Convexity

Prof. Friedrich Eisenbrand
Christoph Hunkenschröder

Assignment Sheet 5 - Solutions

October 27, 2016

Exercise 1

Let $K \subsetneq \mathbb{R}^n$ be a closed convex set and $p \in \mathbb{R}^n \setminus K$.

Prove that there exists a *unique* point $x \in K$ minimizing the distance to p, i.e. $\|x - p\| \leq \|y - p\|$ for all $y \in K$.

Solution:

As K is closed, let $x, y \in K$ be two points with $\|x - p\| = \|y - p\| \leq \|z - p\|$ for all $z \in K$.

By convexity, $\frac{1}{2}x + \frac{1}{2}y \in K$ as well. First notice

$$(\frac{1}{2}x + \frac{1}{2}y - p)^T(x - y) = \underbrace{\frac{1}{2}\|x - p\|^2 - \frac{1}{2}\|y - p\|^2}_{=0} + \frac{1}{2}(y - p)^T(x - p) - \frac{1}{2}(x - p)^T(y - p) = 0.$$

We know $\|x - p\| \leq \|\frac{1}{2}(x + y) - p\|$ by choice of x and y. On the other hand we have

$$\|x - p\|^2 = \|\frac{1}{2}(x + y) - p + \frac{1}{2}(x - y)\|^2 = \|\frac{1}{2}(x + y) - p\|^2 + \|\frac{1}{2}(x - y)\|^2.$$

But this implies $x = y$, hence the closest point is unique.

Exercise 2

Let $K \subset \mathbb{R}^d$ be a compact convex body with a non-empty interior and suppose you are given E_{in}, the ellipsoid of largest volume contained in K.

Show how to compute a vector $u \in \mathbb{Z}^d$ s.t. $\max_{x,y \in K} u^\intercal(x - y) \leq d \cdot w(K)$ by one shortest lattice vector computation, where $w(K)$ is defined to be

$$w(K) = \min_{u \in \mathbb{Z}^d \setminus \{0\}} \max_{x,y \in K} u^\intercal(x - y)$$

Solution:

Suppose the ellipsoid E_{in} is generated by $A \in \mathbb{R}^{d \times d}$ and $b \in \mathbb{R}^d$. Then for any vector $u \in \mathbb{Z}^d \setminus \{0\}$ we have that

$$\max_{x,y,\in K} u^\intercal(x - y) \leq \max_{x,y \in E_{out}} u^\intercal(x - y) = d \max_{x,y \in E_{in}} u^\intercal(x - y)$$

Note that

$$\max_{x,y \in E_{in}} u^\intercal(x - y) = \max_{x,y \in B_1^d} u^\intercal(Ax + b - Ay - b) = \max_{x,y \in B_1^d} (A^\intercal u)^\intercal(x - y) = 2\|A^\intercal u\|$$

In particular, $A^\intercal u \in \Lambda(A)$, and so in one shortest vector computation we get $u \in \mathbb{Z}^d \setminus \{0\}$ minimizing the quantity $\|A^\intercal u\|$. For this u we have

$$\max_{x,y \in E_{in}} u^\intercal(x - y) = \min_{u \in \mathbb{Z}^d \setminus \{0\}} \max_{x,y \in E_{in}} u^\intercal(x - y) = w(E_{in}) \leq w(K)$$

so in fact we have

$$\max_{x,y\in K} u^\intercal (x-y) \le d \cdot w(K)$$

as required.

Exercise 3 [$\star$]
Two sets $X, Y \subseteq \mathbb{R}^n$ are called *strictly separable* if there is a hyperplane $a^T x = b$ such that $a^T x < b$ for all $x \in X$ and $a^T y > b$ for all $y \in Y$.
Prove that two disjoint closed balls $B(z_1, r_1), B(z_2, r_2) \subseteq \mathbb{R}^n$ are strictly separable.
Prove or disprove the following statement: Any two disjoint closed convex sets are strictly separable.

Solution:
The first part. Write $d = \|z_2 - z_1\| > r_1 + r_2$, $g = (z_2 - z_1)$ and define

$$z := z_1 + \frac{d + r_1 - r_2}{2d} g = z_2 + \frac{d - r_1 + r_2}{2d}(-g)$$

to be the middle point between the balls (not the middle point between the centers). We claim that the hyperplane $g^T x = g^T z$ separates the ball. Any point on $\partial B(z_1, r_1)$ can be written as $z_1 + r_1 e$, where e is a vector of unit length. Calculating

$$\begin{aligned} g^T(z_1 + r_1 e) &\le g^T z_1 + r_1 g^T \frac{g}{d} \\ &< g^T z_1 + \frac{2r_1 + d - r_1 - r_2}{2} g^T \frac{g}{d} \\ &= g^T z \end{aligned}$$

shows $g^T x < g^T z$ for all $x \in B(z_1, r_1)$, where we used $0 < d - r_1 - r_2$. By the symmetric characterisation of z, the same calculation shows $g^T x > g^T z$ for $x \in B(z_1, r_1)$, finishing the proof.

