Integer Optimization
Problem Set 8

Presentations: May 8

Exercise 1

Let $\Lambda \subseteq \mathbb{R}^n$ a full rank lattice with basis $b_1, ..., b_n$. 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 Λ, i.e. there are lattice vectors $\tilde{b_2}, ..., \tilde{b_n}$ so that $v, \tilde{b_2}, ..., \tilde{b_n}$ is a basis of Λ.
Hint: This is a question about unimodular matrices. Write $v = \alpha_1 b_1 + ... + \alpha_n b_n$. Using the Euclidean algorithm, show that there exists a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ such that $(\alpha_1, , \alpha_n) \cdot U = (1, 0, ..., 0)$. 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 $gcd(\alpha_1, ..., \alpha_n) = 1$. Finally, argue that the columns of the matrix $(b_1, b_2, ..., b_n) \cdot U^{-T}$ form a basis of Λ and its first column is v.

Exercise 2

A set $\Lambda \subseteq \mathbb{R}^d$ is an additive subgroup if

1. $0 \in \Lambda$
2. $x + y \in \Lambda$ for any two $x, y \in \Lambda$
3. $-x \in \Lambda$ for any $x \in \Lambda$

Furthermore, Λ is called discrete provided there is some $\epsilon > 0$ so that the euclidean ball with radius ϵ centered at 0 does not contain any point of Λ except 0, i.e. $B(0, \epsilon) \cap \Lambda = 0$. Show that a discrete additive subgroup of $\mathbb{R}^2$ is a lattice (possesses a basis).
Hint: pick a vector $v \in \Lambda$ that is not a multiple of another element (why does this exist?) and some other vector w that is closest to the span of v (why is there a closest?)

Exercise 3

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

Exercise 4

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.

Exercise 5

Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Recall that the dual lattice Λ^* 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 $v \in \Lambda^* \backslash \{0\}$ 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.