

Problem Set 2

Instructor: Daniele Micciancio

Due on: Tue. Feb 16, 2010

In the solution of the first three problems, you are allowed to use calculators, computers, etc. All problems can be solved by hand. If you prefer to write and run a computer program to carry some of the steps, that's fine too. In such a case, there is no need to submit your computer code, but you should state clearly what you did.

Problem 1

Find an LLL reduced basis (with $\delta = 1/2$) for the lattice generated by $\mathbf{B} = \begin{bmatrix} 3 & 9 & 3 \\ 4 & 3 & 5 \\ 8 & 6 & 2 \end{bmatrix}$ by executing the LLL basis reduction algorithm. Then answer the following questions:

1. What is the value of the potential function \mathcal{D} for the input matrix?
2. What is the number of iterations (swaps) predicted by the running time analysis of LLL?
3. What is the value of \mathcal{D} upon finding a reduced basis?
4. Give an upper bound on the number of iterations based on the initial and final value of \mathcal{D}
5. What is the number of iterations actually executed?
6. What is the upper bound on the length of the shortest vector obtained from Minkowski's theorem?
7. What is the length of the shortest vector in the final output of LLL?

Problem 2

Compute the HNF of the lattice from Problem 1. Then, give the value of the lower bound $\min_i \|\vec{b}_i^*\|$ on the minimum distance of the lattice obtained using

1. The original basis \mathbf{B}
2. The LLL reduced basis you found in Problem 1
3. The HNF basis

Problem 3

Use the Nearest Plane algorithm to find lattice vectors close to the targets

$$\vec{v}_1 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \quad \vec{v}_2 = \begin{bmatrix} 4 \\ -2 \\ 14 \end{bmatrix} \quad \vec{v}_3 = \begin{bmatrix} -1 \\ 3 \\ 17 \end{bmatrix} \quad \vec{v}_4 = \begin{bmatrix} 7 \\ 3 \\ -3 \end{bmatrix}$$

1. using the LLL reduced basis from Problem 1
2. using the HNF basis from Problem 2

In each case, give also the distance of the vector you found from the target.

Problem 4

Let \mathbf{B} be an LLL reduced basis (with $\delta = 1$) of a full rank 2-dimensional lattice. Prove that $\|\vec{b}_1\| = \lambda(\mathbf{B})$, i.e., the first basis vector solves SVP exactly.

Problem 5

Find a “bad” basis for the LLL algorithm, i.e., an n -dimensional basis which is LLL reduced, and still the first basis vector is much longer than the minimum distance of the lattice.