Convexity

Prof. Friedrich Eisenbrand
Christoph Hunkenschröder

Assignment Sheet 8

November 24, 2016

Exercise 1
Let b_1, b_2 be an LLL-reduced basis of a lattice $\Lambda \subseteq \mathbb{R}^2$. Show that a shortest vector of Λ is among b_1, b_2.

Exercise 2 [$\star$]
Let $B = (b_1, \ldots, b_n) \in \mathbb{Q}^{n \times n}$ be an LLL-reduced basis of a lattice $\Lambda \subseteq \mathbb{Q}^n$. Let $x = a_1 b_1 + \cdots + a_n b_n$ be a shortest vector of Λ.

1. Show that $|a_j| \leq 2^{O(n)}$.
2. Show that a shortest vector can be computed in time $2^{O(n^2)}$.

[*Hint: For part 1., is there a certain index for which you you can show the claim easily? Can you go on from there?*]

Exercise 3
In the LLL-algorithm, we swapped two vectors b_j, b_{j+1} in our basis whenever we had

$$\left\| b^\star_{j\ new} \right\|^2 < \delta \left\| b^\star_j \right\|^2$$

for $\delta = \frac{3}{4}$. The first vector of the output basis was an approximation to a shortest vector.

1. How does the running time change when we change δ? How does the approximation guarantee change?
2. Show that the algorithm still terminates when we choose $\delta = 1$. Is the running time still polynomial?

The deadline for submitting solutions is **Thursday, December 1, 2016**.