Convexity

Prof. Friedrich Eisenbrand
Christoph Hunkenschröder

Assignment Sheet 2 - Solutions

September 29, 2016

Exercise 1
Let $\mathrm{X} \subseteq \mathbb{R}^2$. For each point $x \in \mathrm{X}$, let us denote $V(x)$ the set of all points $y \in \mathrm{X}$ that can "see" x, i.e. points s.t. the segment xy is contained in X. More formally, for $x \in \mathrm{X}$ let

$$V(x) = \{y \in \mathrm{X} : \forall \lambda \in [0,1], \lambda x + (1-\lambda)y \in \mathrm{X}\}$$

The *kernel* of X is the set of all points $x \in \mathrm{X}$ for which $V(x) = \mathrm{X}$.

a) Prove that the kernel of any set $\mathrm{X} \subseteq \mathbb{R}^2$ is convex.

b) Construct a nonempty set $\mathrm{X} \subseteq \mathbb{R}^2$ such that each of its finite subsets can be seen from some point of X but the kernel of X is empty.

Solution:

a) Let $\mathrm{X} \subseteq \mathbb{R}^2$ and let K be its kernel. Fix $x, y \in K$ and $\lambda \in (0,1)$. We want to show that $z = \lambda x + (1-\lambda)y$ is in K. So $\forall w \in \mathrm{X}$ and $\mu \in (0,1)$, we want that $\mu z + (1-\mu)w \in \mathrm{X}$.

   But

$$\begin{aligned} \mu z + (1-\mu)w &= \mu\lambda x + \mu(1-\lambda)y + (1-\mu)z \\ &= (\mu\lambda)x + (1-\mu\lambda)\left(\frac{\mu(1-\lambda)}{(1-\mu\lambda)}y + \frac{1-\mu}{(1-\mu\lambda)}w\right) \end{aligned}$$

   Now, it is easy to check that

$$u = \frac{\mu(1-\lambda)}{(1-\mu\lambda)}y + \frac{1-\mu}{(1-\mu\lambda)}w \in \mathrm{X}$$

   as $y \in K$. But then also $(\mu\lambda)x + (1-\mu\lambda)y \in X$ as $x \in K$. So we are done.

b) An example is $\mathbb{R}^2 \backslash \{0\}$, or any other convex set in $\mathbb{R}^2$ without one interior point. Another example is an open half-strip with a square cut out of it as shown on the picture below:

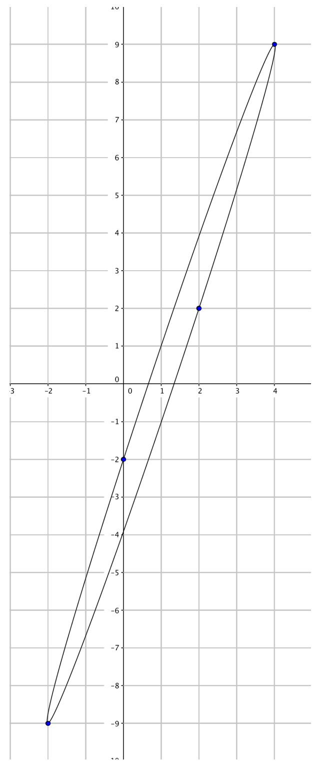
1. 

Figure 1: The ellipsoid E

Exercise 2
Let E be the ellipsoid $f(B(0,1))$, where $f: \ x \mapsto Ax + b$ with a non-singular matrix $A \in \mathbb{R}^{n \times n}$.

1. Let $n = 2$ and
$$A = \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} \qquad b = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
Draw the ellipsoid E. What are the axes of E?

2. Let $\Lambda = \Lambda(B)$ be a lattice and $E = \{x \in \mathbb{R}^n \mid x^T Q x \leq 1\}$ with matrices
$$B = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} \\ 0 & \frac{1}{2} \end{pmatrix}, \qquad Q = \begin{pmatrix} \frac{1}{4} & \frac{1}{8} \\ \frac{1}{8} & \frac{5}{16} \end{pmatrix}.$$
Show that there is a bijection between the sets $\Lambda \cap B(0,1)$ and $E \cap \mathbb{Z}^2$.
[Hint: Is there a relation between the matrices B and Q?]