The second part is not always true. For example, choose $K_1 = \{x \in \mathbb{R}^2 : x_1 \le 0\}$, which is a polyhedron, hence closed and convex, and choose $K_2 = \{x \in \mathbb{R}^2 : x_1, x_2 \ge 0,\ x_1 x_2 \ge 1\}$. Let us first show that K_2 is indeed closed and convex. Consider a sequence $\{y_k\}_{k\in\mathbb{N}}$ in K_2, converging to $y^\star$. As K_2 is a subset of the closed set $\{x \in \mathbb{R}^2 : x_1, x_2 \ge 0\}$, we have $y^\star = (y_1^\star, y_2^\star) \ge 0$. For any $\epsilon > 0$ we can find some index k and $\epsilon_1, epsilon_2 \in [0, \epsilon]$ s.t. $y_k = y^\star + (\epsilon_1, \epsilon_2)$. Hence, $(y_1^\star + \epsilon_1)(y_2^\star + \epsilon_2) \le y_1^\star y_2^\star + \epsilon(y_1^\star + y_2^\star) + \epsilon^2 \ge 1$. Thus $y^\star \in K_2$.

For convexity, consider $x, y \in K_2$ and find

$$\begin{aligned} (\lambda x_1 + (1-\lambda) y_1)(\lambda x_2 + (1-\lambda) y_2) &= \lambda^2 x_1 x_2 + (1-\lambda)^2 y_1 y_2 + \lambda(1-\lambda)(x_1 y_2 + x_2 y_1) \\ &= 1 - 2\lambda(1-\lambda) + \lambda(1-\lambda)(x_1 y_2 + x_2 y_1) \\ &\ge 1 + \lambda(1-\lambda) \underbrace{\left(\frac{x_1}{y_1} + \frac{y_1}{x_1} - 2\right)}_{=x_1^2 + y_1^2 - 2x_1 y_1 \ge 0} \\ &\ge 1. \end{aligned}$$

Remember that K_1 is described by $x_1 \le 0$ and notice that $x_1 x_2 \ge 1$ in fact tightens the condition $x_1 \ge 0$ for K_2 to be strict. Hence, $K_1 \cap K_2 = \emptyset$.

It remains to show that there is no strictly separating hyperplane. As K_1 is the half space $e_2^x \le 0$, each strictly separating hyperplane has to be of the form $e_2^T x = h$, where $h > 0$. But defining $y_2 = \frac{h}{2}$ and $y_1 = \frac{2}{h}$ shows that each of those hyperplanes intersects non-trivially with K_2, hence there is no hyperplane strictly separating K_1 and K_2. Note that this counterexample can be lifted to an arbitrary dimension n by considering $K_i' := K_i \times \mathbb{R}^{n-2}$.

Exercise 4
Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $\mathcal{V}$ its voronoi cell.

1. Show $\operatorname{vol}\mathcal{V} = \det\Lambda$.
2. Show $\mu(\Lambda) = \max_{x\in\mathcal{V}} \|x\|$.

Solution:

1. Let B be a basis of Λ and let $\mathcal{P}$ denote the fundamental parallelepiped to this basis.

   We saw in the lecture that $\Lambda + \mathcal{P}$ tiles the space, and also briefly discussed that $\Lambda + \mathcal{V}$ tiles the space (up to a set of measure 0). For now, assume both statements to be true, we will show it for the voronoi cell in detail later on.

   Consider $L = B(0,R) \cap \Lambda$ and compare $\operatorname{vol}(L+\mathcal{P})$ with $\operatorname{vol}(L+\mathcal{V})$. Let $d_p \in \mathbb{R}$ large enough s.th. $\mathcal{P} \subseteq B(0,d_p)$, and $d_v \in \mathbb{R}$ large enough s.th. $\mathcal{V} \subseteq B(0,d_v)$ (note that according to the lecture, both $\mathcal{P},\mathcal{V}$ are bounded). This means that $\operatorname{vol}(L+\mathcal{P}) \subseteq B(0,R+d_p)$ and $\operatorname{vol}(L+\mathcal{V}) \subseteq B(0,R+d_v)$ and by the tiling property

   $$|L|\operatorname{vol}\mathcal{P} \le \operatorname{vol}B(0,R+d_p)$$
   $$|L|\operatorname{vol}\mathcal{V} \le \operatorname{vol}B(0,R+d_v)$$
   $$\Rightarrow \qquad \frac{\operatorname{vol}\mathcal{P}}{\operatorname{vol}\mathcal{V}} \le \frac{R+d_p}{R+d_v} \qquad \text{and} \qquad \frac{\operatorname{vol}\mathcal{V}}{\operatorname{vol}\mathcal{P}} \le \frac{R+d_v}{R+d_p}.$$

   Taking the limit yields $\operatorname{vol}\mathcal{V} = \operatorname{vol}\mathcal{P}$.

   It is left to show that $\mathcal{V}$ tiles the space up to a set of measure zero. This is, we want to show $\mathbb{R}^n \subseteq \Lambda + \mathcal{V}$ and $\operatorname{int}\mathcal{V} \cap \operatorname{int}(p+\mathcal{V}) = \emptyset$.

