CPSC 536C: Algorithms for Convex Optimization
University of British Columbia

# Cutting Plane Methods

Akshay Ram
January 5, 2025

*These notes are subject to change and may contain errors.*

## 1 GLS Oracle Model

### 1.1 Definitions

**Definition 1** (Oracle Model)**.** *The following are algorithmic problems for closed convex set $K \subseteq \mathbb{R}^n$:*

*MEM bership($x \in \mathbb{R}^n, K \subseteq \mathbb{R}^n$):*
*Output: YES if $x \in K$; NO otherwise.*

*SEP aration($x \in \mathbb{R}^n, K \subseteq \mathbb{R}^n$):*
*Output: YES if $x \in K$;*
*otherwise output separating hyperplane $w$ such that $\langle w, x\rangle > \sup_{y \in K} \langle w, y\rangle$;*

*OPT imization($w \in \mathbb{R}^n, K \subseteq \mathbb{R}^n$)*
*Output: $h_K(w) = \sup_{x \in K} \langle w, x\rangle$*
*and optimizer $x_* \in K$ such that $h_K(w) = \langle w, x_*\rangle$;*

*VAL idity($w \in \mathbb{R}^n, b \in \mathbb{R}, K \subseteq \mathbb{R}^n$):*
*Output: YES if $\langle w, x\rangle \le b$ for all $x \in K$; NO otherwise.*

*VIOL ation($w \in \mathbb{R}^n, b \in \mathbb{R}, K \subseteq \mathbb{R}^n$):*
*Output: YES if $\langle w, x\rangle \le b$ for all $x \in K$;*
*otherwise output $x \in K$ such that $\langle w, x\rangle > b$.*

We can also consider *approximate* versions of all these oracles. For the formal definitions, see [GLS 2.1]. Many of the algorithms we study in this class can be thought of as reductions between these algorithmic problems.

### 1.2 Relations between Oracles

The various oracles for $K$ and its polar dual $K^\circ$ are related.

**Proposition 2.** *In the following, we assume $B(0,\varepsilon) \in int(K)$ and $B(0,\varepsilon) \in int(K^\circ)$.*

- *OPTimization oracle for $K$ can be (approximately) implemented using VIOLation or VALidity oracle for $K$;*
- *MEMbership oracle for $K$ is equivalent to VALidity oracle for $K^\circ$; and vice-versa MEM($K^\circ$) is equivalent to VAL($K$);*

- *SEParation oracle for $K^\circ$ can be implemented using a VIOLation oracle for $K$; VIOL($K$) can be implemented using SEP($K^\circ$) and one of MEM($K$) or VAL($K^\circ$).*

**Proof:**

- In the following we use VAL if we only need the optimum value, and VIOL if the optimizer is also required. Using the VAL/VIOL oracles we can check if $\exists x \in K : \langle w, x\rangle \geq b$. Therefore, to compute $h_K(w) = \sup_{x\in K}\langle w, x\rangle$ approximately, we perform binary search over $b$.

- We first implement MEM($K^\circ$) using VAL($K$). Given input $w$ we want to check if $w \in K^\circ$ iff $\sup_{x\in K}\langle w, x\rangle \leq 1$. For this we return the output of VAL($w, 1, K$).

  Conversely, we want to implement VAL($K$) using MEM($K^\circ$). So given an input $(w, b)$ we want to check if $\forall x \in K : \langle w, x\rangle \leq b$. First we use that $B(0, \varepsilon) \subseteq K$ so if $b \leq 0$ we output NO. Otherwise note that $v \in K^\circ$ iff $\sup_{x\in K}\langle v, x\rangle \leq 1$. So we can return the output of MEM($w/b, K^\circ$).

  The dual statement, swapping $K$ and $K^\circ$, follows due to bi-duality $(K^\circ)^\circ = K$.

- We first implement SEP($K^\circ$) using VIOL($K$). Given input $w$ we want to check if $w \in K^\circ$, and if not to output a separating hyperplane. Note $w \in K^\circ$ iff $\sup_{x\in K}\langle w, x\rangle \leq 1$, so we query VIOL($w, 1, K$); if the output is YES, we return YES; if the output is NO then the oracle returns $x \in K$ such that $\langle w, x\rangle > 1 \geq \sup_{v\in K^\circ}\langle v, x\rangle$, where the last step is by definition of $K^\circ$, so we can output $x$ as our separating hyperplane for $K^\circ$.

  Conversely, we want to implement VIOL($K$) using SEP($K^\circ$). So given an input $(w, b)$ we want to check if $\sup_{x\in K}\langle w, x\rangle \leq b$, and if not to output $x \in K$ such that $\langle w, x\rangle > b$. First we use that $B(0, \varepsilon) \subseteq K$ so if $b \leq 0$ we output $0 \in K$ as $\langle w, 0\rangle = 0 > b$. Otherwise we query SEP($w/b, K^\circ$); if the output is YES then $\sup_{x\in K}\langle w/b, x\rangle \leq 1$ so we return YES; if the output is NO then the oracle returns separating hyperplane $x \in \mathbb{R}^n$ such that $\langle w/b, x\rangle > \sup_{v\in K^\circ}\langle v, x\rangle$. If we knew this right hand side $h_{K^\circ}(x) = \sup_{v\in K^\circ}\langle v, x\rangle$ then we could output $y := x/h_{K^\circ}(x) \in K^{\circ\circ} = K$ with $\langle w, y\rangle > b$ as our violating point. But we can approximately compute this value using binary search with the VALidity oracle for $K^\circ$ as shown in the first part. Equivalently, since $0 \in \mathrm{int}(K)$, there is a point $y \in [0, x] \cap \partial K$ at the intersection of the line $[0, x]$ with the boundary of $K$, and this also gives a violating point $\langle w, y\rangle > b$ ($y \in \partial K$ implies $\sup_{v\in K^\circ}\langle v, y\rangle = 1$). And this boundary point we can approximately compute using binary search with the MEMbership oracle for $K$.

