# Integer Optimization
# Problem Set 8

Presentations: May 8

i) Let $\Lambda \subseteq \mathbb{R}^n$ a full rank lattice with basis $b_1, \ldots, b_n$. A non-zero lattice vector $v$ is said to be primitive if $v$ is not a multiple of any other lattice vector, i.e. $v \neq kw$ for any $w \in \Lambda$ and any $k \in \mathbb{N}_{\geq 2}$. Show that any primitive lattice vector $v$ can be extended to a basis of $\Lambda$, i.e. there are lattice vectors $\tilde{b_2}, \ldots, \tilde{b_n}$ so that $v, \tilde{b_2}, \ldots, \tilde{b_n}$ is a basis of $\Lambda$.

*Hint: This is a question about unimodular matrices. Write $v = \alpha_1 b_1 + \ldots + \alpha_n b_n$. Using the Euclidean algorithm, show that there exists a unimodular matrix $U \in \mathbb{Z}^{n\times n}$ such that $(\alpha_1,$ ůůů$, \alpha_n) \cdot U = (1, 0, \ldots, 0)$. Observe each operation of the Euclidean algorithm only adds / subtracts multiples of some number to / from another number - in the matrix world, this operations corresponds to a unimodular matrix. It may be useful to show that gcd$(\alpha_1, \ldots, \alpha_n) = 1$. Finally, argue that the columns of the matrix $(b_1, b_2, \ldots, b_n) \cdot U^{-T}$ form a basis of $\Lambda$ and its first column is v.*

ii) Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $v \in \Lambda \setminus \{0\}$ be a shortest vector w.r.t. the $\ell_2$-norm. For $x \in \mathbb{R}^n$ we let

$$\pi(x) = x - (x^T v / v^T v)\, v$$

be the projection of $x$ and we define $\Lambda_1 = \pi(\Lambda)$ as well as $\Lambda_1^* = \{y \in \mathbb{R}^n : y \perp v, \forall x \in \Lambda_1 : y^T x \in \mathbb{Z}\}$.

Prove or provide a counterexample to the following:

$$\Lambda_1^* = \pi(\Lambda^*).$$

*This is Edwin's question!*

iii) Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. Assume $b_1, \ldots, b_n \in \Lambda$ are linearly independent and that minimize $|det(b_1, \ldots, b_n)|$ over all n linearly independent lattice vectors. Prove that $b_1, \ldots, b_n$ is a basis of $\Lambda$.

iv) Let $B \in \mathbb{Q}^{n\times n}$ be a lattice basis that consists of pairwise orthogonal vectors. Prove that the shortest vector of $\Lambda(B)$ is the shortest column vector of B.

v) Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Recall that the dual lattice $\Lambda^*$ is defined by $\Lambda^* = \{y \in \mathbb{R}^n : y^T v \in \mathbb{Z} \quad \forall v \in \Lambda\}$.
Let $x \in \mathbb{R}^d$ a vector. Prove that for every $v \in \Lambda^* \setminus \{0\}$ we have that

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

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