Edoardo Persichetti Lecture 10: Lattices 30/04/2014

Exercise 1 Kernel Lattice

1. Given an $m \times n$ integer matrix A show that $ker(A) = \{\underline{x} \in \mathbb{Z}^m : \underline{x}A = 0\}$ is a lattice. Show that the rank of the lattice is $m - rank(A)$.
2. Given an $m \times n$ integer matrix A and an integer M show that $\{\underline{x} \in \mathbb{Z}^m : \underline{x}A \equiv 0 \pmod{M}\}$ is a lattice of rank m.

Exercise 2 . Let $\{\underline{b}_1, \dots \underline{b}_n\}$ be a basis for a lattice L. Show that the the orthogonality defect of $\{\underline{b}_1, \dots \underline{b}_n\}$ is 1 if and only if the basis is orthogonal.

Definition 1 Let $L \subset \mathbb{R}^m$ be a lattice of rank n. The *successive minima* of L are $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ such that, for $1 \leq i \leq n$, λ_i is the minimal value such that there exist i linearly independent vectors $\underline{v}_1, \dots \underline{v}_n \in L$ with $||\underline{v}_j|| \leq \lambda_i$ for all $1 \leq j \leq i$.

It follows that $0 < \lambda_1 \leq \lambda_2 \cdots \leq \lambda_n$. *Note also that* λ_1 *is the length of the shortest vector in* L.

Exercise 3 Let $L \subset \mathbb{Z}^n$ be the set $L = \{(x_1, \dots, x_n) : x_1 \equiv x_2 \equiv \cdots \equiv x_n \pmod{2}\}$.

1. Show that L is a lattice.
2. For $n = 2, 3, 4$ find the values of the successive minima, then write down a basis whose vectors have length equal to the values of the successive minima.
3. What happens when $n > 4$?

Exercise 4 Dual Lattices

1. Let $L \subseteq \mathbb{R}^m$ be a lattice and let $V \subseteq \mathbb{R}^m$ be the $\mathbb{R}$-vector space spanned by the vectors in L. Show that the dual lattice $L^\perp = \{\underline{y} \in V : \langle \underline{x}, \underline{y} \rangle \in \mathbb{Z} \text{ for all } \underline{x} \in L\}$ is a lattice.
2. Let B be a basis matrix of a full rank lattice L. Show that $(B^T)^{-1}$ is a basis matrix for the dual lattice. Hence, show that the determinant of the dual lattice is $det(L)^{-1}$.

Exercise 5 Let $L \subset \mathbb{R}^2$ be the lattice with basis $\underline{b}_1 = (137, 312)$ and $\underline{b}_2 = (215, -187)$ and let $\underline{w} = (53172, 81743)$.

1. Use Babai's method with the above basis to find the closest lattice vector to $\underline{w}$.
2. Repeat the procedure using the alternative basis given by $\underline{b}'_1 = (1975, 438) = 5\underline{b}_1 + 6\underline{b}_2$ and $\underline{b}'_2 = (7548, 1627) = 19\underline{b}_1 + 23\underline{b}_2$.
3. Calculate and compare the Hadamard Ratio of the two bases to justify your results.