Complexité avancée - TD 9

Simon Halfon

November 16, 2016

Definition 1 *Recall that* $\mathsf{AM}[f]$ *for a proper function* f *denotes the class of languages* L *such that for any* $\ell \geq 0$*, there exists a game of Arthur and Merlin* (M, A, D) *such that for any* x *of size* n*, letting prot* $= (AM)^{f(n)}$*:*

1. *Completeness: if* $x \in L$ *then* $prot[A, M]_D = \top$ *with probability at least* $1 - 1/2^{n^\ell}$
2. *Soundness: if* $x \notin L$ *then for any Merlin's function* M'*,* $prot[A, M']_D = \bot$ *with probability at least* $1 - 1/2^{n^\ell}$

Exercise 1: Arthur-Merlin protocols

Prove the following statements, directly from definition of Arthur-Merlin games:

- $\mathsf{M} = \mathsf{NP}$;
- $\mathsf{A} = \mathsf{BPP}$;
- $\mathsf{NP}^{\mathsf{BPP}} \subseteq \mathsf{MA}$;
- $\mathsf{AM} \subseteq \mathsf{BPP}^{\mathsf{NP}}$.

Exercise 2: Collapse of the Arthur-Merlin hierarchy

Recall that, for each $\Pi \in \{A, M\}^*$, the class $\mathbf{\Pi}$ is the class of languages recognized by Arthur-Merlin games with protocol Π.

(a) Without using any result about the collapse of the Arthur-Merlin hierarchy, prove that for all $\Pi_0, \Pi_1, \Pi_2 \in \{A, M\}^*$, we have $\mathbf{\Pi_1} \subseteq \mathbf{\Pi_0 \Pi_1 \Pi_2}$.

(b) Now assume the fact that for all $\Pi \in \{A, M\}^*$, one has $\mathbf{\Pi} \subseteq \mathsf{AM}$. Prove the following statement: For all $\Pi \in \{A, M\}^*$ such that Π has a strict alternation of symbols, and $|\Pi| > 2$, we have $\mathbf{\Pi} = \mathsf{AM}$.

Exercise 3: The BP operator

We say that a language B reduces to language C under a randomized polynomial time reduction, denoted $B \leq_r C$, if there is a probabilistic polynomial-time Turing machine such that for every x, $Pr[C(M(x)) = B(x)] \geq \frac{2}{3}$.

1. Show that $\mathsf{BP} \cdot \mathcal{C} = \{L \mid L \leq_r L',\ \text{for some } L' \in \mathcal{C}\}$
2. Show that BPP is closed under randomized polynomial time reduction.
3. Deduce that $\mathsf{BP} \cdot (\mathsf{BP} \cdot \mathcal{C}) = \mathsf{BP} \cdot \mathcal{C}$.

Exercise 4: The class $\mathsf{BP} \cdot \mathsf{NP}$

1. Show that $\mathsf{BP} \cdot \mathsf{P} = \mathsf{BPP}$
2. Show that $\mathsf{BP} \cdot \mathsf{NP} = \mathsf{AM}$
3. Show that $\mathsf{BP} \cdot \mathsf{NP} \subseteq \mathsf{NP}/poly$
4. Show that $\mathsf{BP} \cdot \mathsf{NP} \subseteq \Sigma_3^P$ (give a direct proof, do not use $\mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$).
5. Show that if $\overline{\mathbf{3SAT}} \leq_r \mathbf{3SAT}$ then PH collapses to the third level.

Exercise 5: One Merlin to rule them all

Show that the following definition of AM if actually equivalent to the one given in introduction: $L \in \mathsf{AM}$ iff for any $\ell \geq 0$, there exists an Arthur A and a polynomial-time-checkable predicate D such that for any x of size n, letting $prot = (AM)^{f(n)}$:

1. Completeness: if $x \in L$ then there exists some Merlin M such that $prot[A, M]_D = \top$ with probability at least $1 - 1/2^{n^\ell}$
2. Soundness: if $x \notin L$ then for any Merlin M', $prot[A, M']_D = \bot$ with probability at least $1 - 1/2^{n^\ell}$

Exercise 6: Unreliable Merlin

Show that allowing Merlin to use randomness (in a private manner) does not change the class AM.