CS 535: Complexity Theory, Fall 2020

Homework 9

Due: 2:00AM, Saturday, December 5, 2020.

Reminder. Homework must be typeset with LaTeX preferred. Make sure you understand the course collaboration and honesty policy before beginning this assignment. Collaboration is permitted, but you must write the solutions *by yourself without assistance*. You must also identify your collaborators. Assignments missing a collaboration statement will not be accepted. Getting solutions from outside sources such as the Web or students not enrolled in the class is strictly forbidden.

Problem 1 (Perfect Interactive Proofs)**.** For parameters $c, s \geq 0$, define the class $\mathbf{MA}_{c,s}$ to consist of Merlin-Arthur interactive proofs with completeness probability c and soundness probability s. That is, a language $L \in \mathbf{MA}_{c,s}$ if there exists a probabilistic poly-time verifier V and a polynomial $m(n)$ such that

$$x \in L \implies \exists u \in \{0,1\}^{m(n)} \ \Pr[V(x,u) = 1] \geq c$$
$$x \notin L \implies \forall u \in \{0,1\}^{m(n)} \ \Pr[V(x,u) = 1] \leq s.$$

Recall that in class we defined $\mathbf{MA} = \mathbf{MA}_{2/3,1/3}$.

(a) Prove that $\mathbf{MA}_{1,1/3} = \mathbf{MA}$. That is, we may assume Merlin-Arthur proofs have perfect completeness probability. Hint: Modify the proof of the Sipser-Gács Theorem (Theorem 7.15). (6 points)

(b) Prove that $\mathbf{MA}_{2/3,0} = \mathbf{NP}$. That is, Merlin-Arthur proofs with perfect soundness are no more powerful than deterministic proofs. (4 points)

(c) *Bonus* Prove the same relationships for general interactive proofs. That is, show that $\mathbf{IP}_{1,1/3} = \mathbf{IP}$ and $\mathbf{IP}_{2/3,0} = \mathbf{NP}$.

Problem 2 (Counting k-Colorings)**.** Let $G = ([n], E)$ be a graph on n vertices. A k-coloring of G is a vector of colors $(c_1, \ldots, c_n) \in [k]^n$ such that for every edge $(i,j) \in E$, we have $c_i \neq c_j$.

(a) Show that there is a rational polynomial p of degree $\mathrm{poly}(k, n)$ such that the number of k-colorings of a graph G is given by

$$\sum_{c_1=1}^{k} \sum_{c_2=1}^{k} \cdots \sum_{c_n=1}^{k} p(c_1, \ldots, c_n).$$

Hint: `https://en.wikipedia.org/wiki/Lagrange_polynomial`. (4 points)

(b) Modify the sumcheck protocol to show that for every constant k, the language $\#\mathsf{kCOL_D} = \{\langle G, t\rangle \mid G \text{ has exactly } t \text{ } k\text{-colorings}\} \in \mathbf{IP}$. (6 points)