$\square$

### 1.3 Function Oracles: TODO

What is the relation to function oracles? In particular, recall that we prove duality of convex functions by reducing to duality of the epigraph, which is a convex set.

**Definition 3** (Fenchel dual)**.** *For convex $f : \mathbb{R}^n \to \mathbb{R}$, the Fenchel dual is*

$$f^*(w) := \sup_y \langle w, y\rangle - f(y).$$

**Lemma 4.** *For differentiable closed convex $f$, the supporting hyperplane for the epigraph of $f$ at $(x, f(x))$ is given by slope $(\nabla f(x), -1)$ and value $f^*(\nabla f(x)) = \sup_y\langle \nabla f(x), y\rangle - f(y)$.*

*Similarly, the supporting hyperplane for the sub-level set $L_{f(x)} := \{y \in \mathbb{R}^n \mid f(y) \leq f(x)\}$ is given by slope $\nabla f(x)$ and value $\langle \nabla f(x), x\rangle$.*

*Both these statements can be generalized to non-differentiable $f$ using subgradients.*

**Proposition 5.** *In the following, we assume $f : \mathbb{R}^n \to \mathbb{R}$ is a closed convex function.*

- *EVALuation oracle for $f$ can be implemented using MEMbership oracle for epi$(f)$;*
- *GRADient oracle for $f$ can be implemented using SEParation oracle for epi$(f)$;*
- *OPTimization oracle for epi$(f)$ is equivalent to EVALuation for the Fenchel dual $f^*(w) := \sup_y \langle w, y\rangle - f(y)$.*

## 2 Cutting Plane Methods

Our eventual goal is to find an algorithm to solve convex programs $\min_{x \in K} f(x)$. Cutting plane methods solve this using just SEParation oracle for $K$ and EVAL and GRAD oracles for $f$. We first show how to solve the much simpler FEASibility problem: given SEParation oracle for $K$, either find $x \in K$ or output that $K$ is 'small'. Note that linear optimization over $K$ can be reduced to this: test FEASibility for

$$K' := K \cap \{x \mid \langle w, x\rangle \geq b\}.$$

and run binary search on $b$. Note that SEP for $K'$ can be easily implemented using SEP for $K$ and testing the linear inequality $\langle w, x\rangle \geq b$.

The intuition for cutting plane methods comes from binary search: say we are attempting to find some point $x \in [0,1]^n$, and we have oracle access to coordinate queries $y_i \geq x_i$ or $y_i \leq x_i$. Then in each iteration, we should query the center of the remaining grid and eliminate the elements with chosen coordinate too large or small, depending on the output of the oracle. This procedure is optimal in the worst case, as it eliminates the maximum possible options in each iteration. This is the correct intuition for the Center of Gravity method, described below, which generalizes the procedure to arbitrary convex $K \subseteq \mathbb{R}^n$. In general, it is not clear how to query the 'center' of a convex body, so the next algorithm will maintain an Ellipsoid in each iteration to contain the feasible set, and update according to the separation oracle.

## 3 Center-of-Gravity Method

We first describe the algorithm to solve feasibility. In each iteration, we maintain a feasible convex set $K_t \supseteq K$; we query the separation oracle with the Center of Mass $c_t := \mathcal{E}_{x \sim K_t} x = \int_{x \in K_t} x dx$; if $c_t \in K$ then we are done; otherwise we get $\langle w, c_t\rangle > \sup_{x \in K}\langle w, x\rangle$; therefore, we know $K$ is contained in the following halfspace

$$H_t := \{x \mid \langle w, x\rangle \leq \langle w, c_t\rangle,$$

so we update accordingly $K_{t+1} := K_t \cap H_t$. We claim that this solves feasibility:

**Theorem 6.** *Given $K \subseteq B(0, R) \subseteq \mathbb{R}^n$ via separation oracle, the center-of-gravity method requires $O(n \log(R/\varepsilon))$ iterations to either*

1. *find $x \in K$;*
2. *certify $K$ does not contain a ball of radius $\varepsilon$, or certify vol$(K) \leq \varepsilon^n$.*

The key step in the analysis is the following beautiful result from convex geometry:

**Theorem 7** (Grunbaum's Theorem). *For convex $K \subseteq \mathbb{R}^n$, let $c := \mathcal{E}_{x\in K} x$ be the center-of-gravity of $K$. Then for any hyperplane $H \ni c$, the two halfspaces $H_+, H_-$ satisfy*

$$\max\{vol(K \cap H_+), vol(K \cap H_-)\} \leq vol(K)(1 - 1/e).$$

We do not prove this in this class but refer to the excellent survey of Keith Ball: An Elementary Introduction to Modern Convex Geometry. With this result, the analysis is straightforward.

