Homework 12
Due Wed Jun 1, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

For this homework, we use the notation $\mathsf{PCP}_{c,s}[r,q]$ for the class of languages that have probabilistically checkable proof systems with completeness c, soundness s, using r random bits, and making q queries. All of these parameters can be functions of n, the input length.

When c and s are unspecified, the default values are $c = 1$ and $s = \frac{1}{2}$. We also define the shorthand notation $\mathsf{PCP}[\log, \text{const}] = \bigcup_{c,d=1}^{\infty} \mathsf{PCP}[c \log n, d]$. The PCP theorem then states that $\mathsf{NP} = \mathsf{PCP}[\log, \text{const}]$.

27. Recall that the querying done by the verifier in a PCP system is required to be non-adaptive.

    Let A be a language. Prove that if A has a PCP-verifier using r random bits and q *adaptive* queries (i.e., the locations to be queried may depend on the outcomes of previous queries), then $A \in \mathsf{PCP}[r, 2^q]$. [2 points]

28. Prove that if $\text{SAT} \in \mathsf{PCP}[r(n), \text{const}]$ for some function $r(n) = o(\log n)$, then $\mathsf{P} = \mathsf{NP}$. [2 points]