Lecturer: Thomas Rothvoss Due date: Friday, Jan 27, 2023, 11pm, on GradeScope

Problem Set 3

CSE 599S - Lattices

Winter 2023

Exercise 1.5 (10pts)
Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. Show that $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geq 1$, where Λ^* is the dual lattice.

Exercise 1.6 (10pts)
Prove that for any lattice $\Lambda \subseteq \mathbb{R}^n$, one has $\lambda_1(\Lambda) \cdot \lambda_1(\Lambda^*) \leq n$.
Remark 1: You will need a fact that we will see in the Monday, Jan 23 lecture.
Remark 2: A stronger theorem of Banaszczyk that we will see in Chapter 4 shows that even $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \leq n$. This has an important consequence. Consider the following computational problem: Given a lattice Λ and a parameter K, distinguish the cases $\lambda_1(\Lambda) \leq L$ and $\lambda_1(\Lambda) > n \cdot L$. The consequence of this exercise is that this problem is in **NP**$\cap$**coNP** in the sense that one can give an efficiently checkable proof for $\lambda_1(\Lambda) \leq L$ (simply give me a short vector) and one can also certify is $\lambda_1(\Lambda) > n \cdot L$ (give me the short dual basis). The remarkable fact is that this gap problem is not known to be in **P**.

Exercise 1.12 (10pts)
Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and let $\boldsymbol{B} \in \mathbb{R}^{n \times n}$ be an LLL-reduced basis for Λ. Prove that for all $i \in \{1, \dots, n\}$ one has $\|\boldsymbol{b}_i\|_2 \leq 2^{(n+1)/2} \lambda_i(\Lambda)$.
Hint. You may use following observation: Consider an LLL-reduced $\boldsymbol{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ and for some index $i \in \{1, \dots, n\}$, define the subspace $U := \mathrm{span}\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_{i-1}\}$ and let $\tilde{\boldsymbol{b}}_j := \Pi_{U^\perp}(\boldsymbol{b}_j)$ where $\Pi_{U^\perp}$ denotes the projection into the subspace $U^\perp$. Then $\tilde{\boldsymbol{b}}_i, \dots, \tilde{\boldsymbol{b}}_n$ is an LLL-reduced basis for the lattice $\tilde{\Lambda} := \{\sum_{j=i}^n y_j \tilde{\boldsymbol{b}}_j : y_j \in \mathbb{Z}\}$.