Complexity Theory

VU 181.142, WS 2019

Homework Assignment 1

Name:	N.N.
Matr-Nr:	xxxxxxx
Begin:	22 October, 2019
Submission Deadline:	5 Nobember, 2019
send to:	`complexity@dbai.tuwien.ac.at`
Maximum credits:	10

Exercise 1 (5 credits) Recall the problem reduction from an arbitrary language $L \in \mathsf{NP}$ to the **SAT**-problem given in the lecture. In particular, recall the construction of an instance $R(x)$ of **SAT** from an arbitrary instance x of L. Give a rigorous proof of the correctness of this reduction, i.e. $x \in L \Leftrightarrow R(x) \in \mathbf{SAT}$.

Hint. Prove both directions of the equivalence separately. The intended meaning of the propositional atoms in $R(x)$ is clear. You have to be careful, what is given, what is constructed (or defined), and what has to be proved.

- Suppose that $x \in L$.
  - given: Then we know that there exists a successful computation of the NTM T on input x. By our assumption, this computation consists of exactly N steps. Let $conf_0, \ldots, conf_N$ denote the configurations of the NTM T along this computation.
  - constructed/defined: We define a truth assignment $\mathcal{I}$ appropriate to $R(x)$ according to the intended meaning of the propositional atoms in $R(x)$.
  - to be proved: It remains to show that all conjuncts in $R(x)$ are indeed satisfied by $\mathcal{I}$. For this purpose, you have to inspect all groups of conjuncts in $R(x)$ and argue that each of them is true in $\mathcal{I}$.
- Suppose that $R(x) \in \mathbf{SAT}$.
  - given: Then there exists a satisfying truth assignment $\mathcal{I}$ of $R(x)$.
  - constructed/defined: We can construct a sequence $conf_0, \ldots, conf_N$ of configurations of the NTM T according to the intended meaning of the propositional atoms in $R(x)$.
  - to be proved: First argue that the configurations $conf_0, \ldots, conf_N$ are well-defined (by using the the fact that $\mathcal{I}$ satisfies all conjuncts of $R(x)$).

    It remains to show that there exists a computation of T on input x which produces exactly this sequence of configurations $conf_0, \ldots, conf_N$. Note that, in particular, this is a successful computation by the conjunct $state_{s_m}[N]$ (with s_m = "yes") in $R(x)$ and by the intended meaning of $state_{s_m}[N]$. For this purpose, you have to show by induction on τ that there exists a computation of T on input x whose first τ configurations are $conf_0, \ldots, conf_\tau$.

For your convenience. The groups of conjuncts in $R(x)$ are recalled below.

1. Initialization facts.

$symbol_{\triangleright}[0,0]$
$symbol_{\sigma}[0,\pi]$ for $1 \leq \pi \leq |x|$, where $x_\pi = \sigma$
$symbol_{\sqcup}[0,\pi]$ for $|x| < \pi \leq N$
$cursor[0,0]$
$state_{s_0}[0]$

2. Transition rules. For each pair (s,σ) of state s and symbol σ let $\langle s,\sigma,s'_1,\sigma'_1,d_1\rangle$, ..., $\langle s,\sigma,s'_k,\sigma'_k,d_k\rangle$ denote all possible transitions according to the transition relation Δ (for the cursor movements, we write $d_i \in \{-1,0,1\}$ rather than $d_i \in \{\leftarrow, -, \rightarrow\}$).
Then $R(x)$ contains the following conjuncts for each value of τ and π such that $0 \leq \tau < N$ and $0 \leq \pi < N$

$state_s[\tau] \wedge symbol_\sigma[\tau,\pi] \wedge cursor[\tau,\pi] \rightarrow$
$[(state_{s'_1}[\tau+1] \wedge symbol_{\sigma'_1}[\tau+1,\pi] \wedge cursor[\tau+1,\pi+d_1]) \vee \ldots \vee$
$(state_{s'_k}[\tau+1] \wedge symbol_{\sigma'_k}[\tau+1,\pi] \wedge cursor[\tau+1,\pi+d_k])]$

3. Uniqueness constraints. Let $K = \{s_0,\ldots,s_m\}$ and $\Sigma = \{\sigma_1,\ldots,\sigma_n\}$.
Then $R(x)$ contains the following formulae for each value of τ and π such that $0 \leq \tau \leq N$, $0 \leq \pi \leq N$, $0 \leq i \leq m$, and $1 \leq j \leq n$.

$state_{s_i}[\tau] \leftrightarrow (\neg state_{s_0}[\tau] \wedge \ldots \wedge \neg state_{s_{i-1}}[\tau] \wedge$
$\wedge \neg state_{s_{i+1}}[\tau] \wedge \ldots \wedge \neg state_{s_m}[\tau])$
$cursor[\tau,\pi] \leftrightarrow (\neg cursor[\tau,0] \wedge \ldots \wedge \neg cursor[\tau,\pi-1] \wedge$
$\wedge \neg cursor[\tau,\pi+1] \wedge \ldots \wedge \neg cursor[\tau,N]$
$symbol_{\sigma_j}[\tau,\pi] \leftrightarrow (\neg symbol_{\sigma_1}[\tau,\pi] \wedge \ldots \wedge \neg symbol_{\sigma_{j-1}}[\tau,\pi] \wedge$
$\wedge \neg symbol_{\sigma_{j+1}}[\tau,\pi] \wedge \ldots \wedge \neg symbol_{\sigma_n}[\tau,\pi]$

4. Inertia rules. $R(x)$ contains the following conjuncts for each value τ,π,π',σ, where $0 \leq \tau < N$, $0 \leq \pi < \pi' \leq N$, and $\sigma \in \Sigma$,

$symbol_\sigma[\tau,\pi], cursor[\tau,\pi'] \rightarrow symbol_\sigma[\tau+1,\pi]$
$symbol_\sigma[\tau,\pi'], cursor[\tau,\pi] \rightarrow symbol_\sigma[\tau+1,\pi']$

5. Acceptance. Let s_m = "yes".
Then $R(x)$ contains the following atom as a conjunct:

$state_{s_m}[N]$).

Exercise 2 (5 credits) Recall the basic, polynomial-time decision procedure for HORN-SAT (see cc04.pdf). The correctness of this decision procedure relies on the following lemma:

Lemma. *Let φ be a propositional Horn-formula. Let Y denote the set of atoms which are obtained by initializing Y to the set of facts in φ and by exhaustively applying the rules in φ to Y. Then, for every atom x in φ, the following equivalence holds: $x \in Y \Leftrightarrow x$ is implied by the facts and rules in φ.*

Give a rigorous proof of this lemma.

Terminology. We say that a formula β is implied by a set of formulas α, if $\alpha \models \beta$ holds, i.e., every model of (all formulas in) α is a model of β. In the above lemma, let ψ denote the set consisting of the rules and facts (but not the goals) in φ. The lemma thus claims that $x \in Y \Leftrightarrow \psi \models x$ holds.