Fall 2009
Lattices in Computer Science

Homework 5
Due 2010/2/21

Oded Regev
School of Computer Science
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.

1. Show that for any $\varepsilon < \frac{1}{100}$ we have $\eta_\varepsilon(\Lambda) \geq \frac{1}{\lambda_1(\Lambda^*)} \geq \frac{1}{n}\lambda_n(\Lambda)$.

2. The *discrete Gaussian distribution* on Λ with parameter $s \geq 0$ and center $c \in \mathbb{R}^n$, denoted $D_{\Lambda,s,c}$, is defined as the probability distribution with support Λ that assigns to each $x \in \Lambda$ the probability $\rho_s(x-c)/\rho_s(\Lambda - c)$. Show that for $s \geq \sqrt{2}\eta_\varepsilon(\Lambda)$, any $c \in \mathbb{R}^n$, and any $n-1$-dimensional hyperplane H,

$$\Pr_{x \sim D_{\Lambda,s,c}}[x \in H] < 0.9.$$

Hint: Notice that without loss of generality, we can assume that $H = \{x \in \mathbb{R}^n \mid x_1 = r\}$ for some $r \geq 0$. Then observe that it is enough to show that $\mathrm{Exp}_{x \sim D_{\Lambda,s,c}}[e^{-\pi(\frac{x_1 - r}{s})^2}] < 0.9$. Prove this using the Poisson summation formula.

3. Consider the following algorithm for sampling from $D_{\Lambda,s,c}$. Assume we have a good basis B of Λ. The algorithm samples a point from the *continuous* Gaussian distribution $\rho_s(x-c)/s^n$, rounds it to a nearby lattice point (say, using Babai's nearest plane algorithm), and outputs the result. Show that the output of this algorithm is statistically quite far from $D_{\Lambda,s,c}$, even for radii s that are polynomially bigger than the length of the given basis. Hint: Take the lattice $\mathbb{Z}$ and $c = 0$, and let s be, say, n^{10}. Show that the probability of outputting 0 is noticeably far from what it should be.

4. Consider the following identification scheme. The public and private keys are chosen as in the LWE public key encryption scheme. The verifier picks a random bit string $c \in \{0,1\}^k$ and sends encryptions of $c_1, \ldots, c_k$. The prover decrypts those encryptions and sends back $z_1, \ldots, z_k$. The verifier accepts if and only if $z_i = c_i$ for all i.

   (a) Prove that the scheme is correct (for honest parties).

   (b) Prove that the scheme is secure against passive attacks (i.e., attacks where the adversary just watches interactions and then tries to impersonate).

   (c) Prove that the scheme is not secure against active attacks. Hint: Show that a malicious verifier can recover the private key.