

Problem Set 3

Instructor: Daniele Micciancio

Due: Tue Feb 6, 2024

1 Lattice reduction

Recall that a basis $[\mathbf{a}, \mathbf{b}]$ is reduced if $\|\mathbf{a}\| \leq \|\mathbf{b}\|$ and $|\langle \mathbf{a}, \mathbf{b} \rangle| / \|\mathbf{a}\| \|\mathbf{b}\| \leq 1/2$. In class we have seen how a reduced basis can be efficiently found using the Gauss/Lagrange algorithm.

In class we have described the LLL algorithm as a generalization of the Gauss/Lagrange algorithm to lattices in dimension n . Specifically, the LLL algorithm ensures that the output basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ satisfies the following properties:

- LLL: for any i , the pair of projected vectors $[\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1})]$ (where π_i is the projection orthogonal to $\mathbf{b}_1, \dots, \mathbf{b}_{i-1}$) is reduced.

The use of the projection operation π_i plays an important role in the analysis of the running time of the LLL algorithm. But one may wonder if it also has an impact on the output quality. This is the question explored in this problem.

Question: build a basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ such that

- for any index $i < n$, the pair of vectors $[\mathbf{b}_i, \mathbf{b}_{i+1}]$ (i.e., without projecting) is reduced.
- the SVP approximation factor $\gamma(n) = \|\mathbf{b}_1\|/\lambda_1$ is as large as possible (as a function of n)

(You do not need to prove that your $\gamma(n)$ is the largest possible value. Just make it as large as you can, and analyze your construction.) How does the γ factor achieved by your construction compare to LLL? Can you find a basis $\mathbf{B}$ for which $\gamma(n)$ is worse than the approximation factor guaranteed by LLL?

Optional: If you find the above problem easy enough, consider a variant problem where the first condition is replaced by

- for any indexes $i < j$, the pair of vectors $[\mathbf{b}_i, \mathbf{b}_j]$ is reduced.

Clearly, a basis satisfying this property also satisfies the property in the main question. So, here γ can only get smaller, which is better. Can you still find a basis $\mathbf{B}$ for which $\gamma(n)$ is worse than the approximation factor guaranteed by LLL? What is the worst $\gamma(n)$ you can achieve?