Homework 4
Due 2005/1/10

Oded Regev
Department of Computer Science
Tel Aviv University

1. For a lattice Λ let $\mu(\Lambda)$ denote the covering radius of Λ.

   (a) Let Λ be some arbitrary lattice and let B be some basis for it. Show that if x is chosen uniformly from $\mathcal{P}(B)$ then

   $$\Pr[d(x,\Lambda) \geq \mu(\Lambda)/2] \geq \frac{1}{2},$$

   i.e., the distance of x from Λ is at least half the covering radius of Λ with probability at least half. (The choice of $\mathcal{P}(B)$ is mainly for technical convenience; you might want to first imagine a proof for a point chosen 'uniformly from $\mathrm{span}(\Lambda)$')

   (b) We define the promise problem GapCRP_γ as follows. An input is a pair (B,d) where B is a rank n lattice basis and d is a rational number. In YES inputs $\mu(\mathcal{L}(B)) \leq d$ and in NO inputs $\mu(\mathcal{L}(B)) > \gamma \cdot d$. Find an AM protocol for GapCRP_2.

   (c) For a lattice Λ, we define $\alpha(\Lambda)$ as the smallest $r > 0$ such that

   $$\Pr_x[d(x,\Lambda) \geq \mu(\Lambda)/r] \geq \frac{1}{100}.$$

   We already know that for any lattice Λ, $\alpha(\Lambda) \leq 2$. Show that for any $\varepsilon > 0$, there exists a lattice Λ such that $\alpha(\Lambda) > \sqrt{3} - \varepsilon$. Can you find lattices with larger $\alpha(\Lambda)$?

2. For a lattice Λ let $\mu(\Lambda)$ denote the covering radius of Λ.

   (a) Show that for any lattice Λ, $\mu(\Lambda) \geq \lambda_1(\Lambda)/2$. Hint: We showed something stronger in class.

   (b) Show that for any integer n, there exists an n-dimensional full-rank lattice Λ that satisfies $\mu(\Lambda) \leq 3\lambda_1(\Lambda)/2$ (for starters, show $\mu(\Lambda) \leq 2\lambda_1(\Lambda)$). Hint: Starting with some lattice, say $\mathbb{Z}^n$, show that as long as $\mu(\Lambda) > 3\lambda_1(\Lambda)/2$, one can replace Λ with some $\Lambda' \supseteq \Lambda$ such that $\lambda_1(\Lambda) = \lambda_1(\Lambda')$. The lattice Λ' is obtained from Λ by adding a carefully chosen vector to the basis.