Homework 3 (30 points total)

Due on Friday, 10:20 am, 9 June 2023 (112/06/09)

Question 1 (5 points). Let $\mathcal{H}_{n,k}$ be a pairwise independent collection of hash functions $h : \{0,1\} \to \{0,1\}^k$. Prove that for every $x \in \{0,1\}^n$, for every $y \in \{0,1\}^k$:

$$\mathbf{Pr}_{h\in\mathcal{H}_{n,k}}[\ h(x) = y\ ] \ = \ 2^{-k}$$

Question 2 (5 points) Describe an IP protocol for NON-SQ.
Recall that $\mathsf{NON\text{-}SQ} \stackrel{\mathsf{def}}{=} \{(a, n) \mid a \not\equiv b^2 \pmod{n} \text{ for every integer } b\}$. Here a and n are integers written in binary representation.

Question 3 (5 points) Using Theorem 12.1, prove that $\mathbf{PH} \subseteq \mathbf{IP}$.
Here you should describe an IP protocol for each language $L \in \mathbf{PH}$. You may use the algorithms in Notes 9 and 10 and the IP protocol for $L_{\sharp\mathsf{SAT}}$ as a black box, but you may not use Theorem 12.3.

Question 4 (5 points). Prove that if $\mathbf{PSPACE} \subseteq \mathbf{P}_{/\mathsf{poly}}$, then $\mathbf{PSPACE} = \mathbf{MA}$.
Note: You can assume in an interactive proof, the prover is a polynomial space Turing machine.

Question 5 (5 points). Prove that $\mathbf{MA} \subseteq \mathbf{\Sigma}_2^p$. Is $\mathbf{MA} \subseteq \mathbf{\Pi}_2^p$? Let me know your opinion.

Question 6 (5 points). Prove that $\mathbf{AM} \subseteq \mathbf{\Sigma}_3^p$. Is $\mathbf{AM} \subseteq \mathbf{\Pi}_3^p$? Let me know your opinion.