Solution:

Doing the math yields us
$$Q = A^{-T}A^{-1} = \frac{1}{9}\begin{pmatrix} 9 & -2 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} 9 & -3 \\ -2 & 1 \end{pmatrix} = \frac{1}{9}\begin{pmatrix} 85 & -29 \\ -29 & 10 \end{pmatrix}.$$
The eigenvectors of Q are
$$\xi_{1,2} = \begin{pmatrix} \frac{1}{58}\left(-75 \pm \sqrt{8989}\right) \\ 1 \end{pmatrix}$$
and the axes of E are thus the unit orthogonal eigenvectors $\frac{\xi_1}{\|\xi_1\|}$ and $\frac{\xi_2}{\|\xi_2\|}$.

2. An ellipsoid is the image of the unit ball under an affine transformation A, and can be written as the set $\langle x| \; x^T A^{-T} Ax\rangle$. It is easy to check that in our case $Q = B^T B$, which means that the matrix transforming the unit ball to the ellipsoid is B^{-1}. The matrix B has full rank, hence can be seen as a bijection from Z^2 to Λ. Moreover, for any $t \in \mathcal{E} \cap \mathbb{Z}^2$ we find $t^T B^T Bt \leq 1$ implying that the lattice point Bt is in the unit ball. Vice versa, if Bt is in the unit ball, the vector t is in the ellipsoid.

Exercise 3

Recall the definition of the successive minima of a (for this exercise) full-dimensional lattice $\Lambda \subseteq \mathbb{R}^n$.

$$\lambda_k := \min\{r \geq 0 \mid \dim(B(0, r) \cap \Lambda) \geq k\}, \qquad k = 1, \ldots, n.$$

This definition might suggest that any lattice Λ possesses a basis $B = (b_1, \ldots, b_n)$ with $\|b_k\| = \lambda_k$ for all k.

However, this is not true in general. Show for $n \geq 5$ that there exists a lattice where you cannot find a basis with this property.

Solution:

Let $\Lambda = \{x \in \mathbb{Z}^n \mid x_i \equiv_2 x_j \; \forall \; i, j\}$, i.e. each lattice point has either only even or only odd coordinates. It is easy to check that Λ is indeed a lattice, i.e. closed under addition, multiplication by integral scalars and discrete (as a subset of $\mathbb{Z}^n$).

Let e_i be the i-th canonic unit vector. As $2e_i \in \Lambda$ for all i, we find $\lambda_i \leq 2$, $i = 1, \ldots, n$. Now consider a lattice point p with odd coordinates. Each $|p_i|$ is at least 1, hence $\|p\|^2 \geq n$. Using the assumption $n \geq 5$, we see that $p \notin B(0, 2)$, which means that each set $B = (b_1, \ldots, b_n)$ with $\|b_i\| = \lambda_i = 2$ for all i only spans a sublattice of Λ.

Exercise 4 Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank d.

1. Let $B \in \mathbb{R}^{n \times d}$ be a matrix whose columns are linearly independent vectors in Λ. Show that B is a basis of Λ if and only if the fundamental parallelepiped $\mathcal{P}(B) = \{Bt \mid t \in [0, 1)^d\}$ associated to B does not contain any lattice point apart from 0.

2. Let $p \in \Lambda$ and $p \neq 0$. We call *p primitive* if for each $k \in \mathbb{N}_{\geq 2}$ the vector $\frac{1}{k} p \notin \Lambda$. Show that any primitive vector can be extended to a basis B of Λ.

Solution:

1. For one direction, let B be a basis. By the definition of $\mathcal{P}$ it follows that no nonzero lattice point is contained.

   Now let B be any set of d linear independent lattice vectors s.t. $\mathcal{P}(B)$ does not contain a nonzero lattice point. As the columns of B are linearly independent, any lattice point p can be written as Bt for some $t \in \mathbb{R}^d$. Define the vector t' component wise as $t'_i = t_i - \lfloor t_i \rfloor$ for all i in range. But now Bt' is a lattice point as well, and $Bt' \in \mathcal{P}(B)$, hence $t' = 0$ and t was already integral. Thus B is a basis.

