6.876 Advanced Topics in Cryptography: Lattices *Instructor: Vinod Vaikuntanathan*

Problem Set 1

Handed Out: October 3, 2017 *Due: October 24, 2017*

Notes

- This problem set is worth 90 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.
- *Notation:* $\mathbb{N}$ denotes the natural numbers, $\mathbb{Z}$ denotes the integers, $\mathbb{Q}$ denotes rational numbers and $\mathbb{R}$ the set of real numbers.

Problem 1: Bases (10 points)

Describe a procedure that given any set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$, find a basis for the lattice $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ (notice that these vectors are not necessarily linearly independent and that in particular, n might be greater than m). There is no need to analyze the running time. A corollary is that any set of vectors in $\mathbb{Z}^m$ spans a lattice.

Problem 2: Minkowski's First Theorem (20 points)

Despite lattices with much shorter vectors than predicted, Minkowski's theorem is tight for general lattices. In particular, there is a family of lattices $\{\mathcal{L}_n\}_{n\in\mathbb{N}}$ where $\mathcal{L}_n$ lives in n dimensions, and

$$\lambda_1(\mathcal{L}_n) \geq c \cdot \sqrt{n} \cdot \det(\mathcal{L}_n)^{1/n}$$

where c is a universal constant independent of n.

Show that such a family of lattices exists (your proof doesn't have to construct this family, you merely have to show existence).

Problem 3: Properties of LLL-Reduced Bases (15 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. $||\mathbf{b}_1|| \leq 2^{(n-1)/4} \cdot \det(\mathcal{L}(\mathbf{B}))^{1/n}$.
2. For any $1 \leq i \leq n$, $||\lambda_i(\mathcal{L}(\mathbf{B})) \leq 2^{(i-1)/2} \cdot ||\widetilde{\mathbf{b}}_i||$.
3. For any $1 \leq i \leq n$, $||\lambda_i(\mathcal{L}(\mathbf{B})) \geq 2^{-(n-1)/2} \cdot ||\mathbf{b}_i||$.

Problem 4: Running Time of LLL (15 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.

Problem 5: LLL Weirdness (15 points)

Find a basis $\mathbf{B}$ such that after we apply one reduction step of the LLL algorithm to it, the maximum length of a vector in it *increases* by $\Omega(\sqrt{n})$.

Problem 6: SIVP and CVP (15 points)

Show a reduction from the closest vector problem (CVP) to the shortest independent vectors problem (SIVP). Recall that in SIVP, you are given a basis $\mathbf{B}$ of a full-rank lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ and you are asked to produce n linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$ such that $||\mathbf{v}_i|| \leq \lambda_i$.

For extra credit, show an approximation-preserving reduction. That is, given an oracle to solve γ-approximate SIVP, can you solve γ-CVP for some $\gamma > 1$? Here, in γ-approximate SIVP, you are only required to produce vectors $\mathbf{v}_i$ as above where $||\mathbf{v}_i|| \leq \gamma \cdot \lambda_i(\mathcal{L})$.