Fall 2009
Lattices in Computer Science

Homework 3
Due 2009/12/17

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.

Problems

1. Improve the bound B in Coppersmith's algorithm to $N^{1/d}$. Hint: for some $h \geq 2$, consider the set of polynomials $\{N^{h-i-1} f(x)^i x^j \mid 0 \leq j < d,\ 0 \leq i < h\}$ and work modulo N^{h-1}. For $h = 2$ this is the set we had in class. Show that we can obtain $B = N^{1/d-\varepsilon}$ for any constant $\varepsilon > 0$ by setting h to be a large enough constant. Next show that by setting h to be some function of N, this becomes $B = N^{1/d}/C$ for some constant $C > 0$. Finally, show how to obtain $B = N^{1/d}$ using this.

2. For any $\gamma \geq 1$, describe a randomized Karp reduction from GapSVP_γ to GapCVP_γ. The reduction should map NO instances to NO instances with probability 1 and YES instance to YES instances with some probability $p > 0$. First show this for $p = \frac{1}{n}$ and later try to improve this to $p = \frac{1}{2}$. Hint for $p = \frac{1}{2}$: given an SVP instance $(b_1, \ldots, b_n)$ construct the CVP instance $(2b_1, b_2 + c_2 b_1, \ldots, b_n + c_n b_1)$ with the target vector b_1 where $c_2, \ldots, c_n$ are independently chosen to be 0 or 1 with probability $\frac{1}{2}$.

3. Prove that $\mathsf{GapSVP}_{\sqrt{n}} \in \mathsf{NP} \cap \mathsf{coAM}$ (try to find an AM protocol similar to the one we had in class and not use the 'large cube' approach).