Lecturer: Thomas Rothvoss Due date: Friday, Mar 8, 2024, 11pm, on GradeScope

Problem Set 8

CSE 531 - Computational Complexity

Winter 2024

Preliminaries. A language $L \subseteq \{0,1\}^*$ is in the class **MIP** if it admits an interactive proof with *multiple* provers. More formally we have $m+1$ parties with one *verifier* V which is a probabilistic polynomial time Turing machine and m provers $P_1,\dots,P_m$ which have unlimited computational power. All parties see the input $x \in \{0,1\}^*$; only the verifier sees the random bits r. W.l.o.g. in each round i, the verifier V sends message $a_{ij} \in \{0,1\}^*$ to prover P_j. Then (without seeing the messages send to the other provers) prover P_j sends the answer b_{ij}. After some number k of rounds the verifier decides whether to accept or reject. Here k and m may depend (polynomially) on the input length and all messages need to have polynomial length. Then $L \in$ **MIP** if there is such a PTM V so that

$$\begin{aligned} x \in L \quad &\Rightarrow \quad \exists P_1,\dots,P_m : \Pr[out(V,P_1,\dots,P_m,x)=1] \geq \frac{2}{3} \\ x \notin L \quad &\Rightarrow \quad \forall P_1,\dots,P_m : \Pr[out(V,P_1,\dots,P_m,x)=1] \leq \frac{1}{3} \end{aligned}$$

where $out(V,P_1,\dots,P_m) \in \{0,1\}$ is the output of the verifier (which is a random variable depending on r). Note that in particular **IP** $\subseteq$ **MIP**. In fact, it is true that **MIP** $=$ **NEXP**; though in this homework we will be satisfied with proving two related facts.

Exercise 8.11 (from the book of Arora and Barak; 10pts)
Prove that **MIP** $\subseteq$ **NEXP**.

Exercise 8.12 (from the book of Arora and Barak; 10pts)
Let $\mathbf{MIP}_m$ be the class **MIP** where the number of provers is restricted to m. Prove that $\mathbf{MIP}_2 = \mathbf{MIP}_m$ for any $m := m(n) := \text{poly}(n)$ with $m \geq 2$.
Hint. We can simulate m provers with only 2 provers. One of the provers plays the role of all the m provers. The other prover is asked to simulate one of the provers, chosen randomly among the m provers. Then repeat this a few times.