1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik **185.291 June, 26 2024**			
Kennz. (study id)	Matrikelnummer (student id)	Nachname (surname)	Vorname (first name)

1.) Recall the following decision problems from the lecture:

HAMILTON-CYCLE

INSTANCE: A directed graph $G = (V, E)$, where V is the set of vertices and E is the set of arcs.

QUESTION: Does G contain a Hamilton cycle, i.e., a sequence $v_1, \ldots, v_n, v_1$ of vertices from V such that:

- $\{[v_i, v_{i+1}] \mid 1 \leq i < n\} \cup \{[v_n, v_1]\} \subseteq E$, and
- each vertex in V is contained in the sequence $v_1, \ldots, v_n$ exactly once.

HAMILTON-PATH

INSTANCE: A directed graph $G = (V, E)$, where V is the set of vertices and E is the set of arcs.

QUESTION: Does G contain a Hamilton path, i.e., a sequence $v_1, \ldots, v_n$ of vertices from V such that:

- $\{[v_i, v_{i+1}] \mid 1 \leq i < n\} \subseteq E$, and
- each vertex in V is contained in the sequence $v_1, \ldots, v_n$ exactly once.

(a) Below we describe a reduction from **HAMILTON-CYCLE** to **HAMILTON-PATH**. Let $G = (V, E)$ be an arbitrary instance of **HAMILTON-CYCLE**. If $|V| \leq 1$ then $G' = G$. Otherwise, G' is the following directed graph:

$$\begin{aligned} G' = (&V \setminus \{u\} \cup \{u_{start}, u_{end}\}, \\ &\{[v, v'] \in E \mid v \neq u, v' \neq u\} \cup \\ &\{[u_{start}, v] \mid [u, v] \in E, v \neq u\} \cup \\ &\{[v, u_{end}] \mid [v, u] \in E, v \neq u\}), \end{aligned}$$

where u is an arbitrary element of V and u_{start}, u_{end} are two fresh vertices.

Show that if G is a yes-instance of **HAMILTON-CYCLE** then G' is a yes-instance of **HAMILTON-PATH**.

HINT: Note that if the sequence $v_1, ..., v_{i-1}, u, v_{i+1}, .., v_n, v_1$ is a Hamilton cycle of a graph G, then also the sequence $u, v_{i+1}, ..., v_n, v_1, ..., v_{i-1}$ is a Hamilton cycle of G.

(9 points)

(b) Please answer the following questions and **explain your answers**. You can use the fact that **HAMILTON-CYCLE** is NP-complete.

- Does the reduction in (a) prove the NP-hardness of **HAMILTON-PATH**?
- Is **HAMILTON-PATH** in NP? If so, provide a certificate relation and argue that it is polynomially balanced and polynomially decidable.

(6 points)

2.) (a) Consider Peano arithmetic PA with signature $\Sigma_{PA} = \big\{\{0, 1, +, \cdot\}, \{\doteq\}\big\}$. Here we need only the induction axiom scheme from PA and four additional axioms:

$$F[0] \wedge \big(\forall x\ (F[x] \rightarrow F[x+1])\big) \rightarrow \forall x\ F[x] \qquad \text{(induction)}$$
$$\forall x\ (x^0 \doteq 1) \qquad \text{(exp zero)}$$
$$\forall x\ \forall y\ (x^{y+1} \doteq x^y \cdot x) \qquad \text{(exp succ)}$$
$$\forall x\ \forall z\ (exp_3(x, 0, z) \doteq z) \qquad (exp_3 \text{ zero})$$
$$\forall x\ \forall y\ \forall z\ \big(exp_3(x, y+1, z) \doteq exp_3(x, y, x \cdot z)\big) \qquad (exp_3 \text{ succ})\big)$$

The extended theory is called $\mathcal{T}^+_{PA}$. Show the following:

$$\forall x \forall y \forall z\ (exp_3(x, y, z) \doteq x^y \cdot z) \quad \text{is } \mathcal{T}^+_{PA}\text{-valid.}$$

Hints: Use $F[y]\colon \forall x \forall z\ \big(exp_3(x, y, z) \doteq x^y \cdot z\big)$ and perform induction on y.

i. Base case: Formally prove $F[0]$ using the semantic argument method.

ii. State precisely the induction hypothesis.

iii. Perform the step case. Again use the semantic argument method.