**Proof:** [Proof of theorem 6] If in any iteration we find $c_t \in K$ then we are done. Otherwise, in each iteration we reduce the volume by the factor stated above. Therefore in $T = O(n \log(R/\varepsilon))$ iterations we have

$$\mathrm{vol}(K_T) \leq \mathrm{vol}(K_0)(1 - 1/e)^T \leq \mathrm{vol}(B(0, R)) \exp(-n \log(R/\varepsilon)) \leq \mathrm{vol}(B(0, \varepsilon)),$$

where we used that $K \subseteq B(0, R)$. □

In the following section, we show that this is in fact the optimal query complexity possible for an algorithm using just a SEParation oracle. Of course, as stated it is not at all clear how to compute the center-of-gravity of $K_t$, and it turns out this is at least as hard as optimizing over $K_t$. Therefore in the following sections we will study the Ellipsoid algorithm, which requires more oracle queries but can be efficiently updated.

We next describe a very similar algorithm to solve general convex programs. In each iteration, we still maintain a feasible convex set $K_t \supseteq K$ and query the center $c_t$; if $c_t \notin K$ then we update $K_{t+1} = K_t \cap H_t$ just as in the previous algorithm; if $c_t \in K$ then we query the EVALuation and (sub)-GRADient oracle for $f$, to compute $(f(c_t), g)$; Finally we update $K_{t+1} = K_t \cap H_g$ where

$$H_g := \{x \mid \langle g, x - c_t\rangle \leq\}$$

i.e. the halfspace in the negative (sub-)gradient direction.

**Theorem 8.** *Given $K \subseteq B(0, R) \subseteq \mathbb{R}^n$ via SEParation oracle, and convex $f : \mathbb{R}^n \to \mathbb{R}$ via EVALuation and GRADient oracle, such that $\max_{x\in K} f(x) - \min_{x\in K} f(x) \leq F$; The center-of-gravity method requires $O(n \log(RF/\varepsilon))$ iterations to either*

1. *find $x \in K$ such that $f(x) \leq \min_{y\in K} f(x_*) + \varepsilon$;*
2. *certify $vol(K) \leq \varepsilon^n$.*

The proof rests on the following claim, showing the negative gradient gives a good update.

**Claim 9.** *For closed convex $f : \mathbb{R}^n \to \mathbb{R}$ and $x \in dom(f)$, any subgradient $g \in \partial f(x)$ gives a supporting hyperplane for the sub-level set*

$$L_{f(x)} := \{y \mid f(y) \leq f(x)\}.$$

We leave the proof as an exercise in the first problem set. But intuitively the negative subgradient halfspace always contains the optimizer $x_* := \arg\min_{x\in K} f(x)$, so our update maintains a body containing $x_*$. With this in hand, the analysis follows:

**Proof:** [Proof of theorem 8] We still manage to decrease the volume by a constant factor in each iteration, due to Grunbaums theorem. And the claim above shows that $K_t \ni x_*$ for all $t$. If in every iteration $c_t \notin K$, then by the previous feasibility analysis we can certify small volume in $T = O(n \log(R/\varepsilon))$ iterations. Otherwise, we show that when the volume gets small enough, one of the queried center points must have small function value.

For this we analyze the follows approximate optimal set:

$$X_\delta := (1-\delta)x_* + \delta K = \{(1-\delta)x_* + \delta x \mid x \in K\}.$$

Note that we can bound the function on this set as, for $x \in K$,

$$f((1-\delta)x_* + \delta x) \le (1-\delta)f(x_*) + \delta f(x) = f(x_*) + \delta(f(x) - f(x_*)) \le f(x_*) + \delta F,$$

where the first step was by convexity of $f$, and in the last step we used our bound $\max_{x\in K} f(x) - f(x_*) \le F$. Note that $\mathrm{vol}(X_\delta) = \mathrm{vol}(\delta K) = \delta^n \mathrm{vol}(K)$. Therefore if we reach $T$ such that $\mathrm{vol}(K_T) < \mathrm{vol}(X_\delta)$ then we must have $X_\delta / K_T \neq \emptyset$. Therefore in some iteration we must have queried $c_t$ and cut off some part of $X_\delta$. Let $c_t = (1-\lambda)x_* + \lambda x_\delta$ where $x_\delta \in X_\delta / K_t$ was cut off. Then

$$f(c_t) \le (1-\lambda)f(x_*) + \lambda f(x_\delta) \le f(x_\delta) \le f(x_*) + \delta F,$$

again by convexity and the derived bound on $f(x_\delta \in X_\delta)$. Choosing $\delta \lesssim \varepsilon/F$ gives the result. □

# 4 Lower Bound

**Theorem 10.** *Given $K \subseteq B(0,R) \subseteq \mathbb{R}^n$ via SEParation oracle, any algorithm solving the FEASibility problem requires $\Omega(n \log(R/\varepsilon))$ oracle calls to the SEP oracle.*

**Proof:** [Proof Sketch] Consider the grid example $K = x + [-\varepsilon, \varepsilon]^n \subseteq [0,1]^n$, and note that for each query, the adversay can always choose a separating hyperplane (even a coordinate hyperplane) to keep $\Omega(1)$ fraction of the mass. □

# 5 Ellipsoid Method [Khachiyan 1979]

Note that while the Center-of-Gravity method provably achieves optimal oracle complexity, as shown by the lower bound above, it is not clear how to implement the procedure in general: computing the centerpoint of a general convex body is at least as hard as optimizing over that body! And maintaining the sequence of intersections of halfspaces could become costly. Therefore, in this section we consider the Ellipsoid method:

**Theorem 11.** *Given $K \subseteq B(0,R) \subseteq \mathbb{R}^n$ via separation oracle, the Ellipsoid method requires $O(n^2 \log(R/\varepsilon))$ iterations to either*

