Convexity

Prof. Friedrich Eisenbrand
Christoph Hunkenschröder

Assignment Sheet 3 - Solutions
October 06, 2016

Exercise 1
Let $\Lambda \subset \mathbb{R}^d$ be a lattice, v a shortest non-zero vector in Λ and $(v, a_2, \ldots, a_d)$ a basis of Λ. Moreover, let pr be the projection map on the subspace of $\mathbb{R}^d$ orthogonal to v, i.e.

$$\begin{aligned} \mathrm{pr} : \mathbb{R}^d &\to \mathbb{R}^d \\ x &\mapsto \left(x - \frac{x^\intercal v}{v^\intercal v} v\right). \end{aligned}$$

Show that $\mathrm{pr}(\Lambda)$ is a $(d-1)$-dimensional lattice with basis $(\mathrm{pr}(a_2), \ldots, \mathrm{pr}(a_d))$, in other words,

$$\mathrm{pr}(\Lambda) = \{\mathrm{pr}(a_2)x_2 + \cdots + \mathrm{pr}(a_d)x_d \mid x_2, \ldots, x_d \in \mathbb{Z}\}.$$

Solution:
First, note that for $x, y, \in \mathbb{R}^d$, $\alpha, \beta \in \mathbb{R}$

$$\mathrm{pr}(\alpha x + \beta y) = (\alpha x + \beta y) - \frac{(\alpha x + \beta y)^\intercal v}{v^\intercal v} v = \alpha\left(x - \frac{x^\intercal v}{v^\intercal v} v\right) + \beta\left(y - \frac{y^\intercal v}{v^\intercal v} v\right) = \alpha\,\mathrm{pr}(x) + \beta\,\mathrm{pr}(y)$$

Moreover, $\mathrm{pr}(\Lambda) \subset Im(\mathbb{R}^d)$, and $\dim(Im(\mathbb{R}^d)) = d - 1$.
Since $\Lambda = \{z_1 v + z_2 a_2 + \cdots + z_d a_d : z_1, \ldots, z_d \in \mathbb{Z}\}$ and $\mathrm{pr}(v) = 0$, we have that

$$\begin{aligned} \mathrm{pr}(\Lambda) &= \{\mathrm{pr}(z_1 v + z_2 a_2 + \cdots + z_d a_d) : z_1 \ldots, z_d \in \mathbb{Z}\} \\ &= \{z_2\,\mathrm{pr}(a_2) + \cdots + z_d\,\mathrm{pr}(a_d) : z_2, \ldots, z_d \in \mathbb{Z}\} \end{aligned}$$

so $\mathrm{pr}(\Lambda)$ is indeed a $(d-1)$-dimensional lattice with base $(pr(a_2), \ldots, pr(a_d))$.

Exercise 2
Let $\Lambda \subset \mathbb{R}^d$ be a lattice and let $\Lambda^\star \subset \mathbb{R}^d$ be its dual lattice. Show that the packing radii of Λ and $\Lambda^\star$ satisfy

$$\rho(\Lambda)\rho(\Lambda^\star) \leq \frac{d}{4}.$$

[Hint:] Use Minkowski's first theorem to bound the $\|\cdot\|_2$-length of a shortest vector.

Solution:
Using Minkowski's theorem, we showed $\lambda_1 \leq \sqrt{d}(\det(\Lambda))^{1/d}$ in the lecture. Thus we know there exist $x \in \Lambda$ with $\|x\| \leq \sqrt{d}(\det\Lambda)^{\frac{1}{d}}$ and $x^\star \in \Lambda^\star$ with $\|x^\star\| \leq \sqrt{d}(\det\Lambda^\star)^{\frac{1}{d}}$. The packing radii are at most $\frac{1}{2}\|x\|$ and $\frac{1}{2}\|x^\star\|$, respectively, hence

$$\rho(\Lambda)\rho(\Lambda^\star) \leq \frac{d}{4}\left(\det(\Lambda)\det(\Lambda^\star)\right)^{\frac{1}{d}}$$

It remains to show that $\det(\Lambda)\det(\Lambda^\star) = 1$. Say $\Lambda = \Lambda(A)$. Then $\Lambda^\star = \Lambda(A^{-\intercal})$, and

$$\det(\Lambda)\det(\Lambda^\star) = \det(A)\det(A^{-\intercal}) = \det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(I) = 1$$

Exercise 3
Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $\Lambda^\star$ its dual. The lattice width of a convex body K w.r.t. Λ is defined as

$$w_\Lambda(K) := \min_{v \in \Lambda^\star \setminus \{0\}} \max_{x,y \in K} v^T (x-y).$$

Let $D \subset \mathbb{R}^d$ be a disc of radius R, i.e. $D = \{x \in \mathbb{R}^d : \|x - r\| \leq R\}$.

1. Show that, for $c \in \mathbb{R}^d$, we have

$$\max_{x \in D} c^\intercal x - \min_{x \in D} c^\intercal x = 2R\|c\|.$$

2. Conclude that $w_\Lambda(D) = 2\lambda_1^\star$, where $\lambda_1^\star$ is the length of a shortest non-zero dual lattice vector.

