CSC 2414 Problem Set 2

Due: October 31, 2011

Notes

- This problem set is worth 100 points.
- Collaboration is allowed, *but you must write up the solutions by yourself without consulting to notes from the discussions.* You must also reference your sources.
- Grading is based on correctness as well as the clarity of the solutions. When writing proofs, it is generally a good idea to first explain the intuition behind your solution in words (wherever appropriate), before jumping in to the formalisms.
- There is no deadline for the extra credit problem. You can turn in a solution any time until the last class.

Problem 1: Properties of LLL-Reduced Bases (25 points)

Show that a δ-LLL reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of a lattice L with $\delta = 3/4$ satisfies the following properties.

1. $\|\mathbf{b}_1\| \leq 2^{(n-1)/4} \cdot \det(L)^{1/n}$.
2. For any $1 \leq i \leq n$, $\|\mathbf{b}_i\| \leq 2^{(i-1)/2} \cdot \|\widetilde{\mathbf{b}}_i\|$.
3. $\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq 2^{n(n-1)/4} \cdot \det(L)$.
4. For $1 \leq i \leq n$, consider the hyperplane $H = \mathsf{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n)$. Show that

   $$2^{-n(n-1)/4}\|\mathbf{b}_i\| \leq \mathsf{dist}(H, \mathbf{b}_i) \leq \|\mathbf{b}_i\|$$

   Hint: use (3).

Problem 2: Exponential-time Algorithm to find the Shortest Vector (25 points)

Show an algorithm that solves SVP exactly in time $2^{O(n^2)} \cdot \mathsf{poly}(D)$, where n is the rank of the lattice and D is the input size. (Hint: show that if we represent the shortest vector in an LLL-reduced basis, none of the coefficients can be larger than 2^{cn} for some constant c.)

Problem 3: Rounding to find an Approximately Close Lattice Vector (25 points)

Show that there is a constant $c > 0$ such that the following algorithm, given a basis $\mathbf{B} \in \mathbb{Z}^{m \times n}$ and a target vector $\mathbf{t} \in \mathbb{Z}^m$, finds a lattice point $\mathbf{y} \in \mathcal{L}(\mathbf{B})$ where

$$\|\mathbf{y} - \mathbf{t}\| \leq 2^{cn} \cdot \mathsf{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$$

Algorithm Round($\mathbf{B}, \mathbf{t}$):

1. Run the LLL-reduction algorithm on $\mathbf{B}$ to get an LLL-reduced basis $\mathbf{B}'$.
2. Find $\mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{R}^n$ such that $\mathbf{B}'\mathbf{s} = \mathbf{t}$, say, by Gaussian Elimination.
3. Let $\hat{\mathbf{s}} \triangleq (\lfloor s_1 \rceil, \ldots, \lfloor s_n \rceil)$ be the vector consisting of the entries of $\mathbf{s}$ rounded to the nearest integer. (e.g., $\lfloor 0.5 \rceil = 1$ and $\lfloor 0.49 \rceil = 0$).

   Output $\mathbf{y} = \mathbf{B}'\hat{\mathbf{s}}$.

Problem 4: Running Time of LLL (25 points)

Show that our analysis of the LLL algorithm using LLL-reduced bases is tight (up to some constant). More specifically, find a δ-LLL reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ for $\delta = 3/4$ such that $\mathbf{b}_1$ is longer than the shortest vector by a factor or $c \cdot 2^{n/2}$, for some constant c.
(Note that this does not mean that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is the output of the LLL algorithm when run on some input basis. You do not have to demonstrate that.).

Extra Credit**

For any vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}^n$, let $\mathsf{Rot}(\mathbf{v}) \triangleq (v_2, v_3, \ldots, v_n, v_1)$ denote the cyclic rotation of $\mathbf{v}$. A cyclic lattice is one that is closed under the $\mathsf{Rot}(\cdot)$ operation. That is, a lattice L is cyclic if for every $\mathbf{v} \in L$, $\mathsf{Rot}(\mathbf{v}) \in L$ too. Show any of the following:

- CVP on cyclic lattices is NP-hard (Recall, we saw in class that CVP for general lattices is NP-hard).
- An interactive proof for gapCVP_γ on cyclic lattices, for any $\gamma = o(\sqrt{n/\log n})$, improving on the Goldreich-Goldwasser interactive proof we saw in class.
- A polynomial-time algorithm that finds $2^{o(n)}$-approximate shortest vectors on cyclic lattices, improving on the LLL algorithm.