1. *find $x \in K$;*
2. *certify $K$ does not contain a ball of radius $\varepsilon$.*

The strategy involves approximating our feasible set by an Ellipsoid. This can be maintained and updated efficiently. The key geometric lemma that allows us to make progress is as follows:

**Lemma 12** (Lemma 2.3 in [Bubeck)**.** *] Let $\mathcal{E} := \{x \in \mathbb{R}^n \mid \langle (x-c), Q(x-c)\rangle \le 1\}$ be an Ellipsoid with $Q \succ 0$; and let $H := \{x \in \mathbb{R}^n \mid \langle w, x\rangle \le \langle w, c\rangle\}$ be a halfspace through the center of $\mathcal{E}$. Then there exists ellipsoid $\overline{\mathcal{E}}$ such that*

$$\overline{\mathcal{E}} \supset \mathcal{E} \cap H \quad \textit{and} \quad \textit{vol}(\overline{\mathcal{E}}) \le \textit{vol}(\mathcal{E}) \exp(-1/2n).$$

*Further, this update can be efficiently computed in terms of $c, Q, w$.*

In section 8 we state the explicit update step, showing it can be computed efficiently, and prove the the geometric result using a convex program. Given this result, the complexity follows from the same proof as the Center-of-Gravity algorithm, except with $n$ factor worse oracle complexity.

## 6 Convex Programming Duality

In this section, we consider the following framework for convex programs:

$$\inf_x f(x) \qquad \text{s.t.} \qquad \forall i \in [m] : f_i(x) \leq 0, \tag{1}$$

where $f, f_i$ are all convex functions. It is often difficult to solve problems with constraints, so we would like to relax the problem by incorporating constraint functions into the objective.

**Definition 13** (Lagrangian)**.** *For problem as in eq.* (1)*, let Lagrangian be*

$$\mathcal{L}(x, \lambda) := f(x) + \sum_{i \in [m]} \lambda_i f_i(x).$$

*The dual function is* $g(\lambda) := \inf_x \mathcal{L}(x, \lambda)$ *and the dual program is*

$$\sup_{\lambda \geq 0} g(\lambda) = \sup_{\lambda \geq 0} \left( \inf_x f(x) + \sum_{i \in [m]} \lambda_i f_i(x) \right). \tag{2}$$

Note that the dual problem is always a convex program even for non-convex $f, f_i$: $g$ is concave as it is an inf of affine functions. The Lagrangian and dual give *lower bounds* on problem:

**Fact 14** (Weak Duality)**.** *For any feasible* $x$ *and dual* $\lambda \geq 0$

$$f(x) \geq L(x, \lambda) = f(x) + \sum_{i \in [m]} \lambda_i f_i(x) \geq \inf_x L(x, \lambda) = g(\lambda).$$

In general, there could be a *duality gap*, i.e. the value of the primal and dual programs could be different, so the lower bounds given by the dual program are not effective to understand the primal program. On the other hand, in certain cases there is no gap: for linear programs, strong duality always holds; for semi-definite programs, there are simple counterexamples with duality gap. In general applications, we will use the following sufficient condition:

**Theorem 15** (Slater's Theorem)**.** *Consider the primal and dual programs eq.* (1)*, 2. If there is a strictly feasible solution* $x$ *such that* $\forall i : f_i(x) < 0$*, then the primal and dual programs have equivalent values, and the supremum in the dual is attained.*

We will not prove this result here, but the result follows from the separating hyperplane theorem (as do basically all duality theorems). In fact we can even consider the more general convex program

$$\min_x f(x) \qquad \text{s.t.} \quad \forall i : f_i(x) \leq 0, \quad Ax = b,$$

where we include linear equality constraints. In this setting, Slater's Theorem requires $f_i(x) < 0$ for all $i$ and $Ax = b$, and still implies strong duality.

We next make some observations that can be deduced from optimality.

**Proposition 16.** *Let* $(x^*, \lambda^*)$ *be primal/dual feasible solutions with* $f(x^*) = g(\lambda^*)$*. Then*

1. $x^*$ *is feasible, i.e.* $\forall i : f_i(x) \leq 0$*;*

2. $\lambda^*$ *is feasible, i.e.* $\lambda^* \geq 0$*;*

3. *(Complementary Slackness):* $\forall i : \lambda_i^* f_i(x^*) = 0$*, i.e.* $\lambda^*$ *is supported only on tight constraints;*

*4. (Lagrangian optimality): $x^* = \arg\inf_x L(x, \lambda^*)$.*

**Proof:** The first two properties are assumed. We deduce the remaining from the following sequence of inequalities:

$$g(\lambda^*) = f(x^*) \geq f(x^*) + \sum_i \lambda_i^* f_i(x^*) \geq g(\lambda^*),$$

where the first equality is by assumption, in the second we used primal/ dual feasibility so $\lambda_i^* f_i(x^*) \leq 0$, and the final inequality was by definition of dual $g$. Therefore all inequalities must be tight: the first inequality being tight implies complementary slackness, and the last inequality being tight implies Lagrangian optimality. □

This proposition allows us to reason about the optimizer, and applies even to non-convex programs. Of course in general there does not have to exist optimal solutions with matching primal and dual value, so we still need to check strong duality. But if somehow we have access to the optimizers of a general program, then the proposition allows us to deduce the above properties about the solution. We also note that (1), (2), (3) can be easily checked by evaluating the given functions, whereas (4) is more difficult in general. In the case of a convex (differentiable) program, we can use any of our optimality conditions for convex functions to verify Lagrangian optimality, which may be easier.

