{E}_{inner}$.

This is worse than John's ellipsoid, since $m \ge n$ in a polytope.

First, we prove that $\mathcal{E}_{inner} \subseteq P$. That is, $x \in \mathcal{E}_{inner}$ implies $a_i^T x \le b_i$ for $1 \le i \le m$.

Note that $x \in \mathcal{E}_{inner} \Rightarrow \sum_{i=1}^m \frac{\langle a_i, x - x_{ac} \rangle^2}{(b_i - a_i^T x_{ac})^2} \le 1 \Rightarrow a_i^T (x - x_{ac}) \le b_i - a_i^T x_{ac} \quad \forall i \Rightarrow a_i^T x \le b_i \quad \forall i$.

Next, we prove that $P \subseteq \mathcal{E}_{outer}$. That is, $a_i^T x \le b_i$ for $1 \le i \le m$ implies $x \in \mathcal{E}_{outer}$.

We compute
$$(x - x_{ac})^T H (x - x_{ac}) = \sum_{i=1}^m \frac{\langle a_i, x - x_{ac} \rangle^2}{(b_i - a_i^T x_{ac})^2}$$
$$= \sum_{i=1}^m \frac{\left[(b_i - a_i^T x_{ac}) - \langle a_i, x - x_{ac} \rangle \right]^2}{(b_i - a_i^T x_{ac})^2} - m \qquad \text{using } \sum_{i=1}^m \frac{a_i}{b_i - a_i^T x_{ac}} = 0$$
(the gradient condition)

$$= \sum_{i=1}^{m} \frac{(b_i - a_i^T x)^2}{(b_i - a_i^T x_{ac})^2} - m$$

$$\leq \left(\sum_{i=1}^{m} \frac{b_i - a_i^T x}{b_i - a_i^T x_{ac}} \right)^2 - m$$

using $\left(\sum y_i^2\right) \leq \left(\sum y_i\right)^2$ when $y \geq 0$, which is the case here as $x \in P$.

$$= \left(\sum_{i=1}^{m} \frac{b_i - a_i^T x_{ac}}{b_i - a_i^T x_{ac}} + \frac{a_i^T x_{ac} - a_i^T x}{b_i - a_i^T x_{ac}} \right)^2 - m$$

$$= m^2 - m$$

using again $\sum_{i=1}^{m} \frac{a_i}{b_i - a_i^T x_{ac}} = 0$.

There is a simple proof that if P is symmetric, then $\mathcal{E}_{inner} \subseteq P \subseteq \sqrt{m}\, \mathcal{E}_{inner}$; see homework 1.

Question: Given a symmetric convex body $C \subseteq \mathbb{R}^n$, is there an efficient algorithm to find an ellipsoid $\mathcal{E}$ such that $\mathcal{E} \subseteq C \subseteq \sqrt{n}\, \mathcal{E}$?

References:

[Güler] Foundations of optimization (chapter 12), by Güler.

[Ball] An elementary introduction to modern convex geometry (chapter 3), by Ball.

[Barvinok] A course in geometry (chapter V), by Barvinok.