**Fall 2009**<br>
**Lattices in Computer Science**

# Homework 2
## Due 2009/12/3

**Oded Regev**<br>
**School of Computer Science**<br>
**Tel Aviv University**

### Instructions

**Language:** Submission should be in English only.

**Writeup:** You must do the writeup alone. For each question, cite all references used (or write 'none') and collaborators (or write 'alone'). Explain why you needed to consult any of the references.

**Collaboration:** Collaboration is allowed, but limit yourselves to groups of size at most two.

**References:** Try not to run to reference material to answer questions (this also includes the web!). Try to think about the problem to see if you can solve it without consulting any external sources. If this fails, you may ask me for a hint, or look up any reference material.

**Deadline:** The deadline is strict.

## Problems

1. Show that for any full-rank integer lattice $\Lambda$, $\det(\Lambda) \cdot \mathbb{Z}^n \subseteq \Lambda$.

2. Describe an algorithm that given a basis $b_1, \ldots, b_n \in \mathbb{Q}^n$ of a full-rank lattice and a point $t \in \mathbb{Q}^n$, finds a point $x \in \mathcal{L}(b_1, \ldots, b_n)$ such that $\|x - t\|^2 \le \frac{1}{4}(\|\tilde{b}_1\|^2 + \cdots + \|\tilde{b}_n\|^2)$.

3. (a) For all large enough $n \in \mathbb{Z}$, find an $n$-dimensional full-rank lattice in which the successive minima $v_1, \ldots, v_n$ (in the $\ell_2$ norm) do not form a basis of the lattice. Hint: Cesium Chloride

   (b) Show that for any 2-dimensional full-rank lattice $\Lambda$, the successive minima $v_1, v_2$ *do* form a basis of $\Lambda$. Hint: consider the lattice obtained by projecting $\Lambda$ on the one-dimensional subspace $\{v_1\}^\perp$ and show that the projection of $v_2$ must be a basis of this lattice

   (c) Among all 2-dimensional full-rank lattices with $\lambda_1(\Lambda) = 1$, which one has the smallest $\det \Lambda$? (this lattice is unique up to rotation). Can you guess which 3-dimensional lattice with $\lambda_1(\Lambda) = 1$ has the smallest $\det \Lambda$? (no proof necessary for this)

4. Show that a $\delta$-LLL reduced basis $b_1, \ldots, b_n$ of a lattice $\Lambda$ with $\delta = \frac{3}{4}$ satisfies the following properties.

   (a) $\|b_1\| \le 2^{(n-1)/4}(\det \Lambda)^{1/n}$

   (b) For any $1 \le i \le n$, $\|b_i\| \le 2^{(i-1)/2}\|\tilde{b_i}\|$

   (c) $\Pi\|b_i\| \le 2^{n(n-1)/4} \det \Lambda$
   Remark: the quantity $\Pi\|b_i\|/\det \Lambda$ is known as the *orthogonality defect* of the basis; to see why, notice that it is 1 iff the basis is orthogonal; it can never be less than one by Hadamard's inequality.

   (d) For any $1 \le i \le j \le n$, $\|b_i\| \le 2^{(j-1)/2}\|\tilde{b_j}\|$

   (e) For any $1 \le i \le n$, $\lambda_i(\Lambda) \le 2^{(i-1)/2}\|\tilde{b}_i\|$

   (f) For any $1 \le i \le n$, $\lambda_i(\Lambda) \ge 2^{-(n-1)/2}\|b_i\|$

   (g) For $1 \le i \le n$ consider $H = \mathrm{span}\{\mathrm{b_1}, \ldots, \mathrm{b_{i-1}}, \mathrm{b_{i+1}}, \ldots, \mathrm{b_n}\}$. Show that $2^{-n(n-1)/4}\|b_i\| \le \mathrm{dist}(H, b_i) \le \|b_i\|$. Hint: use (c)

5. Find a basis $b_1, \ldots, b_n$ such that after we apply one reduction step of the LLL algorithm to it, the maximum length of a vector in it *increases* (even by as much as $\Omega(\sqrt{n})$).

6. Show an algorithm that solves SVP exactly in time $2^{O(n^2)} \cdot \text{poly}(D)$ 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 $c$.

7. Show that our analysis of the LLL algorithm is tight (perhaps up to some constant). More specifically, find an LLL reduced basis $b_1, \ldots, b_n$ such that $b_1$ is longer than the shortest vector by a factor or $\Theta(2^{n/2})$.