For convex programs, we also have the following converse.

**Theorem 17** (KKT Conditions)**.** *Let eq.* (1)*,* 2 *be convex primal/dual programs, and assume $(x^*, \lambda^*)$ satisfy (1), (2) primal/ dual feasibility; (3) complementary slackness; and (4) Lagrangian optimality, according to theorem 16. Then in fact $(x^*, \lambda^*)$ are optimal solutions with $f(x^*) = g(\lambda^*)$.*

**Proof:** We follow the same sequence of inequalities, showing they are all tight:

$$f(x^*) = f(x^*) + \sum_i \lambda_i^* f_i(x^*) = g(\lambda^*),$$

the first step is complementary slackness $\forall i : \lambda_i^* f_i(x^*) = 0$, and the second is Lagrangian optimality. □

In this case we do not have to verify strong duality, as any primal and dual solutions satisfying the above conditions automatically certify strong duality. We also note that for differentiable convex programs, Lagrangian optimality is characterized by first-order condition

$$\nabla_x \mathcal{L}(x^*, \lambda^*) = \nabla f(x^*) + \sum_i \lambda_i^* \nabla f_i(x^*) = 0,$$

which could be easy to directly verify if we can compute gradients.

We will use the first proposition to reason about the optimizer to show John's theorem; and we will use KKT conditions to certify optimality for the ellipsoid lemma.

# 7 John's Ellipsoid Theorem

The goal of this section is to prove the following:

**Theorem 18.** *Let $K \subseteq \mathbb{R}^n$ be a compact convex and full-dimensional set. Then there exists an ellipsoid $\mathcal{E}$ with center $c$ such that*

$$c + \frac{1}{n}(\mathcal{E} - c) \subseteq K \subseteq \mathcal{E}.$$

*Further, if $K$ is origin-symmetric, i.e. $K = -K$, then this can be improved to*

$$\frac{1}{\sqrt{n}}\mathcal{E} \subseteq K \subseteq \mathcal{E}.$$

Intuitively, we want to find the smallest ellipsoid containing $K$ so that it is more likely for the scaled down version to fit inside $K$. For this we will use the volume as an objective function, which we will show is convex in the appropriate variables. We will also show that the containment condition can be written as convex constraints.

### 7.1 Convex Program Formulation

In the following, we let ellipsoid $\mathcal{E}$ be defined as

$$\mathcal{E} := c + AB_2^n$$

where $A \in \mathbb{R}^{n\times n}$ is invertible and $B_2^n := \{x \mid \|x\|_2 \leq 1\}$ is the standard Euclidean ball. We first rewrite containment in terms of our above representation. We leave the proof as an exercise.

**Proposition 19.** *Let $K := \mathrm{conv}\{x_i\}$; then $K \subseteq \mathcal{E}$ iff*

$$\forall i: \quad \langle (x_i - c), (AA^T)^{-1}(x_i - c)\rangle \leq 1.$$

*Dually, consider inequality representation $K := \{x \in \mathbb{R}^n \mid Bx \leq d\}$; then $\mathcal{E} \subseteq K$ iff*

$$\forall i: \quad \|A^T b_i\|_2 \leq d_i - \langle b_i, c\rangle.$$

We will eventually perform a change of variable so that these become convex constraints. Note that we have swapped containment between convex hull and inequality representation of $K$. This is for a very good reason: given $K := \mathrm{conv}\{x_i\}$, finding the maximum inscribed ellipsoid $\mathcal{E} \subseteq K$ is actually NP-hard! And similarly given $K := \{x \in \mathbb{R}^n \mid Bx \leq d\}$, finding minimum containing ellipsoid $K \subseteq \mathcal{E}$ is NP-hard.

Next we rewrite the objective function:

**Fact 20.** *For $\mathcal{E} = c + AB_2^n$ as above,*

$$vol(E) \propto |\det(A)| = \sqrt{\det(AA^T)}.$$

**Proof:** [Sketch] $\mathcal{E}$ is an affine transformation of $B_2^n$, so the constant in the proportion is $\mathrm{vol}(B_2^n)$. The first equality can be proven by integrating and noting the Jacobian is exactly $\det(A)$, and the second is by standard linear algebra. □

Putting these together, we can construct a convex program for minimum containing ellipsoid using a change of variable:

**Proposition 21.** *Let $K := \mathrm{conv}\{x_i\}$; then the minimum containing ellipsoid is given by the optimizer of the following convex program:*

$$\min_{Q \succ 0} -\log\det(Q) \qquad s.t. \quad \forall i: \quad \langle x_i, Qx_i\rangle - 2\langle q, x_i\rangle + \langle q, Q^{-1}q\rangle \leq 1.$$

**Proof:** We first consider quadratic polynomial $f(x) := \langle x, Qx\rangle - 2\langle q, x\rangle + q_0$, where our variables are $(Q, q, q_0)$. We want this to represent our ellipsoid $\mathcal{E} = \{x \mid f(x) \le 1\}$ using change of variable $Q := (AA^T)^{-1}$. But if $q_0$ is unconstrained then we can always take it small enough to make any $Q \succeq 0$ feasible. Therefore we constrain it so that the quadratic is 0 at its center. Formally, we constrain $\min_x f(x) = 0$, which is equivalent to $q_0 = \langle q, Q^{-1}q\rangle$ as can be verified directly, noting $Q^{-1}q = \arg\min_x f(x)$. Finally, we claim that $(q, Q) \to \langle q, Q^{-1}q\rangle$ is jointly convex, and sketch the proof below: it is equivalent to show the epigraph is convex:

$$K := \left\{(q, Q, t) \mid \langle q, Q^{-1}q\rangle \le t \iff \begin{pmatrix} Q & q \\ q^T & t \end{pmatrix} \succeq 0\right\},$$

where this last equivalence follows by Schur complement. Therefore the constraints are convex functions of $(q, Q)$.

