MCS 541 – Computational Complexity

Spring 2023

Problem Set 6[*]

Lev Reyzin

Due: 4/28/23 at the beginning of class

1. Prove that if one-way functions exist, then $\mathbf{P} \neq \mathbf{NP}$.

2. Prove that a one-time pad (strongly) satisfies computational security, i.e. that for every function A, if $(\mathtt{E}, \mathtt{D})$ denotes the one-time pad encryption then

$$\Pr_{k \in_R \{0,1\}^n, x \in_R \{0,1\}^n}[A(\mathtt{E}_k(x)) = (i, b) \text{ s.t. } x_i = b] \leq 1/2.$$

3. Prove that any language that has a **PCP** verifier using r coins and q adaptive queries also has a nonadaptive verifier using r coins and 2^q queries.

4. Prove that $\mathbf{PCP}(0, \mathrm{poly}(n)) = \mathbf{NP}$.

[*] Many of these problems are modifications of exercises that appear in Arora-Barak.