   For the first point, let $x \in \mathbb{R}^n$ and let p be a closest vector. If $x - p \in \mathcal{V}$, then $x \in (p+\mathcal{V})$, hence assume $p = 0$. If x was not in $\mathcal{V}$, then there was a point $y \in \Lambda$ s.t. $y^T x > \frac{1}{2}y^T y$, implying $\|x-y\|^2 > \|x\|^2$, a contradiction.

   For the second property, assume there is some $p \in \Lambda$ and $z \in \mathcal{V} \cap (p+\mathcal{V})$. We want to show that p is on the boundary. As the voronoi cell is contained in the half-space $p^T x \le \frac{1}{2}p^T p$, we have $p^T z \le \frac{1}{2}p^T p$, as z is in the interior. But for the shiftet cell $(p+\mathcal{V})$ we have the feasible inequality

   $$\|x-p\|^2 \le \|x-0\|^2 \quad \Leftrightarrow \quad -p^T x \le -\frac{1}{2}p^T p.$$

   Hence, $p^T z = \frac{1}{2}p^T p$ and z is on the boundary.

2. As the voronoi cell is defined to be the set of all vectors for which 0 is the closest lattice vector,

   $$\mu(\Lambda) \ge \max_{x\in\mathcal{V}} \|x\|$$

   follows immediately. For the other direction, let $x \in \mathbb{R}^n$ be any point farthest from the lattice and let p be a closest lattice point. Then $x \in (p+\mathcal{V})$, hence $\mu(\Lambda) \le \max_{x\in\mathcal{V}} \|x\|$ is sufficient.

Exercise 5

Let C be a convex cone and $-C$ the cone $\{x : -x \in C\}$. We call $L = C \cap -C$ the *lineality space* of C. We call a cone *pointed* if 0 is an extreme point.

1. Prove that $\overline{C} := C \cap L^\perp$, where $L^\perp = \{u : u^T x = 0 \ \forall x \in L\}$, is a pointed cone and that C is the direct sum of its lineality space L and the pointed cone $\overline{C}$, i.e.

$$C = (C \cap L^\perp) \oplus L.$$

2. Show that any polyhedron has a decomposition

$$P = (Q + C) \oplus L,$$

where Q is a polytope, C is a pointed cone and L is a linear subspace.

[*Attention: in this exercise,* $\oplus$ *denotes the direct sum, while we refer to Minkowski's sum by* $+$.]

Solution:

1. Let $C \subseteq \mathbb{R}^n$ be the convex cone (and notice that it neither has to be finitely generated, nor polyhedral!). First note that $L \cap (C \cap L^\perp) = \{0\}$ by definition.

   For showing $C \subseteq (C \cap L^\perp) \oplus L$ let $v_1, \ldots, v_r$ be an orthonormal basis of the lineality space. Extend this basis by $v_{r+1}, \ldots, v_n$ to an orthonormal basis of the whole space. For some $\lambda_i \in \mathbb{R}$, any element $u \in C$ can be written as

$$u = \sum_{i=1}^{n} \lambda_i v_i = \underbrace{\sum_{i=1}^{r} \lambda_i v_i}_{=u_1} + \underbrace{\sum_{i=r+1}^{n} \lambda_i v_i}_{=u_2}.$$

   We have to show that $u_1 \in L$ and $u_2 \in (C \cap L^\perp)$. The containments $u_1 \in L$ and $u_2 \in L^\perp$ are clear, so we are left with $u_2 \in C$. But as $u \in C$ and $u_1 \in L \Rightarrow -u_1 \in L \subseteq C$, we find $u_2 = u - u_1 \in C$ as a conic combination.

   As $(C \cap L^\perp) \subseteq C$ and $L \subseteq C$, the other direction is clear.

   On the last sheet we had different characterizations of extreme points. Assume 0 is not an extreme point. Then there are nonzero vectors $u_1, \ldots, u_s \in \overline{C}$ together with nonzero coefficients $\alpha_1, \ldots, \alpha_s \geq 0$ s.t.

$$\sum_{i=1}^{s} \alpha_i u_i = 0 \quad \Rightarrow \quad \alpha_s u_s = -\sum_{i=1}^{s-1} \alpha_i u_i.$$

   But then $\alpha_i u_i \in L$, a contradiction. Hence $\overline{C}$ is a pointed cone.

2. By the lecture we have a decomposition $P = Q + C$ with a polytope Q and a cone C. Now we take the decomposition of the first part for our cone $C = \overline{C} \oplus L$, but it might be that $Q \cap L \neq \{0\}$. As a result of the lecture, we know that Q can be written as the convex hull of points $\{p_i\}_{i \in I}$ for some finite set I. For $i \in I$, define $q_i = \mathrm{pr}_L(p_i)$ as the projection of p_i onto $L^\perp$ and set $\overline{Q} = \mathrm{conv}\{q_i : i \in I\}$. Checking $Q + L = \overline{Q} \oplus L$ finishes the proof, as

$$Q + C = Q + (\overline{C} \oplus L) = (\overline{Q} \oplus L) + (\overline{C} + L) = (\overline{Q} + \overline{C}) \oplus L.$$