1	2	3	4	Σ

6.0/4.0 VU Formale Methoden der Informatik (185.291)

11 December 2018

Kennz. (study id)	Matrikelnummer (student id)	Nachname (surname)	Vorname (first name)

1.) (a) Consider the following decision problem:

INDEPENDENT DOMINATING SET (IDS)

INSTANCE: A directed graph $G = (V, E)$.

QUESTION: Does there exists a set $S \subseteq V$ of vertices, such that

(1) for each $(u, v) \in E$, $\{u, v\} \not\subseteq S$;

(2) for each $v \in V$ either $v \in S$ or there exists an $(u, v) \in E$, such that $u \in S$.

The following function f provides a polynomial-time many-one reduction from **IDS** to **SAT**: for a directed graph $G = (V, E)$, let

$$f(G) = \bigwedge_{(u,v)\in E} (\neg x_u \vee \neg x_v) \wedge \bigwedge_{v\in V} (x_v \vee \bigvee_{(u,v)\in E} x_u).$$

It holds that G is a yes-instance of **IDS** $\iff$ $f(G)$ is a yes-instance of **SAT**.
Prove the $\implies$ direction of the claim.

(10 points)

(b) Given that **SAT** is NP-complete, what can be said about the complexity of **IDS** from the above reduction? NP-hardness of **IDS**, NP-membership of **IDS**, neither of them, or both (NP-completeness of **IDS**)

(5 points)

2.) (a) The topic of this exercise is *translation validation* (discussed in the fifth lecture of the second block). Given a statement in a source program of the form

$$z = (y_1 * x) + (y_2 * x) \tag{S}$$

and the result of the compiler optimization of the form

$$u_1 = y_1 + y_2, \quad u_2 = u_1 * x, \tag{O}$$

the goal is to check the correctness of the translation.

i. Formulate the verification condition.

____ (VC)

ii. Formulate the abstract verification condition (using uninterpreted functions).

____ (AVC)

iii. Prove the correctness of the translation process (using the semantic proof method from the third lecture (on First-order Logic and Theories), or present a counter-example for (AVC). The symbols u_1, u_2, x, y_1, y_2, z are all free variables!
Hint: Do **not** use Ackermann!

(6 points)

(b) Let φ be the first-order formula

$$\forall x \forall y \left[\big(r(x,y) \rightarrow (p(x) \rightarrow p(y)) \big) \wedge \big(r(x,y) \rightarrow (p(y) \rightarrow p(x)) \big) \right] .$$

i. Is φ valid? If yes, present a proof. If no, give a counter-example and prove that it falsifies φ.

ii. Replace r in φ by $\doteq$ (equality) resulting in ψ. Is ψ E-valid? Argue formally!

(9 points)

3.) (a) Show that the assertion

$$\{F \ : \ y > 0\}$$
$$x := 0;$$
$$i := y;$$
while $i > 0$ **do**
$$x := x + 2;$$
$$i := i - 1$$
od
$$\{G \ : \ x = 2 * y\}$$

is correct with respect to partial correctness.

(12 points)

(b) Consider the program q below.

$$
\begin{array}{l}
y := 1; \\
\textbf{while } x > 0 \textbf{ do} \\
\quad \textbf{if } y > 0 \textbf{ then} \\
\quad\quad x := x - 1; \\
\quad\quad y := y - 1 \\
\quad \textbf{else} \\
\quad\quad y := y + 5 \\
\textbf{od}
\end{array}
$$

Find a loop variant t that is positive at the start of each loop iteration, and strictly decreases with each loop iteration.

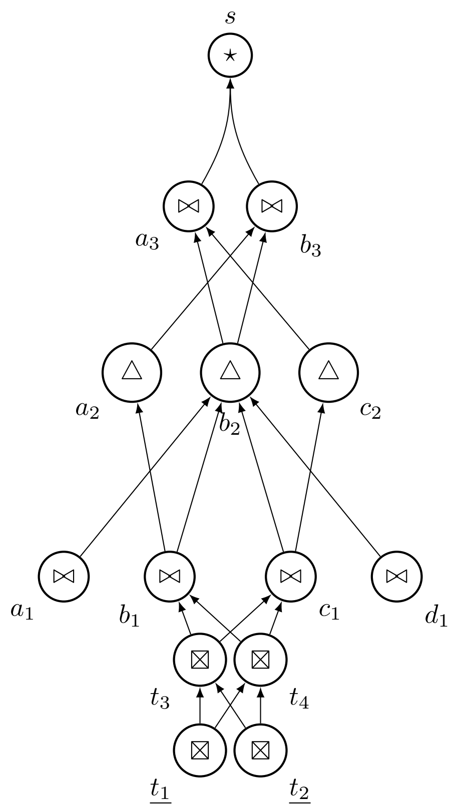
(3 points)

4.) (a) The Kripke structure $M_1 = (S, S_0, R, AP, L)$ is depicted below, with $S_0 = \{t_1, t_2\}$ and $AP = \{\boxtimes, \bowtie, \triangle, \star\}$.

i. Find a Kripke structure M_2 with the smallest number of states and transitions, for which $M_1 \leq M_2$, and write down a witnessing simulation relation.

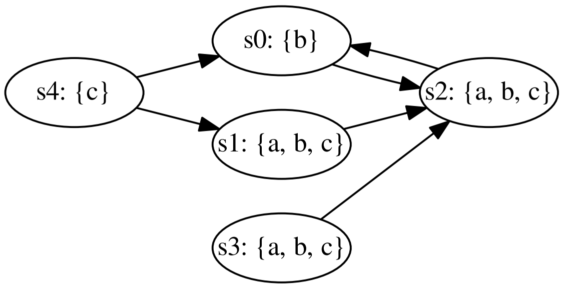
ii. Show that there exists no Kripke structure M_3 with fewer states than M_2, for which $M_1 \leq M_3$.

iii. Does $M_2 \leq M_1$ hold?



(5 points)

(b) Consider the following Kripke structure M:



For each of the following formulae φ,

i. check the respective box if the formula is in CTL, and
ii. list the states s_i on which the formula φ holds; i.e. for which states s_i do we have $M, s_i \models \varphi$?

Recall that for an LTL formula φ it holds that $M, s \models \varphi \iff M, s \models \mathbf{A}\varphi$.

φ	CTL	States s_i
$\mathbf{X}(a)$	☐	
$\mathbf{AG}(b \wedge c)$	☐	
$\mathbf{AX}(a \wedge c)$	☐	
$\mathbf{A}[(b)\ \mathbf{U}\ (c)]$	☐	
$\mathbf{E}[(b \wedge c)\ \mathbf{U}\ (a)]$	☐	

(5 points)

(c) **LTL tautologies**

Prove or disprove that the following formulas are tautologies, i.e., they hold for every Kripke structure M and every path π:

i.
$$\mathbf{XFX}p \iff \mathbf{XF}p$$

ii.
$$(\mathbf{G}\neg p)\ \mathbf{U}\ p \iff p$$

(5 points)

Grading scheme: 0–31 nicht genügend, 32–38 genügend, 39–45 befriedigend, 46–52 gut, 53–60 sehr gut