Problem Set 5

- Due Date: **8 May (Tue), 2018**
- If you submit handwritten solutions, start each problem on a fresh page.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring sources other than the lectures and the text-book is strongly discouraged. But if you do use an outside source (eg., other text books, lecture notes, any material available online), acknowledge the same in your writeup. This will not affect your grades.
- The points for each problem are indicated on the side.
- If you don't know the answer to a problem, then just don't answer it. Do not try to convince yourself or others into believing a false proof.
- Be clear in your writing.

---

1. **[2-sided versus 1-sided error for MA and AM.]** (10+10)

   In the characterizations below, y, z, y', z' are all strings whose length is polynomial in $|x|$.

   (a) Recall that a language L is in **MA** if there is a language R in **P** for which:

   $$\begin{aligned} x \in L &\Rightarrow \exists y \text{ for which } \Pr_z[(x,y,z) \in R] \geq 2/3, \text{ and} \\ x \notin L &\Rightarrow \forall y \ \Pr_z[(x,y,z) \in R] \leq 1/3. \end{aligned}$$

   Prove that for every such language L, there is a language R' in **P** for which:

   $$\begin{aligned} x \in L &\Rightarrow \exists y' \text{ for which } \Pr_{z'}[(x,y',z') \in R'] = 1, \text{ and} \\ x \notin L &\Rightarrow \forall y' \ \Pr_{z'}[(x,y',z') \in R'] \leq 1/3. \end{aligned}$$

   (b) Recall that a language L is in **AM** if there is a language R in **P** for which:

   $$\begin{aligned} x \in L &\Rightarrow \Pr_y[\exists z \text{ for which } (x,y,z) \in R] \geq 2/3, \text{ and} \\ x \notin L &\Rightarrow \Pr_y[\exists z \ (x,y,z) \in R] \leq 1/3. \end{aligned}$$

   Prove that for every such language L, there is a language R' in **P** for which:

   $$\begin{aligned} x \in L &\Rightarrow \Pr_{y'}[\exists z' \text{ for which } (x,y',z') \in R'] = 1, \text{ and} \\ x \notin L &\Rightarrow \Pr_{y'}[\exists z' \ (x,y',z') \in R'] \leq 1/3. \end{aligned}$$

[Hint: For this problem you may want to recall strong error reduction for the purpose of proving $\mathbf{BPP} \subseteq \mathbf{\Sigma_2^P} \cap \mathbf{\Pi_2^P}$. For both parts, use a similar strong error reduction, and then allow Merlin to pick half of Arthur's random string.]

2. **[Round reduction for AM[k]]** (3+9+5+3)

Let $\mathbf{prAM}[k]$ be the promise problem version of $\mathbf{AM}[k]$ (i.e, it has the same completeness and soundness properties for the YES and NO instances as $\mathbf{AM}[k]$, but the YES and NO instances do not partition the universe (there could be "don't care" instances)).

For a class $\mathbf{C}$ of promise problems, we define $\mathbf{pr\Sigma} \cdot \mathbf{C}$ to be the class of promise problems Π such that there exists a promise problem $\Pi' \in \mathbf{C}$ and a polynomial p for which

$$\begin{aligned} x \in \Pi_Y &\Rightarrow \exists y \in \{0,1\}^{p(n)} (x,y) \in \Pi'_Y \\ x \in \Pi_N &\Rightarrow \forall y \in \{0,1\}^{p(n)} (x,y) \in \Pi'_N \end{aligned}$$

Similarly, we define $\mathbf{prBP} \cdot \mathbf{C}$ to be the class of promise problems Π such that there exists a promise problem $\Pi' \in \mathbf{C}$ and a polynomial p for which

$$\begin{aligned} x \in \Pi_Y &\Rightarrow \Pr_{y \in \{0,1\}^{p(n)}} [(x,y) \in \Pi'_Y] \geq 2/3 \\ x \in \Pi_N &\Rightarrow \Pr_{y \in \{0,1\}^{p(n)}} [(x,y) \in \Pi'_N] \geq 2/3 \end{aligned}$$

(a) Show that for every integer $k \geq 1$, $\mathbf{prMA}[k] = \mathbf{pr\Sigma} \cdot \mathbf{prAM}[k-1]$ and $\mathbf{prAM}[k] = \mathbf{prBP} \cdot \mathbf{prMA}[k-1]$, where $\mathbf{prMA}[0] = \mathbf{prAM}[0] = \mathbf{prP}$ (by definition).

(b) Prove that for any class $\mathbf{C}$ of promise problems, $\mathbf{pr\Sigma} \cdot \mathbf{prBP} \cdot \mathbf{C} \subseteq \mathbf{prBP} \cdot \mathbf{pr\Sigma} \cdot \mathbf{C}$.

