Advanced Complexity Exam (2021-22)

You may answer in English or in French. If you answer in French, and you do not know the French equivalent of some English word that I am using, by all means do not invent your own translation: use the English word instead in that case.

Let me stress the value of rigor. In all arguments, you must: (a) stress the important idea; (b) unless stated otherwise, give explicit values for all required bounds (errors, probabilities, time and space usage, and so on); (c) give explicit references to the results you use, preferably by name (e.g., “the Immerman-Szelepcsényi theorem”).

By “polynomial”, I mean “univariate polynomial with coefficients in \(\mathbb{N}\), of degree at least 1, and whose value is strictly positive on every element of \(\mathbb{N}\)”… unless stated otherwise.

1 More on MA

For every \(\epsilon\) such that \(0 < \epsilon < 1/2\), let \(\text{MA}_\epsilon\) be defined as \(\text{MA}\), except with error \(\epsilon\). In other terms, a language \(L\) is in \(\text{MA}_\epsilon\) if and only if there is a language \(D \in \text{P}\) and there are polynomials \(p\) and \(R\) such that for every input \(x\) (whose size I will always write as \(n\)):

- if \(x \in L\), then there is a \(y\) of size \(p(n)\) such that \(Pr_r[x\#y\#r \in D] \geq 1 - \epsilon\);
- if \(x \not\in L\), then for every \(y\) of size \(p(n)\), \(Pr_r[x\#y\#r \in D] \leq \epsilon\),

where \(r\) has size \(R(n)\).

One may use the following definition of \(\text{MA}\), which is a simplification of the definition given in the lecture notes. \(L\) is in \(\text{MA}\) if and only if for every polynomial \(q\), there is a language \(D \in \text{P}\) and there are polynomials \(p\) and \(R\) such that for every input \(x\) (whose size I will always write as \(n\)):

- if \(x \in L\), then there is a \(y\) of size \(p(n)\) such that \(Pr_r[x\#y\#r \in D] \geq 1 - 1/2^q(n)\).
• if \( x \not\in L \), then for every \( y \) of size \( p(n) \), \( \Pr_r[x\#y\#r \in D] \leq 1/2^{q(n)} \),

where \( r \) has size \( R(n) \). Let me draw your attention to the fact that, in this
definition, the polynomials \( p \) and \( R \), as well as the language \( D \), may depend on
\( q \).

We define the class \( \text{MA}' \) by requiring that \( p \) is independent of \( q \). That is, \( L \)
is in \( \text{MA}' \) if and only if there is a polynomial \( p \) such that for every polynomial
\( q \), there is a language \( D \in \text{P} \) and a polynomial \( R \) such that [etc.]

**Question 1** Show that \( \text{MA}_{1/3} \subseteq \text{MA}' \).

**Question 2** Show that \( \text{MA} \subseteq \text{MA}_{1/3} \subseteq \text{MA}' \subseteq \text{MA} \), hence all these classes are equal.

## 2 The class \( S^p_2 \)

For every class of languages \( C \), we define a new class of languages \( S_2 \cdot C \) as follows.
A language \( L \) is in \( S_2 \cdot C \) if and only if there is a language \( D \) in \( C \) and a polynomial
\( p \) such that, for every input \( x \):

1. if \( x \in L \), then there is a \( y \) of size at most \( p(n) \) such that for every \( z \) of size
   at most \( p(n) \), \( x\#y\#z \in D \);

2. if \( x \not\in L \), then there is a \( z \) of size at most \( p(n) \) such that for every \( y \) of size
   at most \( p(n) \), \( x\#y\#z \not\in D \).

Note that the existence of \( y \) satisfying 1 and the existence of \( z \) satisfying 2 are
mutually exclusive conditions.

It will be practical to call the words \( y \) above the proofs (or proof candidates)
that \( x \in L \), while \( z \) is a counter-proof (candidate). Taking an analogy with trials
and courtrooms, proofs are provided by the attorney general, counter-proofs are
provided by the defense counsel, and \( L \) is in \( S_2 \cdot C \) if and only if every input word
\( x \) is either a clear win for the attorney general (whatever counter-proofs are given
by the defense) or a clear win for the defense (whatever proofs are put forward
by the attorney general).

The class \( S^p_2 \) is \( S_2 \cdot \text{P} \). It is pretty clear that \( \text{NP} \cup \text{coNP} \subseteq S^p_2 \subseteq \Sigma^p_2 \cap \Pi^p_2 \).

