Complexité avancée - TD 8

Benjamin Bordais

December 02, 2020

We recall the definition of the Arthur-Merlin hierarchy.

Definition 1 *An* Arthur and Merlin triplet *is the data of* $(M, \mathcal{A}, D)$ *where* M *is a Merlin function, that is a function with the size of the output polynomial in the size of the input, possibly not computable, a randomized Turing machine* $\mathcal{A}$ *running in polynomial time and a language* $D \in \mathsf{P}$. *Then, for all* $w \in \{\mathsf{A}, \mathsf{M}\}^*$, *let us denote by* k *the number of times* A *appears in the word* w. *We consider the following algorithm induced by the word* w *(with* $n = |w|$ *and* $r_1, \ldots, r_k$ k *random tapes of size polynomial in* n*).*

$prot_w(M; x, r_1, \ldots, r_k)$:
imp = x
i = 0
for *j = 1, ..., n:*
  if w_j = A ***then*** *(i = i+1,* $q_j = \mathcal{A}(imp, r_i)$*; imp = imp #* r_i *#* q_j*)*
  else *(*$y_j = M(imp)$*; imp := imp #* y_j*)*
accept if *(imp* $\in$ *D),* ***else reject***

We denote $prot[\mathcal{A}, M]_D(x, r_1, \ldots, r_k) = \top$ *if the previous algorithm accepts, otherwise* $prot[\mathcal{A}, M]_D(x, r_1, \ldots, r_k) = \bot$.

Now, $\mathsf{AM}[f]$ *for a proper function* f *denotes the class of languages* L *such that for any polynom* q, *there exists an Arthur and Merlin triplet* $(M, \mathcal{A}, D)$ *such that for any* x *of size* n, *letting* $w \in \{\mathsf{A}, \mathsf{M}\}^{f(n)}$:

1. *Completeness: if* $x \in L$ *then* $Pr[prot_w[\mathcal{A}, M]_D(x, r_1, \ldots, r_k) = \top] \geq 1 - 1/2^{q(n)}$
2. *Soundness: if* $x \notin L$ *then for any Merlin's function* M', $Pr[prot_w[\mathcal{A}, M']_D(x, r_1, \ldots, r_k) = \bot] \geq 1 - 1/2^{q(n)}$

Exercise 1 Another way to see **MA** and **AM**

Prove the following with a definition of the Arthur-Merlin hierarchy with a bound on the probability set to 2/3 and 1/3:

- A language $L \in \mathbf{AM}$ if and only if there exists a language $D \in \mathsf{P}$ and a polynom p such that:
  - $x \in L \Rightarrow Pr_{r \in \{0,1\}^{p(|x|)}}[\exists y \in \{0,1\}^{p(|x|)},\ (x, r, y) \in D] \geq 2/3$
  - $x \notin L \Rightarrow Pr_{r \in \{0,1\}^{p(|x|)}}[\exists y \in \{0,1\}^{p(|x|)},\ (x, r, y) \in D] \leq 1/3$
- A language $L \in \mathbf{MA}$ if and only if there exists a language $D \in \mathsf{P}$ and a polynom p such that:
  - $x \in L \Rightarrow \exists y \in \{0,1\}^{p(|x|)},\ Pr_{r \in \{0,1\}^{p(|x|)}}[(x, r, y) \in D] \geq 2/3$

– $x \notin L \Rightarrow \forall y \in \{0,1\}^{p(|x|)},\ Pr_{r\in\{0,1\}^{p(|x|)}}[(x,r,y) \in D] \leq 1/3$

Exercise 2 Arthur-Merlin protocols

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

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

Exercise 3 Collapse of the Arthur-Merlin hierarchy

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

(a) Without using any result about the collapse of the Arthur-Merlin hierarchy, prove that for all $w_0, w_1, w_2 \in \{\mathbf{A}, \mathbf{M}\}^*$, we have $\mathbf{w_1} \subseteq \mathbf{w_0 w_1 w_2}$.

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

Exercise 4 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 $\mathcal{M}$ such that for every x, $Pr[\mathcal{M}(x) \in C \Leftrightarrow x \in B] \geq \frac{2}{3}$.

Recall the definition of $\mathsf{BP}\cdot\mathcal{C}$: $L \in \mathsf{BP}\cdot\mathcal{C}$ iff there exists a probabilistic Turing machine A running in polynomial time and a language $D \in \mathcal{C}$ 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 $\mathsf{co}(\mathsf{BP} \cdot \mathcal{C}) = \mathsf{BP} \cdot \mathsf{co}(\mathcal{C})$ and if $\mathcal{C} \subseteq \mathcal{C}'$, then $\mathsf{BP} \cdot \mathcal{C} \subseteq \mathsf{BP} \cdot \mathcal{C}'$
3. Show that BPP is closed under randomized polynomial time reduction.
4. Give a criterion on $\mathcal{C}$ so that: $\mathsf{BP} \cdot (\mathsf{BP} \cdot \mathcal{C}) = \mathsf{BP} \cdot \mathcal{C}$.

The class $\mathsf{BP} \cdot \mathsf{NP}$

1. Show that $\mathsf{BP} \cdot \mathsf{P} = \mathsf{BPP}$
2. Recall the proof that $\mathsf{BP} \cdot \mathsf{NP} = \mathbf{AM}$
3. Show that $\mathsf{BP} \cdot \mathsf{NP} = \{L \mid L \leq_r \mathsf{SAT}\}$
4. Show that $\mathsf{BP} \cdot \mathsf{NP} \subseteq \Sigma_3^P$ (with a direct proof)

5. (bonus) Show that if $\overline{\mathsf{3SAT}} \leq_r \mathsf{3SAT}$ then PH collapses to the third level.

Exercise 5 The PP class

The first 3 questions were already there in the last TD. Only question 4 is new.

The class PP is the class of languages L for which there exists a polynomial time probabilistic Turing machine M such that:

- if $x \in L$ then $Pr[M(x,r)$ accepts $] > \frac{1}{2}$
- if $x \notin L$ then $Pr[M(x,r)$ accepts $] \leq \frac{1}{2}$

Also define $\mathsf{PP}_<$ as the class of languages L for which there exists a polynomial time probabilistic Turing machine M such that:

- if $x \in L$ then $Pr[M(x,r)$ accepts $] > \frac{1}{2}$
- if $x \notin L$ then $Pr[M(x,r)$ accepts $] < \frac{1}{2}$

1. Show that $\mathsf{BPP} \subseteq \mathsf{PP}$ and $\mathsf{NP} \subseteq \mathsf{PP}$;
2. Show that $\mathsf{PP} = \mathsf{PP}_<$ and that PP is closed under complement;
3. Consider the decision problem MAJSAT:
   (a) Input: a boolean formula ϕ on n variables
   (b) Output: the (strict) majority of the 2^n valuations satisfy ϕ.

   Show that $\mathsf{MAJSAT} \in \mathsf{PP}$. In fact, MAJSAT is PP-complete.

   One may also consider the decision problem MAXSAT:
   (a) Input: a boolean formula ϕ on n variables, a number K
   (b) Output: more than K valuations satisfy ϕ.

   Show that MAXSAT is also PP-complete (to prove that $\mathsf{MAXSAT} \in \mathsf{PP}$ one may reduce MAXSAT to MAJSAT).
4. Show that $\mathbf{MA} \subseteq \mathsf{PP}$.