CSC 2414 Lattices in Computer Science *Instructor: Vinod Vaikuntanathan*

Problem Set 1

Handed Out: September 13, 2011 *Due: October 3, 2011*

Notes

- This problem set is worth 100 points.
- Collaboration is allowed, *but you must write up the solutions by yourself without consulting to notes from the discussions.* You must also reference your sources.
- Grading is based on correctness as well as the clarity of the solutions. When writing proofs, it is generally a good idea to first explain the intuition behind your solution in words (wherever appropriate), before jumping in to the formalisms.
- *Notation:* $\mathbb{N}$ denotes the natural numbers, $\mathbb{Z}$ denotes the integers, $\mathbb{Q}$ denotes rational numbers and $\mathbb{R}$ the set of real numbers.

Problem 1: Fun with Lattice Bases (25 points)

Consider the basis

$$\mathbf{B} = \begin{pmatrix} 123 & 1 \\ 6764 & 55 \end{pmatrix}$$

- (5 points) Which of the following vectors belong to the lattice $\mathcal{L}(\mathbf{B})$?

$$\mathbf{v}_1 = \begin{pmatrix} 129 \\ 143 \end{pmatrix} \qquad \mathbf{v}_2 = \begin{pmatrix} 1/2 \\ 10 \end{pmatrix} \qquad \mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

  Briefly justify your answers. (A simple yes/no does not suffice).

- (5 points) What is the determinant of $\mathcal{L}(\mathbf{B})$?
- (5 points) Find the Gram-Schmidt orthogonalization of $\mathbf{B}$. Show your calculations.
- (5 points) Find a shortest vector in $\mathcal{L}(\mathbf{B})$ (note that there may be many).
- (5 points) Find a shortest basis of $\mathcal{L}(\mathbf{B})$ (note that there may be many).

Problem 2: More Bases and Determinants (25 points)

- (15 points) Prove that for every $n \in \mathbb{N}$, there is a unique full-rank integer lattice $\mathcal{L} = \mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$ with determinant 1. [*Hint: Show that* $\mathcal{L}(\mathbf{B}) = \mathbb{Z}^n$.]
- (10 points) For any full-rank integer lattice $\mathcal{L} = \mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$, show that the vector $(\det(\mathcal{L}), 0, 0, \ldots, 0)^T$ is in the lattice.

Problem 3: Minkowski's Convex Body Theorem (25 points)

Let $\mathcal{L}$ be a lattice. Recall that Minkowski's Convex Body Theorem states that any *convex*, *centrally symmetric* n-dimensional body S with $\mathsf{vol}(S) > 2^n \det(\mathcal{L})$ contains a *non-zero* lattice point.

Show that all the three conditions – convexity, central symmetry and the lower-bound on the volume – are necessary for this theorem to be true. Namely, for the lattice $\mathcal{L} = \mathbb{Z}^n$, show:

- (10 points) a convex set S_1 with $\mathsf{vol}(S_1) > 2^n \cdot \det(\mathcal{L})$ that does not contain a lattice point. Note that S_1 has to be necessarily *centrally asymmetric.*
- (10 points) a centrally symmetric set S_2 with $\mathsf{vol}(S_2) > 2^n \cdot \det(\mathcal{L})$ that does not contain a lattice point. Note that S_2 has to be necessarily *non-convex.*
- (5 points) a convex, centrally symmetric set S_3 with $\mathsf{vol}(S_3) = 2^n \cdot \det(\mathcal{L})$ that does not contain a non-zero lattice point.

The elegance of your solution counts.

Problem 4: Minkowski's First Theorem (25 points)

- (20 points) Find the analog of Minkowski's first theorem for the ℓ_1 and ℓ_∞ norms.

  [*Hint: Which part of the proof of Minkowski's first theorem is specific to the ℓ_2 norm?*]

- (5 points) Show a lattice in n dimensions for which the shortest vector is much *smaller* than what Minkowski's theorem predicts. In particular, show an n-dimensional (full-rank) lattice $\mathcal{L}$ with determinant 1 such that

$$\lambda_1(\mathcal{L}) < 10^{-100}$$

Extra Credit**

Despite lattices with much shorter vectors than predicted, Minkowski's theorem is tight for general lattices. In particular, there is a family of lattices $\{\mathcal{L}_n\}_{n\in\mathbb{N}}$ where $\mathcal{L}_n$ lives in n dimensions, and

$$\lambda_1(\mathcal{L}_n) \geq c \cdot \sqrt{n} \cdot \det(\mathcal{L}_n)^{1/n}$$

where c is a universal constant independent of n.

Show that such a family of lattices exists (your proof doesn't have to construct this family, you merely have to show existence).