Solution:
First, note that

$$\max_{x \in D} c^\intercal x - \min_{x \in D} c^\intercal x = \max_{x,y \in D} c^\intercal (x-y) \leq \max_{x,y \in D} \|c\| \, \|x-y\| = 2R\|c\|$$

so we just need to show this bound is attained for some $x, y \in D$. But since $D = r + B_1$ and $\pm\frac{R}{\|c\|} c \in B_1$,

$$\begin{aligned} \max_{x \in D} c^\intercal x - \min_{x \in D} c^\intercal x &= \max_{x \in B_1} c^\intercal (x+r) - \min_{x \in B_1} c^\intercal (x+r) = \max_{x \in B_1} c^\intercal x - \min_{x \in B_1} c^\intercal x \\ &\geq c^\intercal \left(\frac{R}{\|c\|} c \right) - c^\intercal \left(-\frac{R}{\|c\|} c \right) = \frac{2R}{\|c\|} c^\intercal c = 2R\|c\| \end{aligned}$$

which proves the claim.

For the second part, simply observe that a shortest nonzero lattice vector minimizes the term $2R\|v\|$ over $\Lambda^\star$.

Exercise 4 Let $u_1, \ldots, u_d \in \Lambda$ be linearly independet lattice vectors. Prove that

$$\mu(\Lambda) \leq \frac{1}{2} \sum_{i=1}^{d} \|u_i\|.$$

Solution:
First, we observe that the lattice generated by the vectors u_i is a sublattice of Λ. Let U denote the matrix with columns u_i and denote with $\Lambda(U)$ the lattice spanned by U, denote any basis of Λ by B. As $u_i \in \Lambda$, there is an integral matrix A s.t. $U = BA$. For any integral t, the corresponding lattice point $Ut = B(At)$ is in Λ as well, showing $\Lambda(U) \subseteq \Lambda$.

We will show that any $x \in \mathbb{R}^d$ is within $B(p, r)$, where $p \in \Lambda(U)$ and $r = \frac{1}{2} \sum_{i=1}^{d} \|u_i\|$ is the bound above. The claim then follows since $\Lambda(U)$ is a sublattice of Λ.

Let $x \in \mathbb{R}^d$ be arbitrary and define z by $x = Uz$ with $z \in \mathbb{R}^d$, i.e. $z = U^{-1}x$. Denote with $y = \lfloor z \rceil$ the vector x componentwise rounded to the closest integer, and set $p = Uy$. Now

$$\|x - p\|_2 = \|U(z - \lfloor z \rceil)\|_2 \leq \sum_{i=1}^{d} \frac{1}{2} \|b_i\|$$

by linearity of the norm and triangle inequality. There is nothing left to prove.

Exercise 5 [⋆] Let $\Lambda \subset \mathbb{R}^d$ be a lattice and let $x \in \mathbb{R}^d$ be a point. Prove that for every $v \in \Lambda^\star \setminus \{0\}$

$$\frac{\{\langle v, x\rangle\}}{\|v\|} \leq \mathrm{dist}(x, \Lambda),$$

where $\{r\} := |\lceil r \rfloor - r|$ is defined to be the distance from $r \in \mathbb{R}$ to the closest integer.

Solution:
Let B be a basis of Λ. Moreover, let $x \in \mathbb{R}^d$ be some point and $v \in \Lambda^\star \setminus \{0\}$ some dual lattice vector. Let $\alpha = v^T x$. We know that for any lattice point $p \in \Lambda$, we have $v^T p \in \mathbb{Z}$ by definition of the dual lattice. This implies

$$\mathrm{dist}(x, \Lambda) \geq \min\left\{\mathrm{dist}(x, \{y :\ v^T y = \lfloor \alpha \rfloor\}),\ \mathrm{dist}(x, \{y :\ v^T y = \lceil \alpha \rceil\})\right\}.$$

W.l.o.g. let the minimum be attained for $\lfloor \alpha \rfloor$ and let us calculate $\mathrm{dist}(x, \{y :\ v^T y = \lfloor \alpha \rfloor\})$. Observe that $x - (\alpha - \lfloor \alpha \rfloor)\frac{v}{\|v\|^2}$ is the projection of x onto the hyperplane $\{y :\ v^T y = \lfloor \alpha \rfloor\}$. Hence,

$$\begin{aligned}
\mathrm{dist}(x, \{y :\ v^T y = \lfloor \alpha \rfloor\}) &= \|x - (x - (\alpha - \lfloor \alpha \rfloor)\frac{v}{\|v\|^2})\| \\
&= \|(\alpha - \lfloor \alpha \rfloor)\frac{v}{\|v\|^2}\| \\
&= \frac{\{\langle v, x\rangle\}}{\|v\|}
\end{aligned}$$

finishes the proof.

