Convexity

Prof. Friedrich Eisenbrand
Christoph Hunkenschröder

Assignment Sheet 8 - Solutions

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.

Solution:

Let $v = a_1 b_1 + a_2 b_2$ be a shortest vector. If $a_1 = 0$ or $a_2 = 0$, we are done, hence assume $|a_1|, |a_2| \geq 1$. Using $\left\|b_2^\star\right\|^2 \geq 1/2 \left\|b_1\right\|^2$, we calculate

$$\begin{aligned}\|v\|^2 &= \left\|a_1 b_1 + (a_2 b_2^\star + a_2 \mu_{12} b_1)\right\|^2 \\ &= (a_1 + a_2\mu_{12})^2 \left\|b_1\right\|^2 + a_2^2 \left\|b_2^\star\right\|^2 \\ &\geq \left((a_1 + a_2\mu_{12})^2 + \frac{a_2^2}{2}\right) \left\|b_1\right\|^2,\end{aligned}$$

showing that $|a_2| = 1$ holds. But then

$$\begin{aligned}\|v\|^2 &= (a_1 + a_2\mu_{12})^2 \left\|b_1\right\|^2 + \left\|b_2^\star\right\|^2 \\ &\geq \frac{1}{4} \left\|b_1\right\|^2 + \left\|b_2^\star\right\|^2 \\ &\geq \mu_{12}^2 \left\|b_1\right\|^2 + \left\|b_2^\star\right\|^2 \\ &= \left\|b_2^\star + \mu_{12} b_1\right\|^2 \\ &= \left\|b_2\right\|^2\end{aligned}$$

finishes the proof.

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?*]

Solution:

1. We will proceed by reverse induction. Let $v = a_1 b_1 + \cdots + a_n b_n$ be a shortest vector. As $b_n^\star$ is orthogonal to $b_1, \ldots, b_{n-1}$, we have

$$\begin{aligned} \|b_1\|^2 &\geq \|v\|^2 \\ &= a_n^2 \left\|b_n^\star\right\|^2 + \left\| a_1 b_1 + \cdots + a_{n-1} b_{n-1} + a_n \sum_{i=1}^{n-1} \mu_{i,n} b_i^\star \right\|^2 \\ &\geq a_n^2 \left\|b_n^\star\right\|^2 \\ &\geq a_n^2 2^{-(n-1)} \|b_1\|^2 , \end{aligned}$$

implying $a_n \leq 2^{(n-1)/2}$. Now assume we proved

$$|a_j| \leq 2^{\frac{n-1}{2} + (n-j)} =: f(j)$$

for all $j > k$. We have

$$\begin{aligned} \|b_1\|^2 &\geq \|v\|^2 \\ &\geq (a_k + \sum_{j=k+1}^{n} \mu_{k,j} a_j)^2 \left\|b_k^\star\right\|^2 \\ &\geq (a_k + \sum_{j=k+1}^{n} \mu_{k,j} a_j)^2 \left(\frac{1}{2}\right)^{k-1} \|b_1\| , \end{aligned}$$

leading to

$$\begin{aligned} 2^{\frac{k-1}{2}} &\geq \left| a_k + \sum_{j=k+1}^{n} \mu_{k,j} a_j \right| \\ \Rightarrow |a_k| &\leq 2^{\frac{k-1}{2}} + \frac{1}{2} \sum_{j=k+1}^{n} |a_j| \\ &\leq 2^{\frac{k-1}{2}} + \frac{1}{2} \sum_{j=k+1}^{n} 2^{\frac{n-1}{2} + (n-j)} \\ &\leq 2^{\frac{k-1}{2}} + 2^{\frac{n-1}{2}} \frac{1}{2} \sum_{j=0}^{n-k-1} 2^j \\ &\leq 2^{\frac{k-1}{2}} + 2^{\frac{n-1}{2} + n-k-1} \\ &\leq 2^{\frac{n-1}{2} + (n-k)} . \end{aligned}$$

2. For the second part, simply try all combinatios of integers $-f(j) \leq a_j \leq f(j)$ and remember the combination a that minimizes the length so far (except $a \equiv 0$). This gives roughly $(2^{1.5n})^n$ possibilities, hence a $2^{O(n^2)}$-time algorithm, as calculating the length of a certain vector Ba works in time at most $O(n^2) \subseteq 2^{O(n^2)}$.

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?

Solution:

1. We will have a closer look on the potential function of the lecture,

$$\Phi(B) = \prod_{i=1}^{n} \prod_{j=1}^{i} \left\|b^\star_j\right\|^2.$$

We saw that the potential function is integral (assuming our initial basis B is integral, which we can achieve by scaling). Moreover, if B' denotes the basis B after a swap $j \leftrightarrow j+1$, we have the following relation.

$$\Phi(B') = \frac{\left\|b^\star_{j\ new}\right\|^2}{\left\|b^\star_j\right\|^2} \Phi(B) < \delta \Phi(B). \tag{1}$$

Hence, at every swap the potential drops by a constant factor smaller than δ. Of course, if $\delta > 1$, this means that the potential is not decreasing any more. Moreover, this would imply that we want our Gram-Schmidt vectors to *grow* for increasing index, in a certain sense. Hence, it makes sense to restrict to the case $\delta \leq 1$.

Let M denote our initial potential; as our initial basis is integral, we have $\left\|b^\star_i\right\|^2 \leq \|b_i\|^2 \leq n\,\|B\|^2_\infty$, yielding $M \in (n\,\|B\|^2_\infty)^{O(n^2)}$. Considering the potential after k iterations and having in mind that the potential cannot drop below 1, we get (assuming $\delta < 1$)

$$\begin{aligned} &1 \leq \delta^k (n\,\|B\|^2_\infty)^{O(n^2)} \\ \Leftrightarrow\ &0 \leq k \log \delta + O(n^2) \log(n\,\|B\|^2_\infty) \\ \Leftrightarrow\ &k \leq \frac{O(n^2) \log(n\,\|B\|^2_\infty)}{\log 1/\delta}. \end{aligned}$$

This shows that for every constant $\delta < 1$, we get a polynomial time algorithm, where the running time increases for increasing δ. With the case $\delta = 1$, we deal in the next part.

For the approximation of SV, consider the basis B after termination. As we did not swap, we have

$$\left\|b^\star_{j\ new}\right\|^2 = \left\|b^\star_{j+1} + \mu_{j,j+1} b^\star_j\right\| \geq \delta \left\|b^\star_j\right\|^2,$$

implying

$$\left\|b^\star_{j+1}\right\|^2 \geq (\delta - \frac{1}{4}) \left\|b^\star_j\right\|^2.$$

This shows that chosing $\delta \leq \frac{1}{4}$ does not make sense, as we do not have any restriction on the size any more. Let $\delta \in (1/4, 1)$, and $k = \operatorname{argmin}_j \left\| b_j^\star \right\|^2$.

$$\|S V\|^2 \geq \left\| b_k^\star \right\|^2 \geq (\delta - 1/4)^{k-1} \|b_1\|^2 \geq (\delta - 1/4)^{n-1} \|b_1\|^2$$

shows that with increasing δ, we get a better approximation ratio.

2. For $\delta = 1$, take another look on (1). As the inequality is strict, the potential still drops, though we cannot say anything about the factor. But as the potential function is integral, it drops by at least 1 and, using the notation of the part before, we have at most

$$\left(n \|B\|_\infty^2\right)^{O(n^2)}$$

iterations in total, hence the algorithm terminates.