The objective comes from the volume calculation shown above, and it can be shown that $\log\det$ is a concave function for positive-definite input. □

In the remainder, we show how optimality theorem 16 allow us to deduce John's theorem.

### 7.2 Symmetric Case

In this section we prove $\frac{1}{\sqrt{n}}\mathcal{E} \subseteq K \subseteq \mathcal{E}$ for symmetric $K = -K$. We focus on the minimum containing ellipsoid problem because it matches more directly with our proof of the ellipsoid lemma in the next section; but the maximum inscribed ellipsoid has the same (dual) proof. Note that we can assume $q = 0$ by symmetry and convexity: if $(q, Q)$ is feasible then so is $(-q, Q)$ since $K = -K$, so we can assume $q = 0$ without loss of the objective value.

In order to use the theory of convex programming duality, we first need to verify strong duality. We use Slater's condition 15 with, for example $Q = R^{-2}I$ for any $R > \max_i \|x_i\|_2$. This gives a strictly feasible positive definite solution so strong duality and dual attainment holds.

**Proposition 22.** *Let $K \subseteq \mathbb{R}^n$ be compact, compact, full-dimensional, and symmetric $K = -K$. Then the minimum containing ellipsoid satisfies $\frac{1}{\sqrt{n}}\mathcal{E} \subseteq K \subseteq \mathcal{E}$.*

**Proof:** We write the KKT conditions for optimizers $Q, \lambda$: (1) and (2) are simple feasibility conditions; (3) complementary slackness tells us

$$\forall i : \lambda_i(\langle x_i, Qx_i\rangle - 1) = 0 \quad \text{i.e.} \quad (\lambda_i > 0 \implies \langle x_i, Qx_i\rangle = 1).$$

Geometrically, this implies that $\lambda$ is supported on points $x_i$ that lie on the boundary of the optimizing ellipsoid $\partial\mathcal{E} = \{x \mid \langle x, Qx\rangle = 1\}$. Finally (4) Lagrangian optimality gives

$$0 = \nabla_Q \mathcal{L}(Q, \lambda) = -Q^{-1} + \sum_i \lambda_i x_i x_i^T \implies Q^{-1} = \sum_i \lambda_i x_i x_i^T,$$

where we used $\nabla \log\det(Q) = Q^{-1}$, as can be verified by the cofactor expansion for determinant. Note that we implicitly assumed $Q$ is invertible, i.e. $Q \succ 0$. But this follows from the non-degeneracy condition that $K$ is full dimensional.

Using the above conditions, we want to argue that $\frac{1}{\sqrt{n}}\mathcal{E} \subseteq K$. We will argue the contrapositive, so given $y \notin K$ we want to show $y \notin \frac{1}{\sqrt{n}}\mathcal{E}$, i.e. $\langle y, Qy\rangle > 1/n$, since $r\mathcal{E} = \{x \mid \langle x, Qx\rangle \le r^2\}$.

In this section we will mostly perform algebraic manipulations to show the result. In the following non-symmetric case, we will consider a slightly more geometric proof.

So assuming $y \notin K$, we must have a separating hyperplane

$$\exists w : \quad \langle w, y\rangle > \sup_{x\in K} \langle w, x\rangle = \max_i |\langle w, x_i\rangle,$$

where we used that $K = \text{conv}\{x_i\}$ and $K = -K$ is symmetric so we can take the absolute value. Continuing, we have

$$\langle y, Qy\rangle = \|Q^{1/2}y\|_2^2 \geq \frac{\langle Q^{-1/2}w, Q^{1/2}y\rangle^2}{\|Q^{-1/2}w\|_2^2} = \frac{\langle w, y\rangle^2}{\langle w, Q^{-1}w\rangle},$$

where we used that $\|z\|_2 = \max_{\|u\|_2\leq 1}\langle u, z\rangle$. Now we upper bound the denominator

$$\langle w, Q^{-1}w\rangle = \sum_i \lambda_i \langle w, x_i\rangle^2 < \sum_i \lambda_i\langle w, y\rangle^2,$$

where the first step was by optimality $Q^{-1} = \sum_i \lambda_i x_i x_i^T$, and in the final step we used that $w$ is a separating hyperplane. Finally we bound the dual

$$\sum_i \lambda_i \cdot 1 = \sum_i \lambda_i \langle x_i, Qx_i\rangle = \langle Q^{-1}, Q\rangle = n,$$

where the first step was by complementary slackness, $\lambda_i > 0 \implies \langle x_i, Qx_i\rangle = 1$, the second was by optimality for $Q$ again.

