Lecturer: Thomas Rothvoss Due date: Friday, Jan 26, 2024, 11pm, on GradeScope

Problem Set 3

CSE 531 - Computational Complexity

Winter 2024

Exercise 2.5 (slightly modified from Arora and Barak; 10pts)
Let $\texttt{PRIMES} := \{\text{enc}(n) \mid n \in \mathbb{N} \text{ is prime number}\}$[1] be the language of all prime numbers. Prove that $\texttt{PRIMES} \in \mathbf{NP}$.
Hint. You may use the following fact without a proof.

> **Pratt certificate.** Let $n \in \mathbb{Z}_{\geq 3}$. Then n is prime if and only if there exists a number $a \in \{2, \ldots, n-1\}$ so that[2] $a^{n-1} \equiv_n 1$ and for every prime factor q of $n-1$ one has $a^{(n-1)/q} \not\equiv_n 1$.

To certify that n is prime, certify that the condition after the "if and only if" holds where you'll need a recursive argument to certify that any q is prime too. Prove that your certificate has length that is polynomial in $|\text{enc}(n)|$ and can be verified in time polynomial in $|\text{enc}(n)|$.
Remark. Actually it is true that $\texttt{PRIMES} \in \mathbf{P}$, but that proof takes more work. From this exercise we can derive that $\texttt{PRIMES} \in \mathbf{NP} \cap \mathbf{coNP}$ which already is good evidence that PRIMES is not a hard problem.

Exercise 2.17 (modified from Arora and Barak; 10pts)
Define the *Exactly One 3SAT* problem

$$\texttt{E1-3SAT} := \left\{ \psi \mid \begin{array}{c} \psi \text{ is a CNF with at most 3 literals per clause}^3 \text{ that has an} \\ \text{assignment } x \text{ that satisfies exactly one literal per clause} \end{array} \right\}$$

Prove that E1-SAT is **NP**-complete.
Hint. Prove $\texttt{3SAT} \leq_p \texttt{E1-3SAT}$. To do so, replace each occurance of a literal u_i in a clause C by a new variable $z_{i,C}$ and introduce new clauses and auxiliary variables ensuring that if u_i is TRUE, then $z_{i,C}$ is allowed to be either TRUE or FALSE, but if u_i is FALSE, then $z_{i,C}$ must be FALSE too.

[1] For a number n we write $\text{enc}(n) \in \{0,1\}^*$ as the encoding of n as a 0/1-string
[2] We write $a \equiv_n b$, if $a - b$ is an integer multiple of n.