Computer Science 2421 Spring, 2003
St George Campus University of Toronto

Homework Assignment #3
Due: April 25, 5PM, SF2301C

1. In Lecture #9, we gave an algorithm that uses L^3 to solve most subset-sum problems involving n numbers randomly chosen from $\{0, 1, \dots, 2^{n^2} - 1\}$. In the notes, we show that the algorithm solves at least a fraction $1 - 1/n$ of the inputs.

   Doing a better analysis, prove that for every $\epsilon > 0$ and sufficiently large n, the *same* algorithm solves at least a fraction
$$1 - \frac{1}{2^{(n^2/4)(1-\epsilon)}}$$
   of the inputs.

2. Prove that for every constant s, $1 > s \geq 0$,
   $\mathrm{PCP}_{1,s}(O(\log n), 2) = \mathrm{P}$.

3. Consider the proof of Theorem 7 in Notes #11. Show how by repeating this graph composition a non-constant number of times, we can prove the result stated at the top of Page 9:

   If NP $\not\subseteq$ QP, then for every $\epsilon > 0$, no quasi-polynomial time algorithm approximates CLIQUE to within a factor of $2^{(\lg n)^{1-\epsilon}}$ (where n is the number of vertices).

   (Note that $2^{(\lg n)^{1-\epsilon}} < n^\delta$ for every $\delta > 0$, so this result – although easier to obtain – is much worse than the best results given in the notes.)

4. We wish to prove that, relative to an arbitrary oracle, we do not have interactive proof systems for the tautologies.

   Say that a verifier, on input 1^n, has access to an oracle $B : \{0,1\}^n \to \{0,1\}$; he wishes to interact with a prover who also has access to the same oracle, and the prover tries to prove that $B(x) = 0$ for all $x \in \{0,1\}^n$. We place no restriction on the computation time of the prover, and indeed, he is even allowed to query the entire oracle.

   Prove that there is no polynomial-time, probabilistic verifier V that interacts with a prover, such that for all n, given 1^n and access to an oracle $B : \{0,1\}^n \to \{0,1\}$, for all B:

   - If $B(x) = 0$ for all $x \in \{0,1\}^n$, then there is a prover that interacts with V that causes V to accept with probability 1.
   - If $B(x) \neq 0$ for some $x \in \{0,1\}^n$, then for every prover (that also has access to B) that interacts with V, V accepts with probability $< 1/2$.