In order to simplify the proofs, you may use the formulas $(L)\colon \forall x\ (1 \cdot x \doteq x)$ and $(A)\colon \forall x \forall y \forall z\ \big((x \cdot y) \cdot z \doteq x \cdot (y \cdot z)\big)$ as additional lemmas.

Please be precise and indicate exactly why proof lines follow from some other(s). Moreover, recall that equality handling is performed using equality axioms.

(12 points)

(b) Consider the clauses $C_0, \ldots, C_6$ in `dimacs` format (in this order from top to bottom, shown in the box) which are given as input to a SAT solver.

- Apply CDCL using the convention that if a variable is assigned as a decision, then it is assigned 'true'. Select variables as decisions in increasing order of their respective integer IDs in the `dimacs` format, starting with variable `1`. Recall that unit clauses require a special treatment.
- When the *first* conflict occurs, draw the complete implication graph, mark the first UIP, give the resolution derivation of the learned asserting clause that corresponds to the first UIP, and stop CDCL. You do not have to solve the formula!

```
2 0
-1 4 0
-4 5 0
-2 -4 6 0
-3 -6 7 0
-7 9 0
-5 -6 -7 -9 0
```

(3 points)

3.)

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

while $x < n$ **do**
  $x := x - n;$
  $z := 2 * z + x * y;$
  $y := y + n;$
od

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

- $I_1 : \quad x + y = n$
- $I_2 : \quad x + y = z$
- $I_3 : \quad x = n + 1$

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.

(10 points)

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

$$\textbf{skip}; x := 0; \textbf{abort}$$

Give a precondition A and postcondition B such that

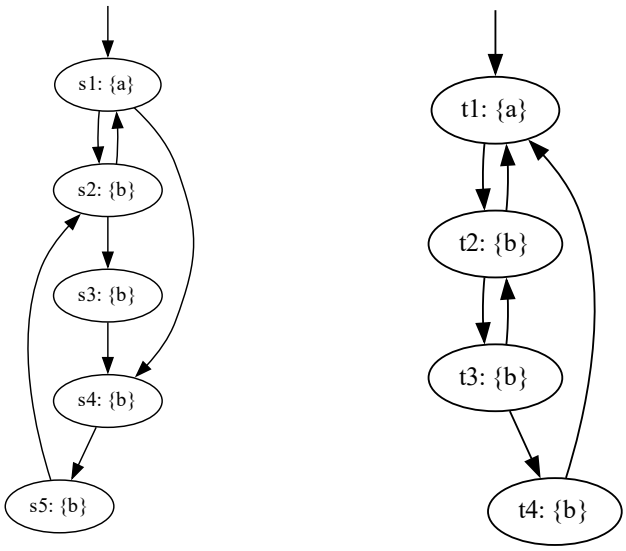
- $\{A\}\ p\ \{B\}$ is valid but $[A]\ p\ [B]$ is not valid;
- $[A]\ p\ [B]$ is valid.

Justify your answers.

(5 points)

4.) (a) Consider the Kripke structures M_1 and M_2. The initial state of M_1 is s_1 and the initial state of M_2 is t_1.

Kripke structure M_1: **Kripke structure M_2:**

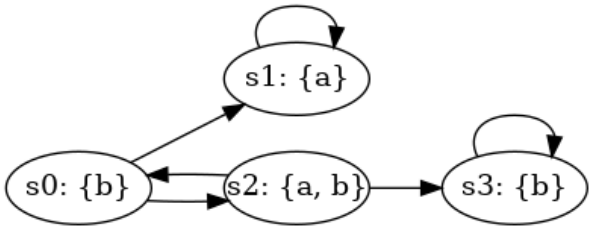


i. Check whether M_2 simulates M_1, i.e., provide a simulation relation that witnesses $M_1 \preceq M_2$, or briefly explain why M_2 does not simulate M_1.

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 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 $M, s_i \models \varphi$? (Note: if φ is a path formula, list the states s_i for which $M, s_i \models \mathbf{A}\varphi$.)

φ	CTL	LTL	CTL*	states s_i
b **U** a	☐	☐	☐	
EG b	☐	☐	☐	
AXEG a	☐	☐	☐	
EGAG b	☐	☐	☐	
E ((**GF** a) $\wedge$ (**GF** $\neg a$))	☐	☐	☐	

(5 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. $\mathbf{GF}a \rightarrow \mathbf{G}(a \rightarrow \mathbf{XF}a)$

ii. $\mathbf{G}(a \rightarrow \mathbf{XF}a) \rightarrow \mathbf{GF}a$

(6 points)

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