Putting this altogether gives our result:

$$y \notin K \implies \langle y, Qy\rangle > \frac{\langle w, y\rangle^2}{\langle w, y\rangle^2}\left(\sum_i \lambda_i\right)^{-1} = \frac{1}{n} \implies y \notin \frac{1}{\sqrt{n}}\mathcal{E}.$$

### 7.3 General Case

In this section we prove the general case of John's theorem. The proof plan is much the same, but a few of the steps are slightly more complicated. We can verify Slater's condition the same way, by choosing a large enough $R > \max_i \|x\|_2$ so that $(0, R^{-2}I)$ is strictly feasible, and we have strong duality by theorem 15. In the remainder we consider optimality conditions and prove the following:

**Proposition 23.** *Let $K \subseteq \mathbb{R}^n$ be compact, convex, and full-dimensional. Then the minimum containing ellipsoid $\mathcal{E}$ with center $c$ satisfies*

$$c + \frac{1}{n}(\mathcal{E} - c) \subseteq K \subseteq \mathcal{E}.$$

**Proof:** We consider KKT conditions for optimizers $(q, Q, \lambda)$: primal feasibility is given in theorem 21, dual feasibility is simply $\lambda \geq 0$; for complementary slackness we have

$$\lambda_i > 0 \implies \quad \langle (x_i - c), Q(x_i - c)\rangle = 0,$$

where $c := Q^{-1}q$ is the center, i.e. $x_i$ is at the boundary of the ellipsoid; and finally Lagrangian optimality gives:

$$\nabla_q \mathcal{L}(q, Q, \lambda) = 2\sum_i \lambda_i(Q^{-1}q - x_i) = 0 \iff \sum_i \lambda_i x_i = \sum_i \lambda_i c$$

$$\nabla_Q \mathcal{L}(q, Q, \lambda) = -Q^{-1} + \sum_i \lambda_i (x_i x_i^T - Q^{-1} q q^T Q^{-1}) = 0 \iff Q^{-1} = \sum_i \lambda_i (x_i - c)(x_i - c)^T,$$

where in both calculations we use $c := Q^{-1} q$ for the center, and in the second we use that $\sum_i \lambda_i x_i = \sum_i \lambda_i c$ from $q$-optimality, so we can replace $\sum_i \lambda_i (x_i x_i^T - cc^T) = \sum_i (x_i - c)(x_i - c)^T$. Next we perform a transformation to simplify notation. Note that all containment relations are invariant under the affine transformation $x \to z := Q^{1/2}(x - c)$. This transformation shifts and scaled our body to $K \to K' := \operatorname{conv}\{z_i\}$, and the minimum containing ellipsoid becomes the Euclidean ball $K' \subseteq B_2^n$. Further, the optimality conditions become

$$c = 0, \quad \sum_i \lambda_i z_i = \sum_i \lambda_i c = 0, \quad I = \sum_i \lambda_i z_i z_i^T,$$

and complementary slackness is $\lambda_i > 0 \implies \|z_i\|_2^2 = 1$.

The remainder follows the original proof of Fritz John (Extremum problems with inequalities as subsidiary conditions). The goal is now to show that $\frac{1}{n} B_2^n \subseteq K'$. For this we will show that $h_{K'}(u) = \sup_{z \in K'} \langle u, z \rangle \geq \|u\|_2 / n$ for all $u$; this implies our containment relation by polar duality:

$$\frac{1}{n} B_2^n \subseteq K' \iff (K')^\circ \subseteq (\frac{1}{n} B_2^n)^\circ \iff \forall u : \sup_{z \in K'} \langle u, z \rangle \geq \frac{1}{n} \sup_{z \in B_2^n} \langle u, z \rangle = \frac{\|u\|_2}{n}.$$

We require two further observations: first note that $K' \subseteq B_2^n$ implies $h_{K'}(u) \leq \|u\|_2$; and second, we can prove $\sum_i \lambda_i = n$ by complementary slackness, just as in the symmetric case.

Now let $u \in S^{n-1}$ and $h_{K'}(u) =: \mu$. Then we must have $\forall i : \langle u, z_i \rangle \in [-1, \mu]$ iff $(\langle u, z_i \rangle + 1)(\langle u, z_i \rangle - \mu) \leq 0$. Now we can use the dual certificate to show the required bound:

$$0 \geq \sum_i \lambda_i (\langle u, z_i \rangle + 1)(\langle u, z_i \rangle - \mu) = \sum_i \lambda_i \langle u, z_i \rangle^2 + (1 - \mu) \sum_i \lambda_i \langle u, z_i \rangle - \sum_i \lambda_i \mu = \|u\|_2^2 + 0 - n\mu,$$

where we used optimality conditions $\sum_i \lambda_i z_i z_i^T = I, \sum_i \lambda_i z_i = 0$ and $\sum_i \lambda_i = n$. Rearranging, this gives $\mu \geq 1/n$, and since $u \in S^{n-1}$ was arbitrary, this shows $\forall u : h_{K'}(u) \geq \|u\|_2 / n$. $\square$

# 8 Ellipsoid Lemma

We restate the required result for the Ellipsoid algorithm:

**Lemma 24** (Lemma 2.3 in Bubeck). *Let $\mathcal{E} := \{x \in \mathbb{R}^n \mid \langle (x - c_p), P(x - c_p) \rangle \leq 1\}$ be an Ellipsoid with $P \succ 0$; and let $H := \{x \in \mathbb{R}^n \mid \langle w, x \rangle \leq \langle w, c_p \rangle\}$ be a halfspace through the center of $\mathcal{E}$. Then there exists ellipsoid $\overline{\mathcal{E}}$ such that*

$$\overline{\mathcal{E}} \supset \mathcal{E} \cap H \quad \textit{and} \quad \mathit{vol}(\overline{\mathcal{E}}) \leq \mathit{vol}(\mathcal{E}) \exp(-1/2n).$$

