

CS675: Convex and Combinatorial Optimization  
Fall 2016  
The Ellipsoid Algorithm

Instructor: Shaddin Dughmi

# History and Basics

- Originally developed in the mid 70s by Iudin, Nemirovski, and Shor for use as a heuristic for convex optimization
- In 1979, Kachiyan shows that it yields a polynomial time algorithm for LP

# History and Basics

- Originally developed in the mid 70s by Iudin, Nemirovski, and Shor for use as a heuristic for convex optimization
- In 1979, Kachiyan shows that it yields a polynomial time algorithm for LP
- Inefficient in practice, has been surpassed by newer interior point methods.

# History and Basics

- Originally developed in the mid 70s by Iudin, Nemirovski, and Shor for use as a heuristic for convex optimization
- In 1979, Kachiyan shows that it yields a polynomial time algorithm for LP
- Inefficient in practice, has been surpassed by newer interior point methods.
- Theoretically most powerful, with deep consequences for complexity and optimization
  - Polynomial-time algorithm for linear programming
  - Polynomial-time algorithm for approximate convex optimization under mild conditions
  - Equivalence of separation and optimization

# Outline

- 1 Description of The Ellipsoid Method
- 2 Properties

## Convex Feasibility Problem

Given as input the following

- A description of a compact convex set  $K \subseteq \mathbb{R}^n$
- An ellipsoid  $E(c, Q)$  (typically a ball) containing  $K$
- A rational number  $R > 0$  satisfying  $\text{vol}(E) \leq R$ .
- A rational number  $r > 0$  such that if  $K$  is nonempty, then  $\text{vol}(K) \geq r$ .

Find a point  $x \in K$  or declare that  $K$  is empty.

- Note: convex optimization reduces to checking feasibility by binary search
  - We will explain later how the parameters  $r, R, E$  figure into this
- Description of  $K$ : any description that admits an efficient implementation of a **separation oracle**

## Separation oracle

An algorithm that takes as input  $x \in \mathbb{R}^n$ , and either certifies  $x \in K$  or outputs a hyperplane separating  $x$  from  $K$ .

- i.e. a vector  $h \in \mathbb{R}^n$  with  $h^\top y < h^\top x$  for all  $y \in K$ .
- Equivalently,  $K$  is contained in the halfspace

$$H(h, x) = \{y : h^\top y < h^\top x\}$$

with  $x$  at its boundary.

## Separation oracle

An algorithm that takes as input  $x \in \mathbb{R}^n$ , and either certifies  $x \in K$  or outputs a hyperplane separating  $x$  from  $K$ .

- i.e. a vector  $h \in \mathbb{R}^n$  with  $h^\top y < h^\top x$  for all  $y \in K$ .
- Equivalently,  $K$  is contained in the halfspace

$$H(h, x) = \{y : h^\top y < h^\top x\}$$

with  $x$  at its boundary.

Examples:



## Separation oracle

An algorithm that takes as input  $x \in \mathbb{R}^n$ , and either certifies  $x \in K$  or outputs a hyperplane separating  $x$  from  $K$ .

- i.e. a vector  $h \in \mathbb{R}^n$  with  $h^\top y < h^\top x$  for all  $y \in K$ .
- Equivalently,  $K$  is contained in the halfspace

$$H(h, x) = \{y : h^\top y < h^\top x\}$$

with  $x$  at its boundary.

Examples:

- Explicitly written polytope  $Ay \leq b$ : take  $h = a_i$  where the  $i$ th constraint is violated by  $x$ .

## Separation oracle

An algorithm that takes as input  $x \in \mathbb{R}^n$ , and either certifies  $x \in K$  or outputs a hyperplane separating  $x$  from  $K$ .

- i.e. a vector  $h \in \mathbb{R}^n$  with  $h^\top y < h^\top x$  for all  $y \in K$ .
- Equivalently,  $K$  is contained in the halfspace

$$H(h, x) = \{y : h^\top y < h^\top x\}$$

with  $x$  at its boundary.

