Advanced Complexity Exam 2023-24

All written documents allowed. No Internet access, no cell phone. You can answer in French or in English. Every result you use must be properly cited (e.g., « by Shamir’s Theorem », or « by Question 4 », not « by a theorem of the lecture notes », not nothing either).

1 OMA

An oblivious Arthur-Merlin protocol is one where an honest Merlin can see the size of the history being presented to him, but not the history itself. A dishonest Merlin has access to the whole history. We will only look at the oblivious variants of MA and NP.

For every map \( err : \mathbb{N} \to [0, 1/2] \), the class \( \text{OMA}(err) \) (oblivious MA) is the class of languages \( L \) such that there is a family of words \( y_n, n \in \mathbb{N} \), of size equal to some polynomial \( p(n) \), and a language \( D \in \mathbb{P} \) such that for every input \( x \) (whose size is always written as \( n \)):

1. if \( x \in L \) then \( \Pr_r [x\#y_n\#r \in D] \geq 1 - err(n) \);
2. if \( x \notin L \) then for every word \( y \) of size equal to \( p(n) \), \( \Pr_r [x\#y\#r \in D] \leq err(n) \).

In other words, Merlin has to answer \( y_n \) when the input \( x \) has size \( n \), independently of what the value of \( x \) really is. Probabilities are taken over all random tapes \( r \) of some polynomial size \( q(n) \). The letter \# is a separator that does not appear in \( x, y_n, r \) or \( y \), which are all on the binary alphabet \( \Sigma \defeq \{0, 1\} \). We also say that \( L \) is decided by an \( \text{OMA}(err) \) protocol with language \( D \), witnesses \( y_n \), and sizes \( p(n), q(n) \).

When \( err \) is the constant function equal to \( \epsilon \in ]0, 1/2[ \), we write \( \text{OMA}(\epsilon) \) instead of \( \text{OMA}(err) \). The class OMA is defined as \( \text{OMA}(1/3) \).

The class ONP is the corresponding non-randomized variant : \( L \in \text{ONP} \) if and only if there is a family of words \( y_n, n \in \mathbb{N} \), of size equal to some polynomial \( p(n) \), and a language \( D \in \mathbb{P} \) such that for every input \( x \):

1. if \( x \in L \) then \( x\#y_n \in D \);
2. if \( x \notin L \) then for every word \( y \) of size equal to \( p(n) \), \( x\#y \notin D \).

It is clear that \( \text{ONP} \subseteq \text{OMA} \), and you don’t need to prove it.

**Question 1** (*) Show that \( \text{OMA} \subseteq \text{OMA}(1/2^g(n)) \) for any polynomial \( g(n) \geq 1 \). Explicitly, fix \( g(n) \), consider any \( L \in \text{OMA} = \text{OMA}(1/3) \), with \( y_n \) and \( D \) as above, and define a new polynomial-time decidable language \( D' \), and polynomial-sized words \( y'_n, n \in \mathbb{N} \) in place of \( D \) and \( y_n \) so as to decide \( L \) with error at most \( 1/2^g(n) \). (I am that explicit mostly in order to force you to use these notations, and to give me \( y'_n \) and \( D' \) explicitly.)

Hence \( \text{OMA} = \text{OMA}(1/2^g(n)) \) for every polynomial \( g(n) \geq 1 \) (no need to prove it).
Question 2 (*) Let \( L \) be decided by an \( \text{OMA}(1/2^{n+1}) \) protocol with language \( D \), witnesses \( y_n \), \( n \in \mathbb{N} \), and sizes \( p(n), q(n) \). Show that, for \( n \) large enough, there is a word \( r_n \) of size \( q(n) \) such that for every \( x \) (of size \( n \)), \( r_n \) makes no mistake on \( x \), meaning that:

- if \( x \in L \) then \( x \# y_n \# r_n \in D \);
- if \( x \notin L \) then for every word \( y \) of size equal to \( p(n) \), \( x \# y \# r_n \notin D \).

Question 3 (**) By imitating a theorem seen in class (give its name), show that \( \text{OMA} \subseteq \text{P/poly} \).

Question 4 (***) Show that, if \( \text{NP} \subseteq \text{P/poly} \), then \( \text{NP} \subseteq \text{ONP} \) (Imitate another theorem.)

Question 5 (*) Deduce that the following are equivalent:

(a) \( \text{NP} \subseteq \text{P/poly} \);
(b) \( \text{NP} \subseteq \text{ONP} \);
(c) \( \text{NP} \subseteq \text{OMA} \).

2 The Zachos Lemma

Let us recall the \( \text{BP} \cdot C \) operator from the lectures: for any complexity class \( C \), \( \text{BP} \cdot C \) is the class of languages \( L \) such that there is a randomized polynomial time Turing machine \( A' \) and a language \( D' \in C \) such that, on input \( x \) (of size \( n \)):

- If \( x \in L \), then \( \Pr_r[A'(x, r) \in D'] \geq 2/3 \);
- If \( x \notin L \), then \( \Pr_r[A'(x, r) \in D'] \leq 1/3 \).

where probabilities are taken on random strings \( r \) of size \( q(n) \), for some polynomial \( q \) in \( n \).

It is clear that \( C \subseteq C' \) implies \( \text{NP}^C \subseteq \text{NP}^{C'} \).

Question 6 (***) Show that \( \text{NP}^{\text{BPP}} \subseteq \text{MA} \).

Question 7 (**) Show that, if \( \text{NP} \subseteq \text{BPP} \), then \( \text{PH} \subseteq \text{BPP} \). Here is the proof; I am asking you to replace the “why?” questions by appropriate justifications. If \( \text{NP} \subseteq \text{BPP} \), then:

\[
\text{PH} = \Sigma_2^p \subseteq \text{NP}^{\text{BPP}} \subseteq \text{MA} = \text{BP} \cdot \text{NP} \subseteq \text{BP} \cdot \text{BPP} \subseteq \text{BPP}
\]

why? (1)

final comments in the n1.pdf lecture notes

\( \subseteq \text{NP}^{\text{BPP}} \)

\( \subseteq \text{MA} \)

\( \subseteq \text{AM} \)

\( = \text{BP} \cdot \text{NP} \)

why? (2)

\( \subseteq \text{BP} \cdot \text{BPP} \)

why? (3)

\( \subseteq \text{BPP} \)

why? (4)

\( \subseteq \text{AM} \)

why? (5)

3 Merlin in polynomial space

Question 8 (***) By an analysis of the Shen-Shamir protocol, show that QBF can be decided by an \( \text{IP} \) protocol in which Merlin computes his answers in polynomial space (in the length of the input formula).

Question 9 (***) Deduce that, if \( \text{PSPACE} \subseteq \text{P/poly} \), then \( \text{PSPACE} = \text{MA} \).