Complexité avancée - TD 10

Rémy Poulain

27 novembre 2019

Exercise 0 : BPP and oracle machines

Prove that $\mathsf{P}^{\mathsf{BPP}} = \mathsf{BPP}$.

Exercise 1 : Probabilistic Logarithmic Space

Propose a definition of RSPACE.

Let $\mathsf{RL} = \bigcup_{k\in\mathbb{N}} \mathsf{RSPACE}(k \cdot log(n), \infty, 0, 1/2)$ be the class of languages that can be decided in probabilistic logarithmic space (the machine does not necessarily halt).

Show that :

1. For L in RL and M a PTM which decides L , If $x \notin L$, then $\forall r$, $M(x, r) \neq \top$
2. $\mathsf{RL} \subseteq \mathsf{NL}$
3. $\mathsf{RL} \subseteq \mathsf{RP}$

Exercise 2 : BPP-completeness

1. Show that the language $L = \{(M, x, 1^t) \mid M$ accepts on input x in time at most $t\}$, where M is the code of a non-deterministic Turing machine, x an input of M and t a natural number, is NP-complete.
2. Let L be the language of words $(M, x, 1^t)$ where M designates the encoding of a probabilistic Turing machine and x a string on $M's$ alphabet such that M accepts x in at most t steps, for at least $2/3$ of the possible random tapes of size t.

   Is L BPP-hard ? Is it in BPP ?

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 3 : Arthur-Merlin protocols

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

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

Exercise 4 : 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 5 : 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, $Pr[C(M(x)) = B(x)] \geq \frac{2}{3}$.

Remember the definition of $\mathsf{BP} \cdot \mathcal{C}$:

$L \in \mathsf{BP} \cdot \mathcal{C}$ iff exists A a PTM polynomial and a language D polynomial s.t. for all input x

— if $x \in L$ then $Pr[A(x, r) \in D] \geq \frac{2}{3}$

— if $x \notin L$ then $Pr[A(x, r) \notin D] \geq \frac{2}{3}$

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

Exercise 5 (bonus) : 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 8 (bonus) : Unreliable Merlin

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