CSE 206A: Lattices Algorithms and Applications (Fall 2017)

Problem Set 2

Lecturer: Daniele Micciancio **Due:** *Thu October 19, 2017*

1 Extremal Lattices

Let $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice achieving Hermite constant

$$\gamma_n = \left(\frac{\lambda(\Lambda)}{\det(\Lambda)^{1/n}}\right)^2.$$

Prove that Λ has n linearly independent vectors of length $\lambda(\Lambda)$, i.e.,

$$\lambda_1(\Lambda) = \lambda_2(\Lambda) = \ldots = \lambda_n(\Lambda).$$

[Hint: Use Minkowski's second theorem.]

2 L1 Norm

Derive an upper bound on the ℓ_1 minimum distance of a full-dimensional lattice (as a function of the determinant) from Minkowski's convex body theorem, similarly to what we did in class for the ℓ_∞ and ℓ_2 norms. Give special cases of your bound in dimension 1, 2 and 3, as well as a general formula for dimension n.

3 Covering Radius

The covering radius of a lattice Λ is the *smallest* radius ρ such that spheres of radius ρ centered around all lattice points cover the entire linear span of the lattice, i.e., $\text{span}(\Lambda) \subset \bigcup \{\mathcal{B}(\vec{x}, r) \mid \vec{x} \in \Lambda\}$. Alternatively, the covering radius can be defined as the *maximum* distance of any point $\vec{t} \in \text{span}(\Lambda)$ to the lattice Λ, i.e., $\rho = \sup \{dist(\vec{x}, \Lambda) \mid \vec{x} \in \text{span}(\Lambda)\}$

1. Determine the minimum distance λ and the covering radius ρ of the integer lattice $\mathbb{Z}^n$, for arbitrary n
2. Prove that if $\Lambda = \mathcal{L}(\mathbf{B})$, then $\rho(\Lambda) \leq \frac{1}{2}\sqrt{\sum_i \|\vec{b}_i^*\|^2}$, where $\vec{b}_i^*$ are the Gram-Schmidt orthogonalized basis vectors.
3. Find a lattice basis $\mathbf{B}$ (for a full rank lattice in arbitrary dimension n) such that $\rho(\Lambda) = \frac{1}{2}\sqrt{\sum_i \|\vec{b}_i^*\|^2}$ holds with equality.