Examen Final. Complexité algorithmique. 4 janvier 2011. (*English version*)

Duration : 3h. Documents (in particular lecture notes) are not allowed.

There are 6 independent exercises.
You can write in either French or English. Remember to justify your answers, this will be taken into account in the score.
If you cannot solve a question you might try to admit the result and address the following questions of the exercise.

Exercice 1.
Give the definitions of the complexity classes BPP, RP and ZPP.
Enumerate all the inclusions known between these classes, as well as between these classes and the complexity classes P, NP and EXP (you do not need to prove these inclusions though).

Exercice 2.

1. Give the definition of an alternating Turing machine and of a language decided by such a machine.
2. State the theorem characterizing the complexity class PSPACE with alternating Turing machines, and prove it.

Exercice 3.

1. Give the definition of P/poly (with boolean circuits) and of $DTIME(T(n))/a(n)$, where T and a are two functions from $\mathbb{N}$ to $\mathbb{N}$.
2. Prove the following theorem : $\mathsf{P/poly} = \cup_{c,d} DTIME(n^c)/n^d$.

Exercice 4. *Error reduction for* RP
Let $L \subseteq \{0,1\}^*$ be such that there exists a probabilistic Turing machine (PTM) $\mathcal{M}$ of polynomial time and a $c > 0$ such that for all x of $\{0,1\}^*$:

1. If $x \in L$, then $Pr[\mathcal{M}(x) = 1] \geq n^{-c}$, and
2. If $x \notin L$, then $Pr[\mathcal{M}(x) = 1] = 0$.

Show that then for any $d > 0$ there exists a PTM $\mathcal{M}'$ of polynomial time such that for all x of $\{0,1\}^*$:

1. If $x \in L$, then $Pr[\mathcal{M}'(x) = 1] \geq 1 - 2^{-n^d}$, and
2. If $x \notin L$, then $Pr[\mathcal{M}'(x) = 1] = 0$.

Remark : beware, you are asked here to prove this result, not to deduce it from another theorem.

Exercice 5.
We say that a directed graph G is *strongly connected* if for any distinct vertices v_1, v_2 of G there exists a directed path from v_1 to v_2 and a directed path from v_2 to v_1. One considers the following language FC :

$$FC = \{< G > \ / \ G \text{ is a strongly connected directed graph}\}.$$

1. Show that the langage FC belongs to NL.
2. Show that this language is NL-complete.

Exercice 6.
We denote [1] $\mathsf{E} = \bigcup_c \mathsf{DTIME}(2^{cn})$ and $\mathsf{ESPACE} = \bigcup_c \mathsf{SPACE}(2^{cn})$. We recall that $A \leq_T^p B$ means that there exists a polynomial time deterministic Turing machine with oracle B which decides A.

1. Prove that $\mathsf{E} \neq \mathsf{ESPACE} \implies \mathsf{P} \neq \mathsf{PSPACE}$.
   Indication : one can use padding.
2. Refine the previous argument to show that $\mathsf{E} \neq \mathsf{ESPACE} \implies \mathsf{P} \neq \mathsf{PSPACE} \cap \mathsf{P/poly}$.
   Indication : one can use the fact that any unary language is in $\mathsf{P/poly}$.
3. The goal of this question is to prove the converse of the previous property.
   (a) Let $L \in \mathsf{P/poly}$ decided by a Turing machine $\mathcal{M}$ with polynomial advice $(\alpha_n)_n$. Show that the language
   $$U = \{1^{\langle n,i,\alpha_{n,i}\rangle} : \alpha_{n,i} \text{ is the } i\text{-th bit of } \alpha_n\}$$
   satisfies $L \leq_T^p U$.
   (b) *(note that this question is slightly more difficult)*
   Let us assume moreover that $L \in \mathsf{PSPACE}$. Show that for any input n, one can compute in polynomial space with respect to n (and not with respect to the length of n) a word β_n satisfying the same property as α_n : the machine $\mathcal{M}$ with polynomial advice $(\beta_n)_n$ decides L.
   (c) Show then that there exists a unary language $U' \in \mathsf{PSPACE}$ such that $L \leq_T^p U'$.
   (d) Finally assume that $L \notin \mathsf{P}$. Show that there exists a unary language in $\mathsf{PSPACE} \setminus \mathsf{P}$.
   (e) Conclude.
4. Prove that $\mathsf{BPP} \subseteq \mathsf{PSPACE}$.
5. By using the results of the previous questions, show that $\mathsf{P} \neq \mathsf{BPP} \implies \mathsf{E} \neq \mathsf{ESPACE}$.

1. Beware : do not get confused with the classes EXP and EXPSPACE.