

## COMP 314 Homework Assignment H

### Chapter 14

**Question H1.** (15 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-hard? Give a rigorous proof of your answer.

**Question H2.** (15 points) Let EXACTLY3SAT be the same as 3SAT, except that each clause must have exactly 3 literals (instead of at most 3). Prove that the decision version of EXACTLY3SAT, which we will call EXACTLY3SATD, is NP-complete.

**Question H3.** (15 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 as a solution. 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.)

[The assignment continues on the next page.]

**Question H4.** (16 points) For each of the problems given below:

- (a) List each complexity class the problem is *known* to be a *member* of.
- (b) List each complexity class the problem is *widely believed* to be *outside* of.

Note: In the list below, FACTOR and DHC are general problems, not decision problems. The other problems are all decision problems, as indicated by the name of the problem ending in “D”.

If it is easier for you, you can copy the table below then just circle the classes the problem is a member of, and cross out the classes it is believed to be outside of.

Problem	Complexity classes
FACTOR	P NP Poly NPoly NPComplete NPHard Exp
FACTORINRANGED	P NP Poly NPoly NPComplete NPHard Exp
DHC	P NP Poly NPoly NPComplete NPHard Exp
TSPD	P NP Poly NPoly NPComplete NPHard Exp
ISPRIMED	P NP Poly NPoly NPComplete NPHard Exp
3SATD	P NP Poly NPoly NPComplete NPHard Exp
5SATD	P NP Poly NPoly NPComplete NPHard Exp
2SATD	P NP Poly NPoly NPComplete NPHard Exp

**Question H5.** (15 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).

Total points on this assignment: 76