6.0/4.0 VU Formale Methoden der Informatik (185.291)

29 January 2016

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

1.) Consider the following problem:

> **SOME-HALTS**
>
> INSTANCE: A triple (Π_1, Π_2, I), where I is a string and Π_1, Π_2 are programs that take a string as input.
>
> QUESTION: Is it true that Π_1 halts on I or Π_2 halts on I?

By providing a reduction from an undecidable problem, prove that **SOME-HALTS** is undecidable. Argue formally that your reduction is correct. **(15 points)**

2.) (a) Clarify the logical status of each of the following formulas:

i. φ_1^{EUF}: $f(x,y) \doteq x \wedge g(x) \not\doteq g(z) \wedge h(y) \doteq g(x) \wedge f(f(x,y),y) \doteq z$

ii. φ_2^{EUF}: $x \doteq y \wedge f(x) \not\doteq f(y)$

If the formula is E-valid or E-unsatisfiable, then give a proof based on E-interpretations and semantics. If the formula is E-satisfiable but not E-valid, then present two E-interpretations, one satisfying the formula and one falsifying it. Argue formally why the formula is true respectively false under the considered E-interpretation.

(4 points)

(b) Prove the following by (structural) induction *without* using the equivalent replacement theorem. For every formula with atoms, truth constants from $\{\bot, \top\}$, connectives from $\{\wedge, \vee\}$ and quantifiers from $\{\forall, \exists\}$, there exists an equivalent formula with the same atoms, truth constants from $\{\top\}$, connectives from $\{\neg, \wedge\}$ and quantifiers from $\{\forall\}$. **(11 points)**

3.) Consider the following axioms of Hoare calculus:

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

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

provided v' does not occur in F and e

$$\{\, F \,\}\, v := e \,\{\, F \wedge v = e \,\} \qquad \text{(as}'')$$

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. **(7 points)**

(b) Show that the axiom (as$''$) is sound, i.e., that each instance of it is a true correctness assertion. **(3 points)**

(c) Show that the Hoare calculus is not complete if it contains axiom (as$''$) but neither (as) nor (as$'$). **(3 points)**

(d) The axioms (as$'$) and (as$''$) are both constrained by a condition saying that some variable may not occur in F and e. Explain why this condition is a serious constraint in one case but not in the other. **(2 points)**

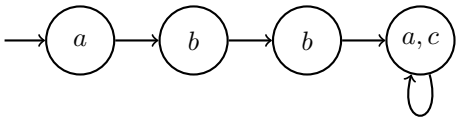
4.) Model Checking

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

Let $AP' \subseteq AP$ be a subset of AP. We define $M' = (S', I', R', L')$ as follows:

- $S' = S$, $I' = I$, $R' = R$, and
- $L'(s) = L(s) \cap AP'$, where $s \in S$.

(a) Consider the concrete instance M over $AP = \{a, b, c\}$ below. Draw M' over $AP' = \{a, b\}$ according to the definition above.



(1 point)

(b) Given any M, M' and AP, AP' according to the definitions above, prove that for any ACTL formula φ over propositions from AP' the following holds:

$$M \models \varphi \text{ if and only if } M' \models \varphi$$

Hint: Use the semantics of ACTL. You can either use induction on the structure of the formula (structural induction) or induction on the formula length.
We recall the definition of ACTL formulae over AP:

- $p \in AP$ is an ACTL formula,
- if φ and ψ are ACTL formulae, then $\neg\varphi$, $\varphi \wedge \psi$, $\mathbf{AX}\,\varphi$, and $\mathbf{A}\,[\varphi\,\mathbf{U}\,\psi]$ are ACTL formulae.

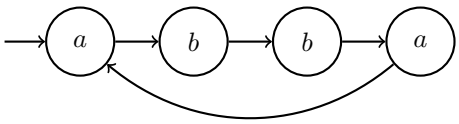
(6 points)

As above, 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:

- $\hat{S} = 2^{AP}$ and $\hat{L}(\hat{s}) = \hat{s}$ for all $\hat{s} \in \hat{S}$
  A state $\hat{s} \in \hat{S}$ is a subset of AP, and is labeled with the atomic propositions it contains.
- $\hat{I} = \{\hat{s} \in \hat{S} \mid \exists s \in I.\ L(s) = \hat{s}\}$
  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 $\hat{s}$.
- $\hat{R} = \{(\hat{s}, \hat{t}) \in \hat{S} \times \hat{S} \mid \exists s, t \in S.\ \hat{s} = L(s) \wedge \hat{t} = L(t) \wedge (s, t) \in R\}$
  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 $\hat{t}$.

(c) Consider the concrete instance M over $AP = \{a, b\}$ below. Draw $\hat{M}$ over 2^{AP} according to the definition above.



(2 points)

(d) Given any $M, \hat{M}$ according to the definitions above, 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 $M_1 \leq M_2$. Let φ be an ACTL formula. If $M_2 \models \varphi$, then $M_1 \models \varphi$.*

(6 points)