CS6190: Lattices in Computer Science August 21, 2017

Homework 1

Instructors: Shweta Agrawal and Satya Lokam *Due: September 01, 2017*

Problem 1: Lattices with Integer and Rational generators

We saw in class that an arbitrary finite set of numbers in $\mathbb{R}^1$ doesn't necessarily generate a lattice in $\mathbb{R}^1$, e.g., when that set contains irrational numbers.

a. Clearly an arbitrary finite set of *integers* generates a lattice in $\mathbb{R}^1$. Given a set $B = \{b_1, \ldots, b_m\}$ with $b_i \in \mathbb{Z}$, what is $\lambda_1(\mathcal{L}(B))$? Recall that $\lambda_1(\mathcal{L}(B))$ is the "length" of the shortest nonzero "vector" in the lattice $\mathcal{L}(B) \subset \mathbb{R}^1$ generated by B.

b. Now, let $B = \{b_1, \ldots, b_m\}$ with $b_i \in \mathbb{Z}^n$ be an arbitrary finite set of integer vectors in $\mathbb{R}^n$. Give a lower bound on $\lambda_1(\mathcal{L}(B))$.

c. Show that an arbitrary finite set of *rational* vectors in $\mathbb{R}^n$ must define a lattice.

Problem 2: Successive Minima and Bases

Here's a lattice for which the linearly independent vectors achieving successive minima don't form a basis of the lattice.
Consider the lattice $\mathcal{L} \subseteq \mathbb{R}^n$ of integer vectors all of whose coordinates have the same parity, i.e., either all coordinates are even numbers or all coordinates are odd numbers.

a. Compute the n successive minima $\lambda_i(\mathcal{L})$ and a corresponding set of linearly independent vectors $v_i \in \mathcal{L}$ such that $\|v\| = \lambda_i(\mathcal{L})$.

b. On the other hand, show that any basis of $\mathcal{L}$ must contain a vector of length at least $\sqrt{n}$.

Problem 3: Orthogonal Sublattices

Although not every lattice has an orthogonal basis, this exercise shows that every *integer* lattice contains an orthogonal sublattice.
Let $B \in \mathbb{Z}^{n \times n}$ be a nonsingular integer matrix with $\Delta := \det(\mathcal{L}(B))$. Show that $\Delta \cdot \mathbb{Z}^n \subseteq \mathcal{L}(B)$. That is, the lattice of integer vectors each of whose coordinates is a multiple of Δ is a sublattice of $\mathcal{L}(B)$. You may use Cramer's rule to prove this.

Problem 4: LLL-reduced bases

Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ with an LLL (δ-LLL with $\delta = 3/4$) reduced basis $b_1, \ldots, b_n$. Prove the following.

a. $\|b_1\| \leq 2^{(n-1)/4} (\det \mathcal{L})^{1/n}$.

b. $\prod_{i=1}^{n} \|b_i\| \leq 2^{n(n-1)/4} \det \mathcal{L}$.