(c) Prove that for all $k \geq 2$, $\mathbf{prAM}[k] = \mathbf{prAM}$. Conclude that $\mathbf{AM}[k] = \mathbf{AM}$.

(d) Where in the above parts was it important that we were working with promise problems?

[Hint: (b) First do error reduction and then show that interchanging $\mathbf{prBP}$ and $\mathbf{pr\Sigma}$ does not change the language.]

3. **[If GI is NP-complete, ...]** (10+10+5)

In class, we used round-reduction of $\mathbf{AM}$ to show that graph-isomorphism is not $\mathbf{NP}$-complete unless the hierarchy collapses to the second level. In this problem, we will give another proof of the same fact.

Recall the definition of complexity classes with advice. In this problem, we will need the classes $\mathbf{NP}/\text{poly}$ and $\mathbf{coNP}/\text{poly}$. A language L is said to be in $\mathbf{NP}/\text{poly}$ if there exists polynomials p, q, r, a sequence of advice strings $\{a_i\}_{i=1}^{\infty}$ such that $|a_i| \leq p(i), \forall i$, a $\mathbf{DTIME}(q(n))$-deterministic Turing machine M, such that

$$x \in L \iff \exists y \in \{0,1\}^{r(|x|)}, \text{ such that } M(x, y, a_{|x|}) = 1.$$

$\mathbf{coNP}/\text{poly}$ is defined similarly with $\exists$ replaced by $\forall$ in the above statement.

(a) Show that $\mathbf{AM} \subset \mathbf{NP}/\text{poly}$.

(b) Show that $\mathbf{coNP} \subset \mathbf{NP}/\text{poly}$ implies $\mathbf{\Pi}_3^P = \mathbf{\Sigma}_3^P$.

(c) Conclude from the above that if graph isomorphism is $\mathbf{NP}$-complete, the polynomial hierarchy collapses to $\mathbf{\Sigma}_2^P$.

[Hint: (a) Use ideas similar to the proof of $\mathbf{BPP} \subset \mathbf{P}/\text{poly}$. (b) Use ideas similar to the proof of Karp-Lipton-Sipser theorem.]

4. **[three vs. two queries]** (10)

In class, we stated that Håstad and then Guruswami, Lewin, Sudan and Trevisan proved the following strengthening of the PCP Theorem which shows that every language in NP has a PCP with 3 queries and soundness error almost 1/2.

$$[\text{Hås, GLST}] : \forall \varepsilon > 0, \mathsf{Circuit\text{-}SAT} \in PCP_{1,1/2+\varepsilon}[O(\log n), 3].$$

Suppose we were able to further strengthen the above result to prove that Circuit-SAT has a 2 query PCP (i.e., Circuit-SAT $\in PCP_{1,s}[O(\log n), 2]$ for some $0 < s < 1$), then show that $NP = P$.

Thus, Håstad's PCP is optimal with respect to the number of queries.

5. [**logarithmic randomness**] Problem 11.8 (12)

6. [**gap preserving reductions**] (13)

   A reduction from one gap problem gap-A_α to gap-B_β (for some $0 < \alpha, \beta < 1$) is said to be a gap preserving reduction if it maps YES instances of gap-A_α to YES instances of gap-B_β and NO instances of gap-A_α to NO instances of gap-B_β. The existence of a gap preserving reduction from gap-A_α to gap-B_β implies that if it is NP-hard to approximate problem A to within α, then it is NP-hard to approximate problem B to within β.

   For every $\alpha > 7/8$, show that there exists $\varepsilon, \beta > 0$ and a gap preserving reduction from gap-$3\mathrm{SAT}_\alpha$ to gap-$2\mathrm{SAT}_{1-\varepsilon,\beta}$. Hence, conclude that there exists a $\gamma \in (0, 1)$ such that approximating MAX2SAT to within γ is NP-hard.

   Note:The gap problems gap-$3\mathrm{SAT}_\alpha$ and gap-$2\mathrm{SAT}_{1-\varepsilon,\beta}$ are defined as follows.
   gap-$3\mathrm{SAT}_\alpha$:

   $$\begin{aligned} \mathsf{YES} &= \{\varphi | \varphi \text{ is a satisfiable 3CNF formula}\} \\ \mathsf{NO} &= \{\varphi | \varphi \text{ is a 3CNF formula such that no assignment satisfies more than } \alpha \text{ fraction of the clauses}\} \end{aligned}$$

   gap-$2\mathrm{SAT}_{1-\varepsilon,\beta}$:

   $$\begin{aligned} \mathsf{YES} &= \{\varphi | \varphi \text{ is a 2CNF formula with an assignment that satsifies at least } (1-\varepsilon)\text{-fraction of the clauses}\} \\ \mathsf{NO} &= \{\varphi | \varphi \text{ is a 2CNF formula such that no assignment satisfies more than } \beta \text{ fraction of the clauses}\} \end{aligned}$$