Examples:

- Explicitly written polytope  $Ay \leq b$ : take  $h = a_i$  where the  $i$ th constraint is violated by  $x$ .
- Convex set given by a family of convex inequalities  $f_i(y) \leq 0$ : Let  $h = \nabla f_i(x)$  for some violated constraint.

## Separation oracle

An algorithm that takes as input  $x \in \mathbb{R}^n$ , and either certifies  $x \in K$  or outputs a hyperplane separating  $x$  from  $K$ .

- i.e. a vector  $h \in \mathbb{R}^n$  with  $h^\top y < h^\top x$  for all  $y \in K$ .
- Equivalently,  $K$  is contained in the halfspace

$$H(h, x) = \{y : h^\top y < h^\top x\}$$

with  $x$  at its boundary.

Examples:

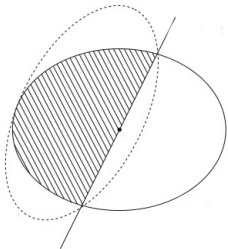
- Explicitly written polytope  $Ay \leq b$ : take  $h = a_i$  where the  $i$ th constraint is violated by  $x$ .
- Convex set given by a family of convex inequalities  $f_i(y) \leq 0$ : Let  $h = \nabla f_i(x)$  for some violated constraint.
- The positive semi-definite cone  $S_n^+$ : Let  $H = -vv^\top$ , where  $v$  is an eigenvector  $X$  corresponding to a negative eigenvalue.



- Unit ball  $B(0, 1) = \{x \in \mathbb{R}^n : x^\top x \leq 1\}$ .
- **Ellipsoid**: the result of applying some affine transformation  $x \rightarrow Lx + c$  to  $B(0, 1)$ .
  - Gives the set  $\{x : (x - c)^\top L^{-\top} L^{-1} (x - c) \leq 1\}$
- It is conventional to take  $Q = LL^\top$ , which is symmetric PSD, and write the ellipsoid as

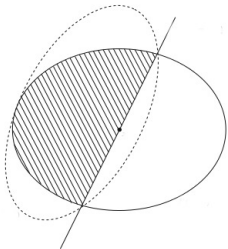
$$E(c, Q) = \{x : (x - c)^\top Q^{-1} (x - c) \leq 1\}$$

- Can calculate **volume** easily:  $\text{vol}(E(c, Q)) = \sqrt{\det Q} \text{vol}(B(0, 1))$
- Note: since  $Q \succeq 0$  has a PSD square root, can take  $L$  to be PSD as well



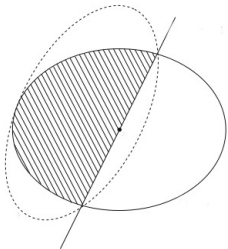
## Ellipsoid Method

- 1 Start with initial ellipsoid  $E = E(c, Q) \supseteq K$
- 2 Using the separation oracle, check if the center  $c \in K$ .
  - If so, terminate and output  $c$ .
  - Otherwise, we get a separating hyperplane  $h$  such that  $K$  is contained in the half-ellipsoid  $E \cap \{y : h^\top y \leq h^\top c\}$
- 3 Let  $E' = E(c', Q')$  be the minimum volume ellipsoid containing the half ellipsoid above.
- 4 If  $\text{vol}(E') \geq r$  then set  $E = E'$  and repeat (step 2), otherwise stop and return “empty”.



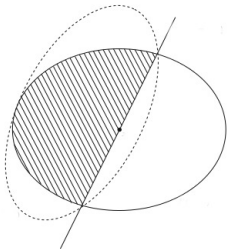
## Ellipsoid Method

- 1 Start with initial ellipsoid  $E = E(c, Q) \supseteq K$
- 2 **Using the separation oracle, check if the center  $c \in K$ .**
  - If so, terminate and output  $c$ .
  - Otherwise, we get a separating hyperplane  $h$  such that  $K$  is contained in the half-ellipsoid  $E \cap \{y : h^\top y \leq h^\top c\}$
- 3 Let  $E' = E(c', Q')$  be the minimum volume ellipsoid containing the half ellipsoid above.
- 4 If  $\text{vol}(E') \geq r$  then set  $E = E'$  and repeat (step 2), otherwise stop and return “empty”.



