

Due: Friday, March 17, beginning of tutorial

NOTE: Each problem set counts 10% of your mark, and it is important to do your own work. You may consult with others concerning the general approach for solving problems on assignments, but you must write up all solutions entirely on your own. Copying assignments is a serious academic offense and will be dealt with accordingly.

1. Consider the following decision problem.

SmallCycle

Instance:

$\langle G \rangle$, where G is an undirected graph with an even number n of vertices.

Question:

Does G have a cycle of size exactly $n/2$?

Prove that SmallCycle is NP-complete. You may assume that HamCycle is NP-complete. (See Notes “NP and NP-Completeness” page 13.)

2. Consider the following decision problem:

HittingSet

Instance: $\langle k, n, T_1, \dots, T_m \rangle$ where k and n are positive integers presented in unary notation, and $T_i \subseteq \{1, \dots, n\}$ for $1 \leq i \leq m$.

Question: Is there $S \subseteq \{1, \dots, n\}$ such that S has at most k elements and $S \cap T_i \neq \emptyset$ for $1 \leq i \leq m$?

Give a reduction showing that HittingSet \leq_p SAT. Prove that your reduction is correct.

3. In this problem all numbers are presented in binary notation. The problem of factoring positive integers into their prime factors can be formalized as follows:

Let FACTOR be the following search problem: (See Notes “Search and Optimization Problems”.)

Instance:

$\langle x \rangle$, where x is an integer ≥ 2 .

Output:

$\langle p_1, \dots, p_m \rangle$, where each p_i is a prime number and x is the product $p_1 p_2 \dots p_m$.

It is an open problem whether this problem can be solved in polynomial time on a Turing machine. (However it can be solved in polynomial time using the mathematical definition of a “quantum computer”.)

Let

$$DIV = \{ \langle x, y \rangle \mid x, y \in \mathbb{N} \text{ and } x \text{ has a divisor } d, 1 < d \leq y \}$$

(a) Show that $FACTOR \xrightarrow{p} DIV$.

(b) Show that $DIV \in \mathbf{NP} \cap \mathbf{coNP}$. For this part you may use the fact that the set of prime numbers is in P.