The class \( S_2\text{BP} \cdot C \) is a probabilistic version of \( S_2 \cdot C \). \( L \) is in \( S_2\text{BP} \cdot C \) if and only if, for every polynomial \( q \), there is a language \( D \in C \) and there are
polynomials \( p \) and \( R \) such that, for every input \( x \):

1. if \( x \in L \), then there is a \( y \) such that for every \( z \), \( \Pr_r[x\#y\#z\#r \in D] \geq 1 - 1/2^{p(n)+q(n)} \);

2. if \( x \not\in L \), then there is a \( z \) such that for every \( y \), \( \Pr_r[x\#y\#z\#r \in D] \leq 1/2^{p(n)+q(n)} \).
where \( y \) and \( z \) are of size \( p(n) \) and \( r \) has size \( R(n) \). Now either the defense counsel or the attorney general have a clear win again, but only with high probability.

**Question 3** Show that \( \text{MA} \subseteq S_2^\text{BP} \cdot \text{P} \).

**Question 4** Let \( L \) be a language in \( S_2^\text{BP} \cdot \text{P} \), and \( q, D, p, R \) be as in the definition of \( S_2^\text{BP} \cdot \text{P} \). Let \( x \) be an arbitrary input, and \( R_{yz} = \{ r \mid x\#y\#z\#r \in D \} \). With the aim of using Lautemann’s technique, show that if \( x \in L \) then \( \bigcap_z R_{yz} \) is huge for some \( y \), in the sense that \( \Pr_r [r \in \bigcap_z R_{yz}] \geq 1 - 1/2^q(n) \); and that if \( x \not\in L \) then \( \bigcup_y R_{yz} \) is small for some \( z \), in that \( \Pr_r [r \in \bigcup_y R_{yz}] \leq 1/2^q(n) \).

**Question 5** With \( L, q, D, p, R \) as above, show that, letting \( m = R(n) + 1 \), and \( m' = R(n)^2 \):

(a) if \( x \in L \), then: (A) there is a proof \( y \) and there are random tapes \( r_1, \ldots, r_m \) such that for all random tapes \( s_1, \ldots, s_m' \), we have: for every \( j \in \{1, \ldots, m'\} \), there is an \( i \in \{1, \ldots, m\} \) such that for every counter-proof \( z \), \( x\#y\#z\#(r_i \oplus s_j) \in D \);  
(b) if \( x \not\in L \), and if \( n \) is large enough, then: (B) there is a counter-proof \( z \) and there are random tapes \( r_1, \ldots, r_m \) such that for all random tapes \( r_1, \ldots, r_m \), we have: there is a \( j \in \{1, \ldots, m'\} \) such that for every \( i \in \{1, \ldots, m\} \), for every proof \( y \), \( x\#y\#z\#(r_i \oplus s_j) \not\in D \).

(Yes, in (B), we require “there is a \( j \) such that for every \( i \)”, and not “for every \( i \), there is a \( j \)”. By “large enough” I mean that there should be a constant \( n_0 \) such that (B) holds for every \( n \geq n_0 \).)

**Question 6** Show that \( S_2^\text{BP} \cdot \text{P} \subseteq S_2 \cdot \text{P} \).

**Question 7** Conclude that \( \text{MA} \subseteq S_2^p \). What theorem(s) from the lecture notes does this improve upon?

### 3 What would happen if polynomial space languages had polynomial circuits?

**Question 8** By looking back at the Shamir(-Shen) protocol, show that if Merlin can convince Arthur that the input QBF formula is true, it can do so in polynomial space. In other words, show that one can implement the Merlin function \( M \) in the definition of the \( \text{IP} \) protocol for QBF by a polynomial space Turing machine. Beware that the obvious way of computing the polynomial that Merlin should play in order to play honestly would take exponential space, because it involves computing polynomials of polynomial size on polynomially many variables. Do not bother to give me a full-fledged proof: give the idea, and explain why this gets around the difficulty that I just mentioned.
Question 9 If \( \text{PSPACE} \subseteq \text{P/poly} \), by the previous question, we can modify the Shamir(-Shen) protocol for QBF by replacing Merlin by a polynomial family of circuits. Iron out the details and show that, if \( \text{PSPACE} \subseteq \text{P/poly} \), then QBF is in \( \text{MA} \). I don’t need a full-fledged formal proof, but I want an explanation of the technical difficulties you must solve, and how you solve them.

Question 10 Conclude that \( \text{PSPACE} \subseteq \text{P/poly} \) implies \( \text{PSPACE} = \text{MA} \), and that the polynomial-time hierarchy then collapses at level 2.