1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik

185.291 **March 24, 2025**

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

Block 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.

Consider now the following decision problem:

> **EQUAL**
>
> INSTANCE: Program Π that is guaranteed to terminate, takes a natural number (excluding zero) as input and returns a natural number or zero as output.
>
> QUESTION: Do there exist natural numbers n_1, n_2, such that $n_1 + n_2 = \Pi(n_1) * \Pi(n_2)$?

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

- Π_{int} takes as input a program Π, a string I, and a natural number 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') of **EQUAL** as follows:

```
Boolean Π′ (Int n)
if (n < 2) return 1;
if Π_int(Π, I, n) return n + 1; // Π and I are hard-coded
return 0;
```

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

(9 points)

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

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

(6 points)

Block 2.)

2.a) Suppose `a`, `b`, `c` are unsigned integers in the programming language `C` and `a` $\leq$ `b`. Which problem can occur with a `C` statement `c=(a+b)/2`? What is a simple solution to the problem? **(2 points)**

2.b) Use the sparse method to translate the following formula φ^E

$$\neg\big(a \doteq b \land a \not\doteq c \rightarrow ((a \doteq d \land e \not\doteq f \land g \not\doteq h) \lor g \not\doteq i \lor h \not\doteq j \lor (b \not\doteq c \land g \doteq i \land i \neq j))\big)$$

into a propositional formula φ^p such that φ^E is E-satisfiable if and only if φ^p is satisfiable. Simplify your formula before you construct the propositional skeleton and the transitivity constraints. In the simplifications steps, indicate the simple contradictory cycles and the pure literals.

Present an E-model for φ^E in a formally correct way. **(13 points)**

Block 3.)

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

$$
\begin{array}{l}
x := n; y := 0; z := 0; \\
\textbf{while } x > 0 \textbf{ do} \\
\quad z := z - 3 * x; \\
\quad y := y + 6 * x; \\
\quad x := x - 1 \\
\textbf{od}
\end{array}
$$

Give a variant and inductive invariant for the loop in p and prove the validity of the total correctness triple:

$$[n > 0] \;\; p \;\; [y + 2 * z = x]$$

(10 points)

3.b) Consider the following rule in Hoare logic:

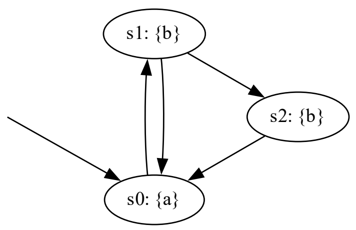
$$\frac{}{\{A\}\ \mathbf{x} := \mathbf{y};\ \mathbf{abort};\ \mathbf{x} := \mathbf{y}\ \{B\}}$$

where A, B are arbitrary assertions and x, y are integer-valued IMP program variables. Is this rule sound? If yes, give a formal proof. Otherwise, give a counterexample and justify your answer.

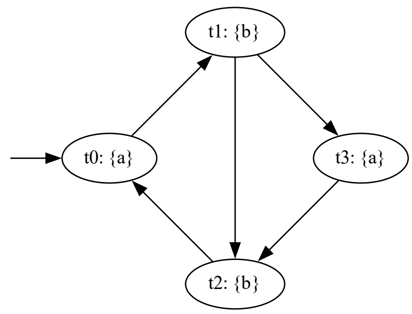
(5 points)

Block 4.) 4.a) Consider the Kripke structures M_1 and M_2. The initial state of M_1 is s_0 and the initial state of M_2 is t_0.

Kripke structure M_1:



Kripke structure M_2:

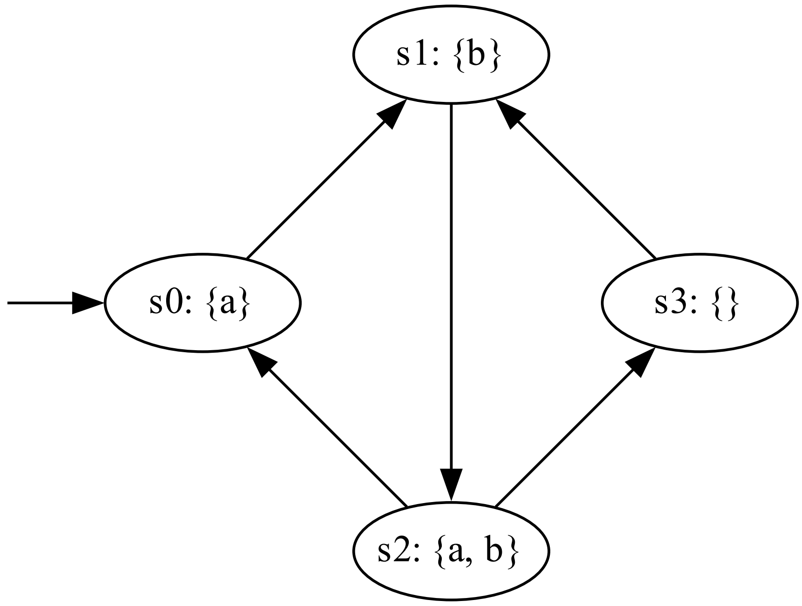


i. Check whether M_2 simulates M_1, i.e., provide a simulation relation that witnesses $M_1 \preceq M_2$, or briefly explain why M_2 does not simulate M_1.

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)

4.b) Consider the following Kripke structure M:



For each of the following formulae φ,

i. indicate whether the formula is in LTL, CTL, 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	LTL	CTL	CTL*	States s_i
$\mathbf{X}[a\ \mathbf{U}\ b]$	☐	☐	☐	
$\mathbf{AX}b$	☐	☐	☐	
$\mathbf{EG}(a \vee b)$	☐	☐	☐	
$\mathbf{F}(\neg a \wedge \neg b)$	☐	☐	☐	
$(\mathbf{EX}a) \wedge \mathbf{X}\neg b$	☐	☐	☐	

(5 points)

4.c) Recall that a LTL formula φ is *satisfiable* if there exists a Kripke structure M and a path π in M such that $M, \pi \models \varphi$. In this case we call the pair (M, π) a *model* of φ.

i. Is there a satisfiable LTL formula φ such that every model of φ has at most three states?

ii. Is there a satisfiable LTL formula φ such that every model of φ has at least three states?

For each question, you should either

- Construct a satisfiable LTL formula φ such that every model of φ has at most/least three states and briefly explain why this is the case.

or

- Prove that no such formula exists by showing that every satisfiable LTL formula φ has a model with more/fewer than three states.

(6 points)

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