1	2	3	4	Σ

6.0/4.0 VU Formale Methoden der Informatik (185.291)

Dec 10, 2019

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

1.) 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 $u \in S$.

(a) 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 $\Longleftarrow$ 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) Let φ be the first-order formula

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

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!

(5 points)

(b) Show the following:

$$\varphi^{EUF} \text{ is satisfiable iff } FC^E \land \mathit{flat}^E \text{ is satisfiable.}$$

FC^E and flat^E are obtained from φ^{EUF} by Ackermann's reduction.
(Hint: FC^E is the same for φ^{EUF} and $\neg\varphi^{EUF}$.) **(10 points)**

3.) (a) Let p be the following program:

$$
\begin{array}{l}
x := 3; \\
y := 1; \\
\textbf{while } y \geq N \textbf{ do} \\
\quad x := x - 4 * y + 2; \\
\quad y := y - 1 \\
\textbf{od}
\end{array}
$$

Give a loop invariant for the **while** loop in p and prove the validity of the partial correctness triple $\{N < 0\}\ p\ \{x = 2 * N * N - 4 * N + 3\}$.

(10 points)

(b) We add **for** loops with the following syntax to the IMP language.

$$\textbf{for } v := e_1 \textbf{ until } e_2 \textbf{ do } c \textbf{ od},$$

where v is a variable, e_1 and e_2 are arithmetic expressions and c is a program. The informal semantics of the **for** loop is as follows.

- v is initialized to e_1;
- in every loop iteration, c is executed and then v is incremented, i.e., $v := v + 1$;
- the loop terminates when $v > e_2$.

Stated differently, the above **for** loop is equivalent to

$$v := e_1; \textbf{while } v \leq e_2 \textbf{ do } c; v := v + 1 \textbf{ od}.$$

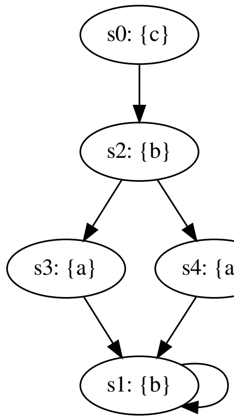
Prove the soundness of or provide a counterexample to the following proof rule.

$$\frac{\{P\}\ v := e_1\ \{I\} \quad \{I \wedge v \leq e_2\}\ c; v := v + 1\ \{I\}}{\{P\}\ \textbf{for } v := e_1 \textbf{ until } e_2 \textbf{ do } c \textbf{ od}\ \{I \wedge v > e_2\}}$$

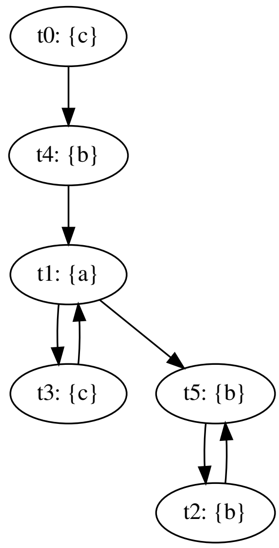
(5 points)

4.) (a) Provide a simulation relation H that witnesses $M_1 \leq M_2$, where M_1 and M_2 are shown below. The initial state of M_1 is s_0, the initial state of M_2 is t_0:

Kripke structure M_1:

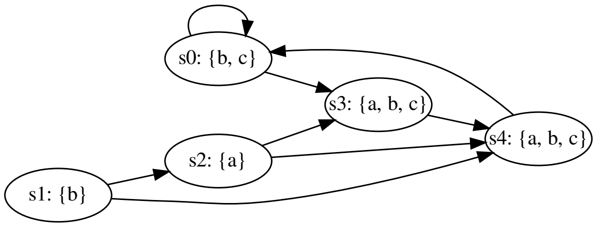


Kripke structure M_2:



(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, LTL, and/or CTL*, and
ii. list the states s_i on which the formula φ holds; i.e. for which states s_i do we have $M, s_i \models \varphi$?

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

(5 points)

(c) **LTL tautologies**

Prove that the following formulas are tautologies, i.e., they hold for every Kripke structure M and every path π in M, or find a Kripke structure M and path π in M, for which the formula does not hold and justify your answer.

i.

$$p \Rightarrow \top \ \mathbf{U} \ (\bot \ \mathbf{U} \ p)$$

ii.

$$q \wedge \mathbf{FG}p \Rightarrow q \ \mathbf{U} \ (\mathbf{G}p)$$

(5 points)

Grading scheme: 0–29 nicht genügend, 30–35 genügend, 36–41 befriedigend, 42–47 gut, 48–60 sehr gut