

## Exercise X

### Problem 1

Consider the following decision problems and show that these problems are in  $\text{NP} \cap \text{coNP}$ . What could be the difference between them?

- a) Given an undirected bipartite graph  $G$ , does  $G$  have a perfect matching? Hint: One can use the “Marriage Theorem”.
- b) Given  $n, k \in \mathbb{N}$  (in binary encoding), is there an  $m \in \{2, \dots, k\}$  such that  $m|n$ ? (I.e., does  $n$  have a factor of size at most  $k$ ?) Hint: Use  $\text{PRIMES} \in \text{P}$ .

### Problem 2

The Completeness Theorem states “ $\Delta \models \Phi \iff \Delta \vdash \Phi$ ”. In particular, all valid sentences can be proven. However, the length of such a proof is not considered.

Recall the satisfiability problem SAT: Given a Boolean expression  $\Phi$  in conjunctive normal form, is there a truth assignment satisfying  $\Phi$ ?

We want to show: There is no polynomial  $p$  such that every valid sentence with  $n$  letters has a proof with at most  $p(n)$  letters, unless  $\text{SAT} \in \text{NP} \cap \text{coNP}$ . (Note that this would imply  $\text{NP} = \text{coNP}$ , because SAT is NP-complete.)

Your task: Find a set of axioms and a first-order logic sentence for an instance of SAT such that the sentence is a valid consequence of the given axioms if  $\Phi$  is satisfiable. If  $\Phi$  is unsatisfiable the sentence should also be unsatisfiable for the given axioms. (It might be convenient to choose a system of axioms that allows only models with exactly two elements.) Then consider a non-deterministic Turing machine that “guesses” proofs for this axiomatic system. What effect does it have on the complexity of SAT if there are polynomial-size proofs for all valid sentences?