CSE 521: Design and Analysis of Algorithms Assignment #8

due: Thursday, Dec 8. 10:30AM.

No late days may be used on this assignment

Each problem is worth 10 points. See the website for grading guidelines.

---

1. Consider the problem of factoring large integers. That is, if x is a positive integer, we would like to find distinct primes $p_1, \ldots, p_k$ and positive integers $a_1, \ldots, a_k$ such that $x = p_1^{a_1} \cdots p_k^{a_k}$. To formulate this as a yes/no question, define FACTOR to be the problem of determining, given positive integers x and t, whether there exists an integer y such that $1 < y \leq t$ and y divides x.

   (a) Prove that given a black box for FACTOR, it is possible to find the prime factorization of x in polynomial time. Recall that "polynomial" means "polynomial in the input length," which in this case means the number of bits required for x.

   (b) Prove that FACTOR is in $\mathbf{NP} \cap \mathbf{co} - \mathbf{NP}$.

   (c) Prove that if FACTOR is NP-complete, then $\mathbf{NP} = \mathbf{co} - \mathbf{NP}$. *Not a hint, just some motivation: Modern cryptography is based on hardness assumptions, although no one has yet successfully devised a cryptosystem that is secure assuming only* $\mathbf{P} \neq \mathbf{NP}$. *Instead, systems used in practice use the assumption that FACTOR is computationally hard, although the problem is considered much easier than problems such as 3-SAT.*

2. KT, Chapter 8, Exercise 13

3. KT, Chapter 8, Exercise 20

4. KT, Chapter 8, Exercise 37