

COMP 314 Homework Assignment 9

1. (5 points) Let 5SAT be defined in the same way as 3SAT, but with clauses of up to 5 literals instead of 3. Is 5SAT NP-complete? Give a rigorous proof of your answer.
2. (5 points) Let EXACTLY3SAT be the same as 3SAT, except that each clause must have exactly 3 literals (instead of at most 3). Prove that EXACTLY3SAT is NP-complete.
3. (5 points) RSA is a popular public key encryption system. For its security, RSA relies on the fact that there is no known efficient way of computing a private RSA key from the corresponding public key. Let CRACKRSA be the problem that takes a public RSA key as input and outputs the corresponding private RSA key. It's not hard to show that CRACKRSA polyreduces to FACTOR. Based on these facts, discuss whether CRACKRSA is likely to be a member of Poly, NPoly, or NPHard. Explain your reasoning. (Detailed reductions are not required. Knowledge of how RSA works is not required. Just use the facts stated in the question.)
4. (16 points) For each of the problems given below:
 - (a) *circle* each complexity class the problem is *known* to be a *member* of; and
 - (b) *cross out* each complexity class the problem is *widely believed* to be *outside* of.

Problem	Complexity classes
FACTOR	P NP Poly NPoly NPComplete NPHard Exp
FACTORDECISION	P NP Poly NPoly NPComplete NPHard Exp
DIRECTEDHAMILTONCYCLE	P NP Poly NPoly NPComplete NPHard Exp
TRAVELINGSALESPERSONDECISION	P NP Poly NPoly NPComplete NPHard Exp
PRIMALITY	P NP Poly NPoly NPComplete NPHard Exp
3SATDECISION	P NP Poly NPoly NPComplete NPHard Exp
5SATDECISION	P NP Poly NPoly NPComplete NPHard Exp
2SATDECISION	P NP Poly NPoly NPComplete NPHard Exp

5. (5 points) Using some brief research (online sources are fine), describe an NP-complete problem that has not been mentioned in class or any homework assignment. Try to find a problem that is not closely related to any we have discussed. Cite your source(s).