2. *Solution 1:* Write $b_1 = p$, and for vectors $b_1, \ldots, b_k$, define $B_k = (b_1, \ldots, b_k)$ and $\Lambda_k = \Lambda \cap \operatorname{span}\{b_1, \ldots, b_k\}$. We will pick the vectors b_i one by one, providing that B_k is a basis of Λ_k.

   As b_1 is primitive, it is a basis of the lattice $\Lambda \cap \operatorname{span}\{b_1\}$.

   Now assume we already picked $b_1, \ldots, b_{k-1}$ s.t. B_{k-1} is a basis of Λ_{k-1}, we will show how to pick b_k accordingly. Pick any primitive vector $q \in \Lambda$ that is not in the span of B_{k-1} and consider the fundamental parallelepiped $\mathcal{P}_k := \mathcal{P}((B_{k-1}, q))$. If it does not contain any lattice vector other than 0, through the kindness of part 1 we are done by setting $b_k = q$. Otherwise, it contains only finitely many lattice points, hence we can choose a vector $b_k \neq 0$ that is closest to span$\{b_1, \ldots, b_{k-1}\}$. This means, rewriting $b_k = b + b^\perp$ with $b \in$ span$\{b_1, \ldots, b_{k-1}\}$ and $b^\perp \perp$ span$\{b_1, \ldots, b_{k-1}\}$, we want to minimize $\|b^\perp\|$.

We still have to ensure that B_k is a basis of Λ_k. Pick any $v \in \Lambda_k$ with representation $v = B_k t$, $t \in \mathbb{R}^k$. If t_k is integral, the vector $v - t_k b_k$ is in Λ_{k-1} and we are done. Otherwise, the vector $v' = v - B\lfloor t \rfloor = \sum_{i=1}^k (t_i - \lfloor t_i \rfloor) b_i$ is the sum of two lattice vectors, hence contained in Λ. It is also contained in $\mathcal{P}_k$ and has less distance from span$\{b_1, \ldots, b_{k-1}\}$ than v, a contradiction.

Hence, B_d is a basis of $\Lambda_d = \Lambda$.

Solution 2: For this solution we need results on the *Hermite Normal Form.* In particular, for any matrix $A \in \mathbb{Z}^{n \times m}$ of full row rank, there exists a unimodular matrix U of suitable dimension s.t. $AU = [B, 0]$, where B is a lower triangular matrix, and $B_{ii} > B_{ij}$ for all j within range, i.e. in every row, the diagonal entry is the largest entry and unique.

Now let p be as in the exercise, B any basis, and t s.t. $p = Bt$. Let U be the unimodular matrix according to the hermite normal form of t^T, i.e. $t^T U = (\alpha, 0, \ldots, 0)$. It is commonly known that α is the gcd of the entries of t, hence 1 in our case, but not difficult to observe either.

Define $B' = BU^{-T}$ and observe that p is the first basis vector in B' as follows.

$$\alpha B' e_1 = BU^{-T} U^T t = p,$$

implying $\alpha = 1$ as p is primitive. This finishes the proof.

Exercise 5 [$\star$] Prove that John's theorem achieves a better approximation ratio for centrally symmetric convex bodies, i.e. prove the following.

Let $K \subseteq \mathbb{R}^n$ be a centrally symmetric convex body. Show that there is an ellipsoid $\mathcal{E}$ (with the origin as center) s.t. $\mathcal{E} \subseteq K \subseteq C\sqrt{n}\mathcal{E}$ for some (large) constant $C > 0$.

Solution:
We will proceed similar to the proof for the general version, i.e. let K be a centrally symmetric convex body and let w.l.o.g. $B_1(0)$ be the largest ellipsoid contained in K. If $K \subseteq \sqrt{n}CB_1(0)$, we are done. Otherwise let $p \in K \setminus \sqrt{n}CB_1(0)$, i.e. $\|p\| \geq \sqrt{n}C$. By rotating K we may assume $p \in$ span(e_1).

