CS 535: Complexity Theory, Fall 2023

Homework 9

Due: 11:59PM, Tuesday, December 5, 2023.

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 (Circuit Lower Bounds from Derandomization)**.** Many complexity theorists believe that **BPP** = **P**, but we're quite far from proving this. A necessary condition to get to this point would be to derandomize the **coRP** polynomial identity testing problem, defined as follows:

$$\mathsf{PIT}_{\mathbb{Z}} = \{C \mid \text{ Arithmetic circuit } C \text{ computes the zero polynomial over } \mathbb{Z}\}.$$

In this problem, you'll show that even the weak derandomization $\mathsf{PIT}_{\mathbb{Z}} \in \mathbf{NP}$ would yield much stronger circuit lower bounds than what are currently known, either for Boolean circuits computing languages in **NEXP**, or for arithmetic circuits computing the matrix permanent.

(a) Show that if $X \in \{0,1\}^{n\times n}$, then

$$\operatorname{perm}(X) = \sum_{i=1}^{n} x_{1,i} \operatorname{perm}(X_{1,i}).$$

Here, $x_{1,i}$ is the entry in the first row and i'th column of X, and $X_{1,i}$ is the submatrix obtained by deleting the first row and the i'th column of X. (2 points)

(b) Part (a) shows that the matrix permanent is downward self-reducible. This has the following useful consequence for *verifying* that a circuit C computes the permanent. An arithmetic circuit $C : \{0,1\}^{n\times n} \to \{0,1\}$ computes the $n \times n$ matrix permanent if and only if, for every $k = 1, \ldots, n$, we have $\tilde{C}_k(X) := C(X \mid I_{n-k}) - \sum_{i=1}^{k} x_{1,k} C(X_{1,k} \mid I_{n-k+1}) \equiv 0$, as integer polynomials over $X_{1,1}, \ldots, X_{k,k}$, where I_{n-k} is the $(n-k)\times(n-k)$ identity matrix and

$$(X \mid I_{n-k}) := \begin{pmatrix} X & 0 \\ 0 & I_{n-k} \end{pmatrix}.$$

That is, given an arithmetic circuit C on n^2 variables, one can efficiently compute a sequence of arithmetic circuits $\tilde{C}_1, \ldots, \tilde{C}_n$ such that C computes the $(n \times n)$ 0/1-permanent if and only if $\tilde{C}_1, \ldots, \tilde{C}_n \in \mathsf{PIT}_{\mathbb{Z}}$,

Use the discussion above to show that if $\mathsf{PIT}_{\mathbb{Z}} \in \mathbf{NP}$ and the 0/1 matrix permanent is computed by polynomial size arithmetic circuits, then $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{NP}$. (3 points)

(c) (*Individual Review*: No collaboration allowed on this part only) Show that if $\mathbf{NE} := \mathbf{NTIME}(2^{O(n)}) \subseteq \mathbf{P}_{/\mathbf{poly}}$, then there exists a constant c such that $\mathbf{NP} \subseteq \mathbf{SIZE}(n^c)$. Hint: You can use without proof the fact that every problem in $\mathbf{NP}$ reduces to $\mathsf{NESAT} = \{\langle M, x, t\rangle \mid$ Deterministic TM accepts x within t steps$\}$ in <u>linear</u> time. (3 points)

(d) Show that the following three statements <u>cannot</u> simultaneously be true:

- $\mathsf{PIT}_{\mathbb{Z}} \in \mathbf{NP}$
- The 0/1 matrix permanent has poly-size arithmetic circuits
- $\mathbf{NE} \subseteq \mathbf{P}_{/\mathbf{poly}}$.

Hint: Use the result of Homework 7, Problem 1(c). (3 points)

Problem 2 (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

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

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-Lautemann Theorem (Theorem 7.15). You can use the statements of Claims 1 and 2 from that proof in your solution without reproving them. (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. (3 points)

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

The following problems didn't make the cut for this assignment, but are nevertheless useful to think about!

Problem 3. (Bonus) Prove that $\oplus\mathbf{P}^{\oplus\mathbf{P}} = \oplus\mathbf{P}$.

Problem 4 (Bonus: 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 polynomial p with degree $\text{poly}(k, n)$ and rational coefficients 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`.

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