1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik

185.291 **January 21, 2025**

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

1.) Recall from the lecture the **HALTING** problem:

> **HALTING**
>
> INSTANCE: A non-empty program Π that takes a string as input, a string I.
>
> QUESTION: Does Π terminate on I.

(Remark: For this exercise, we assume that if (Π, I) is an instance of **HALTING**, then Π is not empty, i.e., Π must contain at least one computation step. This assumption does not affect the decidability of the problem.)

Consider now the following decision problem:

> **EQUAL**
>
> INSTANCE: Programs Π_1 and Π_2; both are guaranteed to terminate, and take an integer as input and return an integer as output.
>
> QUESTION: Do there exist integers n_1, n_2, such that $\Pi_1(n_1) = \Pi_2(n_2)$?

(a) Let Π_{int} be the decision procedure that does the following:

- Π_{int} takes as input a program Π, a string I, and an integer n.
- Π_{int} emulates the first n steps of the run of Π on I. If Π terminates on I within n steps, then Π_{int} returns true. Otherwise, Π_{int} returns false.

The following describes a reduction from **HALTING** to **EQUAL**. Given an arbitrary instance (Π, I) of **HALTING**, we construct an instance (Π_1, Π_2) of **EQUAL** as follows:

```
Boolean Π1 (Int n)
if Πint(Π, I, n) return 1; // Π and I are hard-coded
return 0;

Boolean Π2 (Int n)
return 1;
```

Show the correctness of the reduction above, i.e., show that (Π, I) is a positive instance of **HALTING** $\iff$ (Π_1, Π_2) is a positive instance of **EQUAL**.

(9 points)

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

- Is **EQUAL** undecidable?
- Is **EQUAL** semi-decidable?

(6 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:

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

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 while-loop of the following IMP program containing the integer-valued program variables x, y, z, n:

$$
\begin{array}{l}
x := 0; y := n; z := n; \\
\textbf{while } z < n \textbf{ do} \\
\quad \textbf{if } z > n \textbf{ then} \\
\quad\quad z := z - 1 \\
\quad \textbf{else} \\
\quad\quad x := x + 3 * z; \\
\quad y := y - 3 * z \\
\textbf{od}
\end{array}
$$

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

- $I_1 : \quad x + y = z$
- $I_2 : \quad x + z = y$
- $I_3 : \quad z = n$

Give formal details justifying your answers. 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.

(9 points)

(b) Let p be the following IMP program loop, containing the integer-valued program variables x, y:

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

Provide a non-trivial precondition A and a non-trivial postcondition B such that

(i) $\{A\}\ p\ \{B\}$ is not valid;

(ii) $\{A\}\ p\ \{B\}$ is valid but $[A]\ p\ [B]$ is not valid;

(iii) $[A]\ p\ [B]$ is valid.

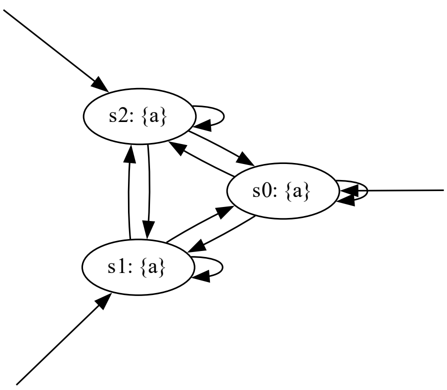
Trivial means equivalent to `true` or `false`, so your precondition A and postcondition B should not be equivalent to `true` or `false`. Give a short justification of your answers!

(6 points)

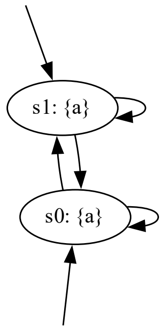
4.) (a) For $n \in \mathbb{N}$, let K_n denote the following Kripke structure:

- K_n comprises n states $s_0, \ldots, s_{n-1}$.
- For each pair of states s_i and s_j, there is a transition from s_i to s_j.
- Every state s_i is labeled with the atomic proposition a.
- Every state s_i of K_n is an initial state.

Kripke structure K_3:



Kripke structure K_2:

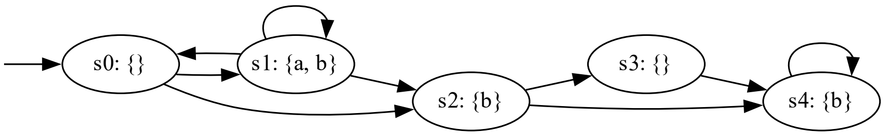


i. Write down a simulation relation H witnessing $K_3 \preceq K_2$ which is not also a bisimulation relation. Explain why H is not a bisimulation relation.

ii. How many simulations witnessing $K_3 \preceq K_2$ are there?

(6 points)

(b) Consider the following Kripke structure M:



For each of the following formulae φ,

i. indicate whether 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 $M, s_i \models \varphi$?
(If φ is a path formula, list the states s_i such that $M, s_i \models \mathbf{A}\varphi$.)

φ	CTL	LTL	CTL*	States s_i
$\mathbf{FG}b$	☐	☐	☐	
$\mathbf{A}[a \ \mathbf{U} \ b]$	☐	☐	☐	
$(\mathbf{EX}a) \wedge \mathbf{X}b$	☐	☐	☐	

(3 points)

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

i. $\mathbf{X}[a\ \mathbf{U}\ \mathbf{G}b] \rightarrow [\mathbf{X}a\ \mathbf{U}\ \mathbf{G}b]$

ii. $[\mathbf{X}a\ \mathbf{U}\ \mathbf{G}b] \rightarrow \mathbf{X}[a\ \mathbf{U}\ \mathbf{G}b]$

(6 points)