## Ellipsoid Method

- 1 Start with initial ellipsoid  $E = E(c, Q) \supseteq K$
- 2 Using the separation oracle, check if the center  $c \in K$ .
  - If so, terminate and output  $c$ .
  - Otherwise, we get a separating hyperplane  $h$  such that  $K$  is contained in the half-ellipsoid  $E \cap \{y : h^\top y \leq h^\top c\}$
- 3 **Let  $E' = E(c', Q')$  be the minimum volume ellipsoid containing the half ellipsoid above.**
- 4 If  $\text{vol}(E') \geq r$  then set  $E = E'$  and repeat (step 2), otherwise stop and return “empty”.



## Ellipsoid Method

- 1 Start with initial ellipsoid  $E = E(c, Q) \supseteq K$
- 2 Using the separation oracle, check if the center  $c \in K$ .
  - If so, terminate and output  $c$ .
  - Otherwise, we get a separating hyperplane  $h$  such that  $K$  is contained in the half-ellipsoid  $E \cap \{y : h^\top y \leq h^\top c\}$
- 3 Let  $E' = E(c', Q')$  be the minimum volume ellipsoid containing the half ellipsoid above.
- 4 If  $\text{vol}(E') \geq r$  then set  $E = E'$  and repeat (step 2), otherwise stop and return “empty”.



# Outline

- 1 Description of The Ellipsoid Method
- 2 Properties

## Theorem

If the ellipsoid algorithm terminates, then it either outputs  $x \in K$  or correctly declares that  $K$  is empty.

- Algorithm outputs some  $x$  only if it was certified in  $K$  by the separation oracle
- $E \supseteq K$  is maintained throughout the algorithm, by definition
- We are promised  $\text{vol}(K) < r$  only if  $K = \emptyset$
- If algorithm outputs empty then  $r > \text{vol}(E) \geq \text{vol}(K)$ , and  $K = \emptyset$ .

To prove that the ellipsoid method runs in polynomial time, we need the following lemma

## Lemma

- The minimum volume ellipsoid  $E'$  containing half of another ellipsoid  $E$  can be computed in  $\text{poly}(n)$  operations.
- Moreover, the volume of  $E'$  is smaller than the volume of  $E$  by a factor of at least  $e^{\frac{1}{2(n+1)}} \approx 1 + \frac{1}{2(n+1)}$ .

This is tricky to show, but there is an explicit, easy-to-compute, closed form for the matrix and center of  $E'$  in terms of the matrix and center of  $E$ . (See notes for proof)

## Theorem

The ellipsoid method terminates after  $2(n + 1) \ln \frac{R}{r}$  iterations. Moreover, each iteration can be implemented using  $\text{poly}(n)$  operations and a single call to the separation oracle.

- Volume of working ellipsoid starts off at  $R$
- Decreases by a factor of  $e^{\frac{1}{2(n+1)}}$  each iteration.
- After  $2(n + 1) \ln \frac{R}{r}$  iterations, volume is less than  $r$ , triggering termination.

## Theorem

The ellipsoid method terminates after  $2(n + 1) \ln \frac{R}{r}$  iterations. Moreover, each iteration can be implemented using  $\text{poly}(n)$  operations and a single call to the separation oracle.

- Volume of working ellipsoid starts off at  $R$
- Decreases by a factor of  $e^{\frac{1}{2(n+1)}}$  each iteration.
- After  $2(n + 1) \ln \frac{R}{r}$  iterations, volume is less than  $r$ , triggering termination.
- In each iteration, we
  - Call the separation oracle (Assumed constant time)
  - Compute the minimum volume ellipsoid ( $\text{poly}(n)$  time by lemma)
  - Compute the volume of  $E'$  (reduces to determinant computation).