*Further, if $n \geq 2$ then $\overline{\mathcal{E}} := \{x \in \mathbb{R}^n \mid \langle (x - c), Q(x - c) \rangle \leq 1\}$ where*

$$c := c_p - \frac{1}{n+1} \frac{P^{-1} w}{\sqrt{\langle w, P^{-1} w \rangle}}, \qquad Q := \left(1 - \frac{1}{n^2}\right) P + \frac{2(n+1)}{n^2} \frac{w w^T}{\langle w, P^{-1} w \rangle}.$$

We first verify that the proposed ellipsoid satisfies the volume bound. Then we show how to derive this update using minimum containing ellipsoid and convex duality. For the remainder, we perform an affine transformation to simplify notation: for $x \to P^{1/2}(x - c_p)$, the original ellipsoid becomes $\mathcal{E} = B_2^n$ with center $c_p = 0$, and without loss we can assume the halfspace is defined by normal vector $\|w\|_2 = 1$.

**Proposition 25.** *For large enough $n$ update ellipsoid given in theorem 24 satisfies*

$$vol(\overline{\mathcal{E}}) \leq vol(\mathcal{E}) \exp(-\Omega(1/n)).$$

**Proof:** We rewrite the update after the affine transformation:

$$c = -\frac{1}{n+1} w, \qquad Q = \left(1 - \frac{1}{n^2}\right) I + \frac{2(n+1)}{n^2} w w^T.$$

Recall the volume of the ellipsoid is proportional to the inverse square root of the determinant, so we want to lower bound

$$\det(Q) = \left(1 - \frac{1}{n^2}\right)^{n-1} \left(1 - \frac{1}{n^2} + \frac{2(n+1)}{n^2}\right) \approx \exp\left(\frac{-(n-1) + 2n + 1}{n^2}\right) \geq \exp\left(\frac{1}{n}\right),$$

where we used the heuristic Taylor approximation $1 + x \approx e^x$ for small $x$. The exact calculation is performed properly in the proof in [Bubeck]. □

In the remainder, we sketch how the KKT conditions for minimum containing ellipsoid allow us to derive and certify the update. We follow the notes of Daniel Dadush. In particular, recall the convex program

$$\min -\log\det(Q) \qquad \text{s.t.} \quad \forall x \in \mathcal{E} \cap H : \quad q(x) := \langle (x - c), Q(x - c) \rangle \leq 1. \tag{3}$$

We first observe that our problem is symmetric around the $w$ axis since $\mathcal{E} = B_2^n$. Therefore if $q$ is feasible, then so is any rotation around $w$, and so by convexity we can without loss assume the solution is symmetric around the $w$ axis. Next, we observe that $p(x) := \langle x, Ix \rangle$, i.e. $c = 0, Q = I$, is a feasible solution as $B_2^n \supseteq B_2^n \cap H$. We also consider another feasible solution given

$$\delta(x) := \langle (x - \frac{1}{2} w), (4ww^T)(x - \frac{1}{2} w) \rangle = 4(\langle x, w \rangle - \frac{1}{2})^2.$$

This defines the degenerate ellipsoid $\{x \mid \langle x, w \rangle \in [0,1]\}$ and clearly also contains $B_2^n \cap H$. By convexity, this implies $q_\gamma := (1 - \gamma)p + \gamma\delta$ is also a feasible solution for all $\gamma \in [0,1]$. We can calculate the center and matrix

$$c_\gamma = (1 - \gamma) \cdot 0 + \frac{\gamma}{2} w = \frac{\gamma}{2} w, \quad Q_\gamma = (1 - \gamma) I + 4\gamma w w^T.$$

This matches the symmetry structure that we expect from our solution.

Finally, we write down the KKT conditions where we used $K := B_2^n \cap H$ for shorthand. Note that we have infinite dual variables $\{\lambda_x\}_{x \in K}$ (we sweep these technicalities under the rug), so we use integrals instead of sums:

$$\nabla = 0 \implies \quad \int_{x \in K} \lambda_x (x - c) = 0; \quad Q^{-1} = \int_{x \in K} \lambda_x (x - c)(x - c)^T;$$

$$(CS): \quad \operatorname{supp}(\lambda) \subseteq \{x \mid q(x) = 1\}.$$

For the candidate primal solution $q_\gamma$, if we can verify feasibility and find a dual solution satisfying the above, then theorem 17 proves optimality. We can interpret the KKT conditions as looking for a measure $\lambda$ on contact points with mean $c$ and covariance $Q^{-1}$. We next show how to construct a family of measures meeting these criteria for $(c_\gamma, Q_\gamma)$: for each $\alpha$, let $\lambda^\alpha$ put $\alpha$ probability at $w$

and the remaining $1-\alpha$ probability uniformly on $S^{n-1} \cap \partial H$, i.e. the great circle at the bound of the intersection $B_2^n \cap H$. We can calculate mean and covariance:

$$\mathbb{E}_{\lambda^\alpha}[x] = \alpha w + (1-\alpha) \int_{S^{n-1} \cap \partial H} x = \alpha w =: c,$$

$$\mathbb{E}_{\lambda^\alpha}[xx^T] - cc^T = \alpha w w^T + (1-\alpha) \int_{S^{n-1} \cap \partial H} xx^T - \alpha^2 w w^T = \alpha(1-\alpha) w w^T + \frac{1-\alpha}{n-1}(I - w w^T).$$

This roughly matches the family $(c_\gamma, Q_\gamma^{-1})$. To finish, we need to check which value of $\gamma$ gives primal feasibility and which value of $\alpha$ gives complementary slackness. We leave these verifications as exercises for the reader.