Exercise 6 Let $\theta_1, \ldots, \theta_n$ be real numbers such that $m_1\theta_1 + \cdots + m_n\theta_n + m_{n+1} = 0$ for integers $m_1, \ldots, m_{n+1}$ implies $m_1 = \cdots = m_{n+1} = 0$. Denote the distance from some real r to the closest integer by $\{r\} := |\lceil r \rfloor - r|$. Prove Kronecker's Theorem:

For any real vector $a = (\alpha_1, \ldots, \alpha_n)$ and for any $\epsilon > 0$ there exists a positive integer m such that $\{\alpha_i - m\theta_i\} < \epsilon$ for $i = 1, \ldots, n$.

[Hint:] Let $d = n + 1$ and let $\tau > 0$ be a number. Consider the set $\Lambda_\tau \subseteq \mathbb{R}^d$ of all integer linear combinations of the vectors $u_i = (e_i^T, 0)^T$, $i = 1, \ldots, n$ and $u_{n+1} = (\theta_1, \ldots, \theta_n, \tau^{-1})$. Convince yourself that Λ_τ is indeed a lattice and that the packing radius of the dual lattice grows to infinity when τ grows. Deduce that the covering radius of Λ_τ tends to 0 as τ grows. Conclude the theorem.

[Hint 2:] In order to show that the packing radius of the dual lattice grows to infinity, you can for example take a shortest non-zero vector $v \in \Lambda_\tau^\star$ and show that there exists τ' such that $\|w\| \geq 2\|v\|$ for all $w \in \Lambda_{\tau'}^\star \setminus \{0\}$.

Solution:
First, we will follow the first hint. As $u_1, \ldots, u_n$ are given as the canonic unit vectors and only u_{n+1} has a nonzero entry in the last component, they are linearly independent and thus form a basis by our definition.

Let us write down our basis matrix and the corresponding dual, called D (Hence, D^T is the inverse of B).

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 & \theta_1 \\ 0 & 1 & & & \theta_2 \\ & & \ddots & & \\ 0 & & \cdots & 0 & \tau^{-1} \end{pmatrix}, \qquad D = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & & 0 \\ & & & \ddots & 0 \\ -\tau\theta_1 & -\tau\theta_2 & \cdots & -\tau\theta_n & \tau \end{pmatrix}$$

(One can deduce the inverse matrix by looking at BD^T and deducing row by row, starting with the last one.)
Now fix some τ and rewrite any nonzero vector $v \in \Lambda_\tau^\star$ as

$$v = Dt = \underbrace{\sum_{i=1}^{n} t_i e_i}_{=:u(v)} + \tau \underbrace{\left(t_{n+1} + \sum_{i=1}^{n} t_i \theta_i \right)}_{=:R(v)} e_{n+1}$$

in order to define $u(v)$ and $R(v)$. First note that

$$\|v\|^2 = \|u(v)\|^2 + \tau^2 R(v)^2 \qquad \Rightarrow \qquad \|v\| \geq \begin{cases} \|u(v)\|, \\ \tau |R(v)| \end{cases} . \tag{1}$$

Moreover, if $R(v)$ was 0, by the structure of the θ_i the whole vector would be the zero vector. Fix v to be a shortest nonzero vector of $\Lambda_\tau^\star$ and define

$$\hat{R}(v) := \min \left\{ \left| t_{n+1} + \sum_{i=1}^{n} t_i \theta_i \right| \ : \ t \in \mathbb{Z}^{n+1}, \ \|t\| \leq 2\|v\| \right\}.$$

As t is integral and bounded by the norm of v (which is the same for any shortest nonzero vector), this is well defined. Now set

$$\tau' = \max \left\{ \tau, \ \frac{2\|v\|}{\hat{R}(v)} \right\}$$

and observe a shortest nonzero vector v' in $\Lambda_{\tau'}^\star$.

$$v' = Dt' = \underbrace{\sum_{i=1}^{n} t'_i e_i}_{=:u(v')} + \tau' \underbrace{\left(t'_{n+1} + \sum_{i=1}^{n} t'_i \theta_i \right)}_{=:R(v')} e_{n+1}.$$

There are two possibilities. If $|R(v')| \geq \hat{R}(v)$, we have $\tau' R(v') \geq 2\|v\|$ and using (1) shows that $\|v'\| \geq 2\|v\|$.

On the other hand, if $R(v') \leq \hat{R}(v)$, this means that the t'_i are too large, i.e. $\|u(v')\| \geq 2\|v\|$.

Hence, the packing radius of $\Lambda_\tau^\star$ grows to infinity. This implies, using the transference bound

$$\frac{1}{4} \leq \mu(\Lambda) \cdot \rho(\lambda^\star) \leq c(n)$$

seen in class, that the covering radius tends to 0. But then for τ large enough, any point $(\alpha_1, \ldots, \alpha_n, 0)$ has a close lattice point, i.e. for any ϵ there exists Bt, $t \in \mathbb{Z}^{n+1}$, with

$$\left\| \begin{pmatrix} \alpha_1 - t_1 + \theta_1 t_{n+1} \\ \alpha_2 - t_2 + \theta_2 t_{n+1} \\ \vdots \\ \alpha_n - t_n + \theta_n t_{n+1} \\ 0 - \tau^{-1} t_{n+1} \end{pmatrix} \right\| \leq \epsilon.$$

This implies that any entry is already smaller than ϵ, choosing $m = t_{n+1}$ finishes the proof.