P vs. NP: Assignment 1

Dr. Holger Dell, Cornelius Brand, Marc Roth
https://www.holgerdell.com/teaching/2017/

The following exercises are intended as a warmup. We will talk about them at our next meeting.

Exercise 1.1 By May 5, register for the seminar online, and participate in the Doodle poll for the date of the next meeting. Before the next meeting, read the first four chapters of Aaronson's survey.

Definition 1.

(a) The complexity class NP_{TM} is defined as the set of languages $L \subseteq \{0,1\}^*$ recognized by **n**ondeterministic **p**olynomial-time **T**uring **M**achines. That is, $L \in \mathsf{NP}_{TM}$ if and only if there is a non-deterministic polynomial-time Turing machine M such that for all $x \in \{0,1\}^*$, $x \in L$ if and only if there is an accepting run of M on input x.

(b) The complexity class NP_{PV} is defined as the set of languages $L \subseteq \{0,1\}^*$ that have **p**olynomial-time **v**erifiers. That is, $L \in \mathsf{NP}_{PV}$ if and only if there is a deterministic polynomial-time Turing machine M and a polynomial p such that for all $x \in \{0,1\}^*$, $x \in L$ if and only if there is $y \in \{0,1\}^{p(|x|)}$ that makes $M(x,y)$ accept.

Exercise 1.2 (Verifiers vs. NTMs) Show that $\mathsf{NP}_{TM} = \mathsf{NP}_{PV}$.

Exercise 1.3 (Polynomial space)

(a) State a definition of PSPACE.

(b) Using your definition, prove that there is a PSPACE-complete problem.

Exercise 1.4 (The polynomial hierarchy)

(a) State a definition of the *polynomial hierarchy* PH, and of its *levels*. We say that the polynomial hierarchy *collapses* if PH is contained in one of its levels.

(b) Prove if there is a PH-complete problem, then PH collapses.

Exercise 1.5 (A PH-paradox)

(a) Prove PH $\subseteq$ PSPACE.

(b) Conclude that if PH $\supseteq$ PSPACE, then PH collapses.

(c) Do you think the converse holds? Argue informally.

Bonus: Explain why you find this at the same time confusing and beautiful.

Exercise 1.6 For a complexity class $\mathcal{C}$, we denote with co-$\mathcal{C}$ the class of complements of languages from $\mathcal{C}$. The problem Factoring is defined as the set of (encodings of) pairs of natural numbers (N, t) such that N contains a factor less than t. The problem Primes is defined as the set of (encodings of) prime numbers. You may use that Primes $\in$ P holds.

(a) Prove that if there is a problem that is NP-complete and contained in co-NP, then PH collapses.

(b) Prove that Factoring is not NP-complete unless PH collapses.

Exercise 1.7 Assume you have an algorithm that decides whether a given instance of SAT of size N has a satisfying assignment in deterministic polynomial time. Give an algorithm that constructs such a satisfying assignment (if one exists) in deterministic polynomial time.