Lecturer: Thomas Rothvoss Due date: Friday, Feb 10, 2023, 11pm, on GradeScope

Problem Set 5

CSE 599S - Lattices

Winter 2023

Exercise 2.1 (20pts)
Let $\Lambda \subseteq \mathbb{R}^n$ be a full-rank lattice with LLL-reduced basis $\boldsymbol{B} \in \mathbb{R}^{n\times n}$ and Gram Schmidt orthogonalization $\boldsymbol{b}_1^*, \dots, \boldsymbol{b}_n^*$. We abbreviate $\mu_{i,j} = \frac{\langle \boldsymbol{b}_j, \boldsymbol{b}_i^* \rangle}{\|\boldsymbol{b}_i^*\|_2^2}$. First, we fix an arbitrary $\boldsymbol{x} = \boldsymbol{B}\boldsymbol{y}$ with $\boldsymbol{y} \in \mathbb{R}^n$.

(i) Prove that $\|\boldsymbol{x}\|_2^2 = \sum_{k=1}^n \|\boldsymbol{b}_k^*\|_2^2 \cdot \left(y_k + \sum_{j>k} \mu_{k,j} y_j\right)^2$

(ii) Prove that for all $k \in \{1, \dots, n\}$ one has $\|\boldsymbol{x}\|_2^2 \geq 2^{-k}\|\boldsymbol{b}_k\|_2^2 \cdot \max\{|y_k| - \frac{1}{2}\sum_{j>k}|y_j|, 0\}^2$.

Now fix a $\boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}$ with $\|\boldsymbol{x}\|_2 = \lambda_1(\Lambda)$ and let $\boldsymbol{y} \in \mathbb{Z}^n$ be so that $\boldsymbol{x} = \boldsymbol{B}\boldsymbol{y}$.

(iii) Prove that for all $k \in \{1, \dots, n\}$ one has $|y_k| \leq \max\{2^{(k+2)/2}, \sum_{j>k}|y_j|\}$.

(iv) Prove that for all $k \in \{1, \dots, n\}$ one has $|y_k| \leq 2^{3n-k}$.

Remark. This exercise proves that all shortest vectors in a lattice $\Lambda \subseteq \mathbb{R}^n$ are contained in the set $S = \{\boldsymbol{B}\boldsymbol{y} \mid \boldsymbol{y} \in \mathbb{Z}^n \text{ and } \|\boldsymbol{y}\|_\infty \leq 2^{3n}\}$ if $\boldsymbol{B}$ is an LLL-reduced basis.