2nd Bar-Ilan Winter School on Cryptography
Lattice-Based Cryptography and Applications: Day 2 Assignments

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

2. Show that an LLL reduced basis $b_1, \ldots, b_n$ of a lattice Λ satisfies the following properties.

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

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

   (c) $\Pi\|b_i\| \leq 2^{n(n-1)/4} \det \Lambda$
   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 $1 \leq i \leq j \leq n$, $\|b_i\| \leq 2^{(j-1)/2}\|\tilde{b_j}\|$

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

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

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

3. 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.

4. (a) Let $\mathbf{S} \in \mathbb{Z}^{m \times m}$ be a basis for $\Lambda^{\perp}(\mathbf{A})$ (i.e., $\mathbf{AS} = \mathbf{0}$ and $\mathbf{S}$ is nonsingular over the integers), and suppose that the columns of $\mathbf{A}$ generate all of $\mathbb{Z}_q^n$ (i.e., $\mathbf{A} \cdot \mathbb{Z}^m = \mathbb{Z}_q^n$). Let $\mathbf{A}' = [\mathbf{A}|\mathbf{A}_1]$ be an arbitrary extension of $\mathbf{A}$. Show how, given $\mathbf{S}$ and $\mathbf{A}'$, to efficiently compute a basis $\mathbf{T}$ of $\Lambda^{\perp}(\mathbf{A}')$ so that $\max\|\tilde{\mathbf{t}}_i\| = \max\|\tilde{\mathbf{s}}_i\|$ (where $\mathbf{s}_i, \mathbf{t}_i$ are the ith columns of $\mathbf{S}, \mathbf{T}$ respectively, and the tilde notation $\tilde{\cdot}$ denotes the Gram-Schmidt orthogonalization).

   (b) In the second trapdoors talk we defined $\mathbf{R}$ to be a (strong) trapdoor for $\Lambda^{\perp}(\mathbf{A})$ if

   $$\mathbf{A}\left[\begin{smallmatrix}\mathbf{R}\\ \mathbf{I}\end{smallmatrix}\right] = \mathbf{G},$$

   the special gadget matrix. Prove that the order of the rows in $\left[\begin{smallmatrix}\mathbf{R}\\ \mathbf{I}\end{smallmatrix}\right]$ is immaterial, i.e., that we can still efficiently invert LWE and sample Gaussian-distributed SIS preimages for $\mathbf{A}$ even if the rows of $\left[\begin{smallmatrix}\mathbf{R}\\ \mathbf{I}\end{smallmatrix}\right]$ are arbitrarily permuted. *Hint:* show that $\left[\begin{smallmatrix}\mathbf{R}\\ \mathbf{I}\end{smallmatrix}\right]$ is a trapdoor (in the above sense) for some matrix $\mathbf{A}'$ whose columns are a permutation of the columns of $\mathbf{A}$. Then show why inverting LWE and sampling SIS preimages are equivalent for $\mathbf{A}$ and $\mathbf{A}'$.

   (c) Using the previous part, give a *very* simple and efficient algorithm for extending a trapdoor $\mathbf{R}$ for $\mathbf{A}$ into a trapdoor $\mathbf{R}'$ for any extended matrix $\mathbf{A}' = [\mathbf{A}|\mathbf{A}_1]$, so that $s_1(\mathbf{R}') = s_1(\mathbf{R})$. (Recall that $s_1(\mathbf{R}) = \max_{\mathbf{u}\neq\mathbf{0}}\|\mathbf{Ru}\|/\|\mathbf{u}\|$ is the spectral norm of $\mathbf{R}$.)