6.0/4.0 VU Formale Methoden der Informatik (185.291)

March 27, 2015

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

1.) Consider the following problem:

> **FIND-INPUT**
>
> INSTANCE: A pair (Π, I), where (i) I is a string, and (ii) Π is a program that takes one string as input and returns a string. It is guaranteed that Π terminates on any input.
>
> QUESTION: Does there exist a string I' such that the program Π on input I' returns I, i.e. $\Pi(I') = I$?

Prove that the problem **FIND-INPUT** is semi-decidable. For this, describe a procedure that shows the semi-decidability of the problem (i.e. a semi-decision procedure for **FIND-INPUT**) and argue that it is correct.

Note: we consider only strings that are built from symbols 0 and 1. **(15 points)**

2.) (a) Let φ be the first-order formula

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

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! (Hint: Substitution axioms)

(9 points)

(b) Let φ be any propositional formula in negation normal form (NNF). Recall that a literal ℓ is pure in a formula φ, if the complement of ℓ, ℓ^c, does not occur in φ, where ℓ^c is b if ℓ is $\neg b$ and ℓ^c is $\neg b$ if ℓ is b.

Prove by induction: If φ contains only pure literals, then φ is satisfiable.

(6 points)

3.) Consider the following modified while-rule:

$$\frac{\{\, Inv \,\}\, p \,\{\, Inv \,\}}{\{\, Inv \,\}\, \textsf{while}\ e\ \textsf{do}\ p\ \textsf{od}\, \{\, Inv \land \neg e \,\}}\ \text{mw}$$

(a) Show that this rule is admissible regarding partial correctness. **(5 points)**

(b) Show that the Hoare calculus for partial correctness is no longer complete, if we replace the regular while-rule by the modified one. **(10 points)**

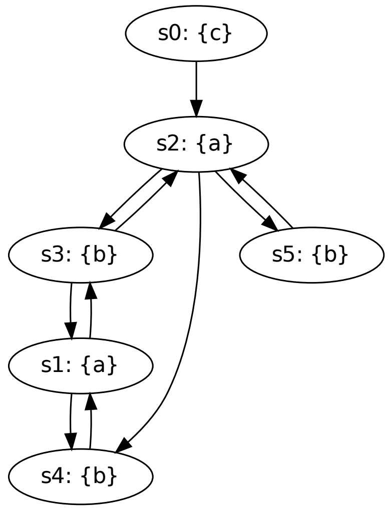
> A rule $\frac{X_1 \cdots X_n}{\{\, F \,\}\, p \,\{\, G \,\}}$ is *admissible regarding partial correctness*, if the conclusion $\{\, F \,\}\, p \,\{\, G \,\}$ is partially correct whenever all premises $X_1, \ldots, X_n$ are valid formulas/partially correct assertions.

> Hoare calculus for partial correctness:
>
> $$\{\, F \,\}\, \textsf{skip} \,\{\, F \,\}$$
>
> $$\{\, F \,\}\, \textsf{abort} \,\{\, G \,\}$$
>
> $$\{\, F[v/e] \,\}\, v \leftarrow e \,\{\, F \,\}$$
>
> $$\frac{\{\, F \,\}\, p \,\{\, G \,\} \quad \{\, G \,\}\, q \,\{\, H \,\}}{\{\, F \,\}\, p; q \,\{\, H \,\}}$$
>
> $$\frac{\{\, F \land e \,\}\, p \,\{\, G \,\} \quad \{\, F \land \neg e \,\}\, q \,\{\, G \,\}}{\{\, F \,\}\, \textsf{if}\ e\ \textsf{then}\ p\ \textsf{else}\ q\ \textsf{fi}\, \{\, G \,\}}$$
>
> $$\frac{\{\, Inv \land e \,\}\, p \,\{\, Inv \,\}}{\{\, Inv \,\}\, \textsf{while}\ e\ \textsf{do}\ p\ \textsf{od}\, \{\, Inv \land \neg e \,\}}$$
>
> $$\frac{F \Rightarrow F' \quad \{\, F' \,\}\, p \,\{\, G' \,\} \quad G' \Rightarrow G}{\{\, F \,\}\, p \,\{\, G \,\}}$$

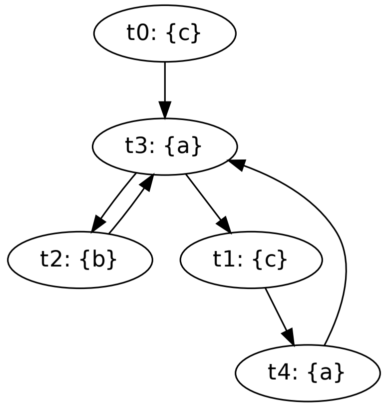
4.) Model Checking

(a) Provide a non-empty simulation relation H that witnesses $M_1 \leq M_2$, where M_1 and M_2 are shown below (M_1 on the left, M_2 on the right), the initial state of M_1 is s_0, the initial state of M_2 is t_0:

Kripke structure M_1:

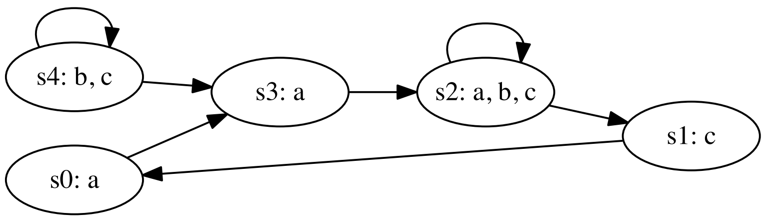


Kripke structure M_2:



(4 points)

(b) Consider the following Kripke structure:



For each of the following formulae

i. determine if the formula is in CTL, LTL, and/or CTL*, and

ii. state on which states s_i the formula holds

$\mathbf{EG}(a)$
$\mathbf{EX}(b)$
$\mathbf{X}(c)$
$\mathbf{F}(a)$

(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)