Complexité avancée - TD 7

Benjamin Bordais

November 25, 2020

Exercise 1 RP*

We define RP* as the class of all languages L for which there exists a probabilistic Turing machine M running in polynomial time, such that:

- If $x \in L$ then $Pr[M(x, r) \text{ reject}] < 1$
- If $x \notin L$ then $Pr[M(x, r) \text{ accept}] = 0$

Do you recognize this class?

Exercise 2 BPP and oracle machines

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

Exercise 3 BPP-completeness?

1. Show that the language $L = \{(M, x, 1^t) \mid M \text{ accepts on input } x \text{ in time at most } t\}$, 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 now 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 ?

Exercise 4 NP and randomized classes

Show that if $\mathsf{NP} \subseteq \mathsf{BPP}$ then $\mathsf{NP} = \mathsf{RP}$.
Hint: you may use the self-reducibility of SAT.

Exercise 5 The PP class

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

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

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).