6.0/4.0 VU Formale Methoden der Informatik (185.291)

January 27, 2017

Kennzahl (study id)	Matrikelnummer (student id)	Familienname (family name)	Vorname (first name)	Gruppe (version)

1.) Consider the following problem:

> **PROB**
>
> INSTANCE: A pair (G_1, G_2) of undirected graphs.
>
> QUESTION: Is it true that G_1 is 3-colorable or G_2 is not 3-colorable? I.e. is it the case that G_1 is a positive instance of **3-COLORABILITY** or G_2 is a negative instance of **3-COLORABILITY**?

By providing a suitable reduction from an NP-complete problem, prove that **PROB** is an NP-hard problem. Argue formally that your reduction is correct.

Recall that **3-COLORABILITY** is defined as follows:

> **3-COLORABILITY**
>
> INSTANCE: An undirected graph $G = (V, E)$.
>
> QUESTION: Does there exist a function μ from vertices in V to values in $\{1, 2, 3\}$ such that $\mu(v_1) \neq \mu(v_2)$ for any edge $[v_1, v_2] \in E$.

(15 points)

2.) (a) Let T be a theory with an unary function symbol $f/1$ and a binary predicate symbol $\approx/2$ such that T forces $\approx/2$ to be symmetric and transitive. Additionally, T includes the following axioms related to f and $\approx$:

$$\forall x \forall y : f(x) \approx f(y) \rightarrow x \approx y \qquad \text{Axiom 1}$$
$$\forall x : f(x) \approx f(f(x)) \qquad \text{Axiom 2}$$

Give a detailed proof that the formula $f(f(f(a))) \approx f(f(b)) \rightarrow a \approx b$ is T-valid.

(6 points)

(b) Let ψ be a propositional formula in conjunctive normal form, and let C be a non-tautological clause containing a literal p such that the literal $\neg p$ does not occur in ψ. Give a detailed proof of the following statement:

$\psi \wedge C$ is satisfiable if and only if ψ is satisfiable

(9 points)

3.) Consider the following axioms of Hoare calculus:

$$\{\, G[v/e] \,\}\; v := e \;\{\, G \,\} \quad \text{(as)} \qquad\qquad \{\, F \,\}\; v := e \;\{\, F[v/e] \,\} \quad \text{(xx)}$$

$$\{\, F \,\}\; v := e \;\{\, \exists v' \, (F[v/v'] \wedge v = e[v/v']) \,\} \quad \text{(as}'\text{)} \qquad\qquad \{\, F \,\}\; v := e \;\{\, F \wedge v = e \,\} \quad \text{(as}''\text{)}$$

provided v' does not occur in F and e provided v does not occur in F and e

(a) Show that the axioms (as) and (as′) are equivalent, i.e., that a complete calculus needs only one of the axioms. **(6 points)**

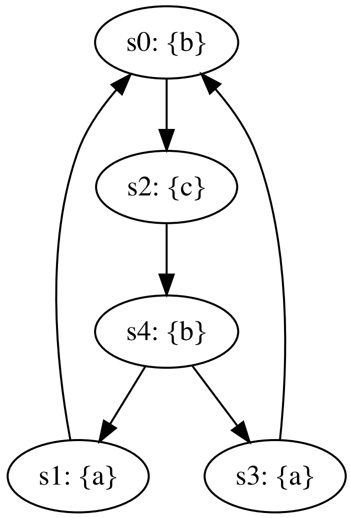
(b) Show that the axiom (as″) is sound, i.e., that each instance of it is a true correctness assertion. You may assume that (as) and (as′) are sound. **(3 points)**

(c) Show that the axiom (xx) is not sound. **(3 points)**

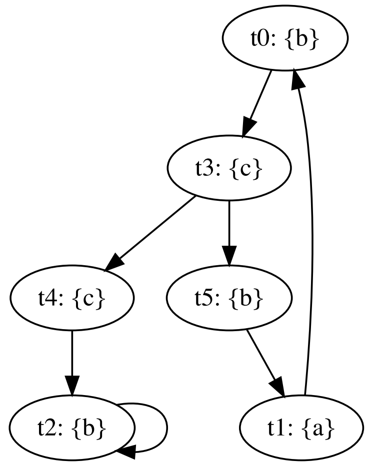
(d) Show that the Hoare calculus is not complete if it contains axiom (as″) but neither (as) nor (as′). **(3 points)**

4.) (a) Provide a non-empty 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:

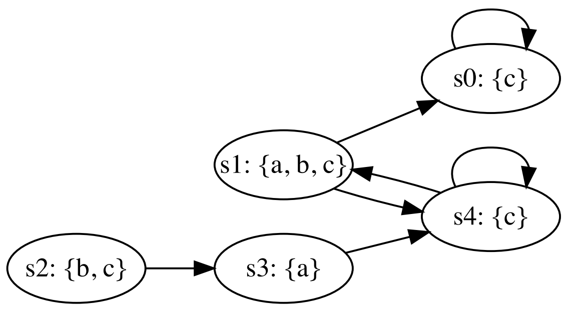


Kripke structure M_2:



(4 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
$\mathbf{X}(a)$	☐	☐	☐	
$\mathbf{EX}(a)$	☐	☐	☐	
$(b \wedge c)\ \mathbf{U}\ c$	☐	☐	☐	
$\mathbf{EF}(a)$	☐	☐	☐	

(4 points)

(c) Let $M = (S, I, R, L)$ be a Kripke structure over a set of propositional symbols AP.

We define a Kripke structure $\hat{M} = (\hat{S}, \hat{I}, \hat{R}, \hat{L})$ as follows:

- $\hat{S} = 2^{AP}$, i.e., a state $\hat{s} \in \hat{S}$ is a subset of AP,
- $\hat{I} = \{\hat{s} \in \hat{S} \mid \exists s \in I.\ L(s) = \hat{s}\}$, i.e.,
  a state $\hat{s} \in \hat{S}$ is an initial state of $\hat{M}$ if there is an initial state $s \in I$ such that s is labeled with $\hat{s}$.
- $\hat{R} = \{(\hat{s}, \hat{t}) \in \hat{S} \times \hat{S} \mid \exists s, t \in S.\ \hat{s} = L(s) \wedge \hat{t} = L(t) \wedge (s, t) \in R\}$, i.e.,
  for each transition $(\hat{s}, \hat{t}) \in \hat{R}$ there are states $s, t \in S$ such that there is a transition from s to t and s is labeled with $\hat{s}$ and t is labeled with $\hat{t}$,
- $\hat{L}(\hat{s}) = \hat{s}$ for all $\hat{s} \in \hat{S}$, i.e.,
  each state $\hat{s} \in \hat{S}$ is labeled with the atomic propositions it contains.

Prove that for any ACTL formula φ over propositions from AP the following holds:

$$\text{If } \hat{M} \models \varphi, \text{ then } M \models \varphi$$

Hint: You can use the following theorem from the lecture:
Let M_1 and M_2 be Kripke structures such that $M_1 \preceq M_2$. Let φ be an ACTL formula. If $M_2 \models \varphi$, then $M_1 \models \varphi$.*

(7 points)