| 1 | 2 | 3 | 4 | Σ | Grade |
|---|---|---|---|---|---|
| | | | | | |

# 6.0/4.0 VU Formale Methoden der Informatik

**185.291** **March 25, 2022** **Variant A**

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

**1.)** Recall the **HALTING** problem which takes a program and a string as input, and consider the following variant thereof:

> **HALTING-C**
>
> INSTANCE: A program $\Pi$ that takes a string as input, a string $I$ of even length $2 * n$.
>
> QUESTION: Does $\Pi$ terminate on both strings resulting from $I$ being cut into two halfs, i.e. does $\Pi$ halt on $I[1..n]$ and $I[n+1..2*n]$.

(a) The following function $f$ provides a polynomial-time many-one reduction from **HALTING** to **HALTING-C**: for a program $\Pi$ and a string $I$, let $f(\Pi, I) = (\Pi', I')$ with $\Pi' = \Pi$ and $I' = I + I$ (i.e. the concatenation of two copies of string $I$)

Show that $(\Pi, I)$ is a yes-instance of **HALTING** $\iff$ $(\Pi', I')$ is a yes-instance of **HALTING-C**.

**(6 points)**

(b) Please answer the following questions and explain your answers

- Is **HALTING-C** decidable?
- Is **HALTING-C** semi-decidable?
- Is the complement of **HALTING-C** semi-decidable?

**(9 points)**

**2.)** (a) Consider the following theory $\mathcal{T}_{tree}$ of trees with the signature

$$\Sigma_{tree} = \{\{tree, le, ri\},\ \{atom, \doteq\}\}.$$

The axioms of $\mathcal{T}_{tree}$ include symmetry, reflexivity and transitivity of equality, functional congruence for *tree*, *le*, *ri*, and predicate congruence for *atom*. In addition we have:

$$\forall x\,\forall y\ le(tree(x,y)) \doteq x \qquad \text{(left subtree)}$$
$$\forall x\,\forall y\ ri(tree(x,y)) \doteq y \qquad \text{(right subtree)}$$
$$\forall x\ \big(\neg atom(x) \rightarrow tree(le(x), ri(x)) \doteq x\big) \qquad \text{(construction)}$$
$$\forall x\,\forall y\ \neg atom(tree(x,y)) \qquad \text{(atom)}$$

We augment theory $\mathcal{T}_{tree}$ by $\mathcal{T}_E$ (with uninterpreted function symbol $h$) resulting in $\mathcal{T}_{tree}^E$. Clarify the logical status of each of the following formulas. If one is $\mathcal{T}_{tree}^E$-valid or $\mathcal{T}_{tree}^E$-unsatisfiable, then prove it using the semantic argument method. If one is $\mathcal{T}_{tree}^E$-satisfiable but not $\mathcal{T}_{tree}^E$-valid, then present a satisfying and a falsifying interpretation. Argue formally that the formula evaluates to true resp. false under the constructed interpretations.

$$\varphi_0\colon\ le(a) \doteq le(b) \wedge ri(a) \doteq ri(b) \wedge \neg atom(a) \wedge \neg atom(b) \rightarrow h(a) \doteq h(b)$$
$$\varphi_1\colon\ \neg atom(x) \wedge le(x) \doteq y \wedge ri(x) \doteq z \wedge x \not\doteq tree(y,z)$$

**(8 points)**

(b) Consider the following clause set $\hat{\delta}(\varphi)$ which has been derived from an (unknown) formula $\varphi$ by an improved version of Tseitin's translation (atoms have not been labeled and $\overline{z}$ means $\neg z$).

| | | | |
|---|---|---|---|
| $C_1\colon\ \overline{\ell_1} \vee x_1 \vee x_2$ | $C_2\colon\ \overline{\ell_1} \vee \overline{x_1} \vee \overline{x_2}$ | $C_3\colon\ \ell_1 \vee \overline{x_1} \vee x_2$ | $C_4\colon\ \ell_1 \vee x_1 \vee \overline{x_2}$ |
| $C_5\colon\ \overline{\ell_2} \vee x_2 \vee x_3$ | $C_6\colon\ \overline{\ell_2} \vee \overline{x_2} \vee \overline{x_3}$ | $C_7\colon\ \ell_2 \vee \overline{x_2} \vee x_3$ | $C_8\colon\ \ell_2 \vee x_2 \vee \overline{x_3}$ |
| $C_9\colon\ \overline{\ell_3} \vee \ell_1 \vee \ell_2$ | $C_{10}\colon\ \overline{\ell_3} \vee \overline{\ell_1} \vee \overline{\ell_2}$ | $C_{11}\colon\ \ell_3 \vee \overline{\ell_1} \vee \ell_2$ | $C_{12}\colon\ \ell_3 \vee \ell_1 \vee \overline{\ell_2}$ |
| $C_{13}\colon\ \overline{\ell_4} \vee x_2$ | $C_{14}\colon\ \overline{\ell_4} \vee \ell_3$ | $C_{15}\colon\ \ell_4 \vee \overline{x_2} \vee \overline{\ell_3}$ | |
| $C_{16}\colon\ \overline{\ell_5} \vee x_1 \vee x_3$ | $C_{17}\colon\ \ell_5 \vee \overline{x_1}$ | $C_{18}\colon\ \ell_5 \vee \overline{x_3}$ | |
| $C_{19}\colon\ \overline{\ell_6} \vee \overline{\ell_4} \vee \ell_5$ | $C_{20}\colon\ \ell_6 \vee \ell_4$ | $C_{21}\colon\ \ell_6 \vee \overline{\ell_5}$ | |

(i) Reconstruct $\varphi$ from $\hat{\delta}(\varphi)$.

