PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Complexity Theory - IIC3242
Homework 2
Deadline: Monday, 30th of May

1 The padding technique [2 points]

[a] (0.5 points) Define the language U as follows:

$$U = \{ \langle M, w, \#^t \rangle \mid M \text{ is a non-deterministic TM which accepts } w \text{ within } t \text{ steps, on some branch of its computation } \}.$$

Show that U is an NP-complete problem. You can assume that # does not appear in the language of M, but this is not important for the problem. The idea of adding a representation of a number in unary at the end of the input is commonly used in complexity theory and is often referred to as *padding*.

[b] (1.5 points) Using the idea of padding the input to a machine with a representation of a number **in unary**, prove that EXPTIME $\neq$ NEXPTIME implies that PTIME $\neq$ NP.

2 Upper bound for wild animals [1 points]

We call a sequence of words $w_1, w_2, \ldots, w_k$ a *rainworm*, is for all $i = 1 \cdots k-1$, it holds that w_i and w_{i+1} differ in only one letter (and are of the same length). For example the sequence of words: "feed, deed, deer, dear, bear, beer" is a rainworm starting with the word "feed", and ending with the work "beer". Let A be the following language:

$$A = \{ \langle D, s, t \rangle \mid \text{ where } D \text{ is a deterministic automaton such that } L(D) \text{ contains a rainworm starting in } s \text{ and ending in } t \}.$$

Show that A is in PSPACE. Note that you only have to show the upper bound.

3 A complete problem in Σ_2^p [3 points]

A model of a propositional formula φ is a valuation $v : vars(\varphi) \to \{0,1\}$, where $vars(\varphi)$ denotes the set of all variables appearing in φ, which makes the formula true. A model v_1 is contained in a model v_2, denoted by $v_1 \subseteq v_2$, if $\{x \in vars(\varphi) \mid v_1(x) = 1\} \subseteq \{x \in vars(\varphi) \mid v_2(x) = 1\}$, that is, if the set of variables that are true under v_1 is contained in the set of variables that are true in v_2. We say that a model v is *minimal*,

if there is no model v' such that $v' \subseteq v$, but they are not equal (i.e. v' makes less variables true, and still satisfies the formula).
For example, if we have $\varphi \equiv (x \vee y \vee z) \wedge (x \vee \neg z)$, then v_1, with $v_1(x) = v_1(y) = v_1(z) = 1$ is a model of φ, and so is v_2, where $v_2(x) = 1$, and $v_2(y) = v_2(z) = 0$, and $v_2 \subseteq v_1$. It is easy to see that v_2 is the minimal model for φ.
Consider the problem:

$$A = \{ \langle \varphi, x \rangle \mid \text{ where } \varphi \text{ is a propositional formula, and } x \text{ is a literal in } \varphi, \\ \text{such that } x \text{ is } \textbf{true} \text{ in some minimal model of } \varphi \}.$$

Show that A is Σ_2^p-complete.

4 Sub-exponential circuits (of sorts) [3 points]

Prove that there is a language L belonging to EXPSPACE which is not decided by circuits of size at most $2^{\frac{n}{2}}$. (Hint: in the class we prove that for every sufficiently large n there is a function from $\{0,1\}^n \to \{0,1\}$ which is not computed by circuits of size $2^{\frac{n}{2}}$. Maybe you can use this fact somehow.)

5 Turing reductions and unary languages [3 points]

Here we introduce another notion of reduction, called a **Turing reduction**. A language A is Turing-reducible to a language B, written $A \leq_T B$, if there exists a deterministic polynomial time oracle machine M such that $A = L(M^B)$; that is, A is decided by a polynomial time machine with the oracle B.

We say that A is Turing-equivalent to B, written $A \equiv_T B$, if $A \leq_T B$ and $B \leq_T A$. Similarly, we define equivalence in terms of PTIME-reductions by saying that $A \equiv_P B$, whenever $A \leq_P B$ and $B \leq_P A$, with $\leq_P$ denoting polynomial time reductions.

Prove the following:

Theorem 1. *There is no language A such that:*

- *A is unary, that is, $A \subseteq \{1^n \mid n \geq 0\}$;*
- *$A \notin$ PTIME, and;*
- *For every language B it holds that: $A \equiv_T B$ implies that $A \equiv_P B$.*

Hint: consider the set

$$B = \{x \in \Sigma^* \mid x \leq A(\varepsilon)A(1)A(11)\cdots A(1^{|x|-1})\},$$

where $\leq$ denotes the lexicographical ordering on Σ^*. What can you say about B and $\overline{B}$? (Here, for a language A, and a word $w \in \Sigma^*$, we use the notation $A(w)$, which equals 1 if $w \in A$, and 0 otherwise. You can assume that the alphabet used by the languages is always $\Sigma = \{0,1\}$.)