We define an ellipsoid

$$\mathcal{E} = \{x | \sum_{i=1}^n \frac{1}{\alpha_i^2} \langle x, e_i \rangle^2 \leq 1\}$$

with $\alpha_1 = 2$ and $\alpha_i = \sqrt{\frac{10n}{10n+1}}$ for $i = 2, \ldots, n$. Note that, in contrast to the lecture, we do not shift the center of $\mathcal{E}$. We claim that the volume of $\mathcal{E}$ is at least the volume of $B_1(0)$ times a constant factor larger than 1, and that E is contained in K, contradicting the choice of $B_1(0)$ as the largest contained ellipsoid. *In fact, we do not need the fact that $B(0,1)$ was the largest ellipsoid. As K is bounded and we increase by a constant factor, this gives a contradiction by itself after finitely many iterations. Note that the proof in Barvinok's book gives you a better constant in the theorem, but he indeed needs the argument that there is a maximum ellipsoid that can be chosen.*

$\mathcal{E}$ has large volume: Using Bernoulli's inequality $(1+x)^r \geq 1 + rx$ for $r \geq 1$ and $x > -1$, we find

$$\begin{aligned}
\operatorname{vol}(\mathcal{E}) &= \prod_{i=1}^{n} \alpha_i \operatorname{vol}(B_1(0)) \\
&= 2\left(\frac{10n}{10n+1}\right)^{(n-1)/2} \operatorname{vol}(B_1(0)) \\
&= 2\left(1 - \frac{1}{10n+1}\right)^{(n-1)/2} \operatorname{vol}(B_1(0)) \\
&\geq 2\left(1 - \frac{1}{10}\underbrace{\frac{n-1}{2n+1/5}}_{\leq 1}\right) \operatorname{vol}(B_1(0)) \\
&\geq 1.5 \operatorname{vol}(B_1(0)),
\end{aligned}$$

as long as $n \geq 3$. For $n = 1$ the factor is 2 and for $n = 3$ one can easily verify the claim by calculating $2\sqrt{20/21} = \sqrt{3 + 17/21} \geq 1.5$.

$\mathcal{E}$ is contained in K: Similar to the lecture, we will show $\mathcal{E} \subseteq S \subseteq K$, where

$$S = \operatorname{conv}(\{x \mid \|x\| = 1,\ x_1 = 0\} \cup \{p, -p\})$$

is the convex hull of the unit disc orthogonal to p together with $p, -p$. As the disc as well as $p, -p$ are contained in K, we have $S \subseteq K$. Let $q = \lambda x + (1-\lambda)p$ be a vector on the boundary of S, i.e. $\lambda \in [0,1]$ and x with $\|x\| = 1$, $x_1 = 0$. Since S and $\mathcal{E}$ are centrally symmetric, considering $-p$ is similar. We have

$$\begin{aligned}
q^T \begin{pmatrix} \alpha_1^{-2} & & 0 \\ & \ddots & \\ 0 & & \alpha_n^{-2} \end{pmatrix} q &\geq \frac{1}{4}\lambda^2 n C^2 + (1-\lambda)^2 \frac{10n+1}{10} \underbrace{\sum_{i=2}^{n} x_i^2}_{=1} \\
&= \frac{\lambda^2 n C^2}{4} + (1-\lambda)^2 \frac{10n+1}{10}.
\end{aligned}$$

For $(1-\lambda) \geq \sqrt{\frac{10n+1}{10n}}$ the second summand is larger than 1, as the other is non-zero, $q \notin S$.
For $(1-\lambda) < \sqrt{\frac{10n+1}{10n}} \Leftrightarrow \lambda > 1 - \sqrt{\frac{10n+1}{10n}}$, we can choose C large enough. The choice of C is independent of n, as for $m \geq n$, one has $\sqrt{\frac{10m+1}{10m}} \geq \sqrt{\frac{10n+1}{10n}}$.

Thus $\mathcal{E}$ is an ellipsoid in K with volume larger than $B_1(0)$ by a constant factor, contradicting the choice of $B_1(0)$. This finishes the proof.