(ii) Prove the validity of $\varphi$ by resolution (no additional translation to normal form is allowed!). You are allowed to add a single unit clause (i.e., a clause containing exactly one literal). Please explain your approach!

**(7 points)**

**3.)** (a) Let $p$ be the following IMP program loop, containing the integer-valued program variables $x, y$:

$$
\begin{array}{l}
\textbf{while } x \neq y \textbf{ do} \\
\quad x := x - 2 * y; \\
\quad y := 2 * y - x \\
\textbf{od}
\end{array}
$$

Which of the following program assertions are inductive loop invariants of $p$?

- $I_1 :\quad x = 0 \wedge y = 0$
- $I_2 :\quad x + y = 0$
- $I_3 :\quad x = 0 \wedge y = 1$

Give formal details justifying your answer. That is, if an assertion is an inductive loop invariant, provide a formal proof of it based on Hoare logic or using weakest liberal preconditions. If an assertion is not an inductive loop invariant, give a counterexample.

**Note:** You need to use the definition of an assertion being an inductive invariant.

**(9 points)**

(b) Let $A$ be an arbitrary post-condition. Which of the following Hoare triples are valid partial correctness assertions?

- $\{true\}$ **skip** $\{A\}$
- $\{false\}$ **skip** $\{A\}$

Give formal details justifying your answer. That is, if a triple is valid, provide a formal proof of it based on Hoare logic. If an assertion is not valid, give a counterexample (that is, an instance of $A$ for which the triple does not hold).

**(4 points)**

(c) Consider the Hoare triple $\{A\}p\{B\}$, where $p$ is an arbitrary IMP program and $A, B$ are arbitrary program assertions. Assume there is a state $\sigma$ that satisfies $A$ and there is a state $\sigma'$ such that $< p, \sigma > \to \sigma'$ and $\sigma'$ satisfies $B$.

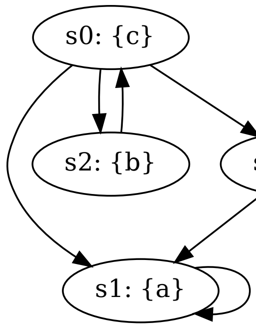
Given this information, is $\{A\}p\{B\}$ partially correct?

Answer the question with either a Yes or a No answer, and provide a short justification for your answer.

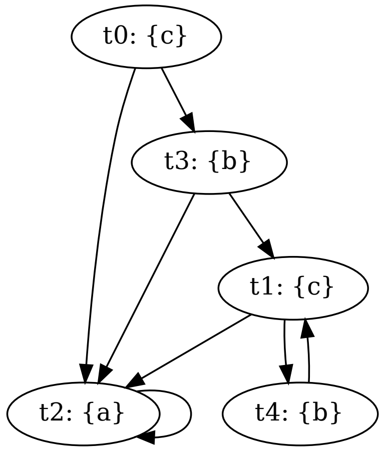
**(2 points)**

**4.)** (a) Consider the Kripke structures $M_1$ and $M_2$. The initial state of $M_1$ is $s_0$, the initial state of $M_2$ is $t_0$.

**Kripke structure $M_1$:**




**Kripke structure $M_2$:**

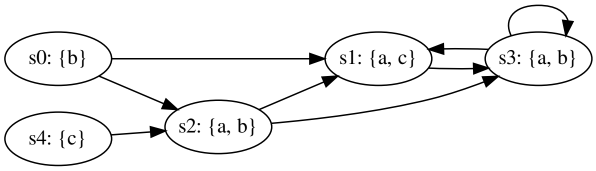



i. Check whether $M_2$ simulates $M_1$, i.e., provide a simulation relation that witnesses $M_1 \preceq M_2$, or briefly explain why $M_2$ does not simulate $M_1$.

ii. Check whether $M_1$ simulates $M_2$, i.e., provide a simulation relation that witnesses $M_2 \preceq M_1$, or briefly explain why $M_1$ does not simulate $M_2$.

**(4 points)**

(b) Consider the following Kripke structure $M$:




For each of the following formulae $\varphi$,

i. indicate whether the formula is in CTL, LTL, and/or CTL*, and

ii. list the states $s_i$ on which the formula $\varphi$ holds; i.e. for which states $s_i$ do we have $M, s_i \models \varphi$?
(If $\varphi$ is a path formula, list the states $s_i$ such that $M, s_i \models \mathbf{A}\varphi$.)

| $\varphi$ | CTL | LTL | CTL* | States $s_i$ |
|---|---|---|---|---|
| $\mathbf{A}[(b)\ \mathbf{U}\ (a)]$ | ☐ | ☐ | ☐ | |
| $\mathbf{G}(a)$ | ☐ | ☐ | ☐ | |
| $\mathbf{FG}(c)$ | ☐ | ☐ | ☐ | |
| $\mathbf{EGF}(c)$ | ☐ | ☐ | ☐ | |
| $\mathbf{EX}(c)$ | ☐ | ☐ | ☐ | |

**(5 points)**

(c) **LTL tautologies**

An LTL formula is a *tautology* if it holds for every Kripke structure $M$ and every path $\pi$ in $M$. For each of the following formulas, prove that it is a tautology, or find a Kripke structure $M$ and path $\pi$ in $M$ for which the formula does not hold and justify your answer.

i. $(b \mathbf{\ U\ } \mathbf{G}(a \wedge \neg b)) \Rightarrow \mathbf{G}(b \Rightarrow \mathbf{F}a)$

ii. $\mathbf{G}(b \Rightarrow \mathbf{F}a) \Rightarrow (b \mathbf{\ U\ } \mathbf{G}(a \wedge \neg b))$

**(6 points)**

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