Lattices and Homomorphic Encryption, Spring 2013	Instructors: Shai Halevi, Tal Malkin

Problem Set #2

February 5, 2013 — Due February 19, 2013

1 Lattices and their Determinant

(a) Prove that if $\mathcal{L} \subset \mathbb{Z}^n$ is a full-rank integer lattice with prime determinant, then it has no nontrivial refinements. Namely, if $\mathcal{L} \subseteq \mathcal{L}'$ for some integer lattice $\mathcal{L}'$ then $\mathcal{L}' = \mathcal{L}$ or $\mathcal{L}' = \mathbb{Z}^n$.

(b) Prove the converse: if $\mathcal{L} \subset \mathbb{Z}^n$ is a full rank lattice and $\det(\mathcal{L})$ is a composite, then $\mathcal{L}$ has a nontrivial refinement. Namely, there exists a lattice $\mathcal{L}'$ such that $\mathcal{L} \subsetneq \mathcal{L}' \subsetneq \mathbb{Z}^n$.

2 Successive Minima and Bases

(a) Consider set of vectors in $\mathbb{Z}^n$ whose entries are either all-even integers or all-odd integers,

$$\mathcal{L}^* = \{x \in \mathbb{Z}^n : x_i \text{ is odd } \forall i\} \cup \{x \in \mathbb{Z}^n : x_i \text{ is even } \forall i\}.$$

Prove that $\mathcal{L}^*$ is a lattice and that $\lambda_i(\mathcal{L}) = 2$ for all $i = 1, 2, \ldots, n$.

(b) Prove that every basis for $\mathcal{L}^*$ must include at least one vector of length $\sqrt{n}$ or more. (Note that in conjunction with Part (a), this means that for $n > 4$ the successive minima do not form a basis for this lattice.)

3 Gram-Schmidt, LLL, and Dual Lattices

Recall that the Gram-Schmidt orthogonalization of a basis $B = (b_1, \ldots, b_n)$ is $\tilde{B} = (\tilde{b_1}, \ldots, \tilde{b_n})$ such that the $\tilde{b_i}$'s are orthogonal to each other and $b_i = \tilde{b_i} + \sum_{j<i} \mu_{i,j}\ \tilde{b_j}$, where $\mu_{i,j} = \left\langle b_i, \tilde{b_j} \right\rangle / \|\tilde{b_j}\|^2$.

Recall also that a basis $B = (b_1, \ldots, b_n)$ is LLL reduced if its Gram-Schmidt orthogonalization satisfies

$$\forall\ 1 \le j < i \le n, \qquad |\mu_{i,j}| \ \le\ 1/2 \tag{1}$$

$$\forall\ 1 \le i < n, \qquad \|\tilde{b}_{i-1}\|^2 \cdot \frac{3}{4} \ \le\ \|\tilde{b_i} + \mu_{i,i-1}\tilde{b}_{i-1}\|^2 \tag{2}$$

Note that all the "smallness" properties of LLL-reduced bases actually rely on a weaker first condition, namely that

$$\forall\ 1 \le j < n, \qquad |\mu_{j+1,j}| \ \le\ 1/2 \tag{3}$$

(The stronger condition from Equation (1) is only needed to prove that the numbers do not grow too large during the LLL procedure.) Below we call a basis "*effectively LLL-reduced*" if it satisfies Equations (3) and (2).

Let $B = (b_1, \ldots, b_n)$ be a basis of a full rank lattice $\mathcal{L}$, let D' be the dual basis (i.e., $D' = (B^{-1})^t$), and let $D = (d_1, \ldots, d_n)$ be the matrix D' with the order of the columns reversed. Namely

$$\langle b_i, d_j \rangle = \begin{cases} 1 & \text{if } i = n + 1 - j \\ 0 & \text{otherwise} \end{cases}$$

(a) Prove that the following relation holds for all i:

$$\tilde{b_i} \;=\; \tilde{d}_{n+1-i}/\|\tilde{d}_{n+1-i}\|^2 \tag{4}$$

(b) Using Equation (4), prove that the following relation holds for all i:

$$\left\langle b_i, \tilde{b}_{i-1}\right\rangle/\|\tilde{b}_{i-1}\|^2 = -\left\langle d_{n+2-i}, \tilde{d}_{n+1-i}\right\rangle/\|\tilde{d}_{n+1-i}\|^2 \tag{5}$$

(c) Using Equations (4) and (5), prove that if B is effectively LLL-reduced then so is D.

4 Easy Lattice Problems

(a) Describe an efficient algorithm that given the bases B_1, B_2 of two full-rank integer lattices $\mathcal{L}_1 = \mathcal{L}(B_1), \mathcal{L}_2 = \mathcal{L}(B_2) \subseteq \mathbb{Z}^n$, computes a basis for their sum, $\mathcal{L}_1 + \mathcal{L}_2 = \{x + y : x \in \mathcal{L}_1, y \in \mathcal{L}_2\}$.

(b) Describe an efficient algorithm that given the bases B_1, B_2 of two full-rank integer lattices $\mathcal{L}_1 = \mathcal{L}(B_1), \mathcal{L}_2 = \mathcal{L}(B_2) \subseteq \mathbb{Z}^n$, computes a basis for their intersection, $\mathcal{L}_1 \cap \mathcal{L}_2$. *Hint.* Consider the duals of $\mathcal{L}_1$, $\mathcal{L}_2$, and $\mathcal{L}_1 \cap \mathcal{L}_2$.