1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik
185.291 December, 12 2023

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

1.) Recall from the lecture the NP-complete problem **VERTEX COVER**:

> **VERTEX COVER (VC)**
>
> INSTANCE: An undirected graph $G = (V, E)$ and integer k.
>
> QUESTION: Does there exist a vertex cover of G of size at most k, i.e., is there $N \subseteq V$ such that for each edge $(i, j) \in E$, $\{i, j\} \cap N \neq \emptyset$?

Let $G = (V, E)$ be an undirected graph and let $S \subseteq V$. We denote by $G - S$ the graph that is obtained by removing from G all vertices from S as well as any edge that is incident to some vertex in S. Formally, $G - S = (V \setminus S, E \setminus \{(i, j) \in E \mid \{i, j\} \cap S \neq \emptyset\})$.

Consider now the following decision problem called **FEEDBACK VERTEX SET**:

> **FEEDBACK VERTEX SET (FVS)**
>
> INSTANCE: An undirected graph $G = (V, E)$ and integer k.
>
> QUESTION: Is there $S \subseteq V$ of size at most k such that $G - S$ is cycle-free?

(a) Show that **FVS** is in NP by providing a suitable certificate relation. Briefly argue why this relation is polynomially balanced and polynomial-time decidable. You may use the fact that checking whether an undirected graph is cycle-free is possible in polynomial time. **(3 points)**

(b) The following describes a polynomial-time many-one reduction from **VC** to **FVS**:

Consider an arbitrary instance (G, k) of **VC**, where $G = (V, E)$ is an undirected graph and k is an integer. Let G' denote the graph (V', E'), where $V' = V \cup \{v_{ij} \mid (i, j) \in E\}$ and $E' = \{(i, j), (v_{ij}, i), (v_{ij}, j) \mid (i, j) \in E\}$.

It holds that (G, k) is a positive instance of **VC** $\iff$ (G', k) is a positive instance of **FVS**. Show the $\Longleftarrow$ direction of the claim.

Hint: Observe that every cycle in G' that can be broken by deleting a vertex of the form v_{ij} can also be broken by deleting i or j.

(9 points)

(c) Check which statements are true/false. 1 point for each correct answer, -1 for each incorrect answer, 0 for no answer. Negative points do not carry over to other exercises.

You may use the fact that both **VC** and **SAT** are NP-complete problems.

true	**false**	
○	○	The correctness of the reduction in (b) proves that **FVS** is in NP.
○	○	There is a polynomial-time many-one reduction from **SAT** to **FVS**
○	○	If we can show **FVS** to be in P, we would also show P=NP.

(3 points)

2.) (a) Consider the theory $\mathcal{T}_A$ of arrays and the following formula

$$\varphi: \quad a\langle j \triangleleft f\rangle\langle i \triangleleft e\rangle[j] \doteq e \ \rightarrow \ e \doteq f \vee i \doteq j \ .$$

If φ is $\mathcal{T}_A$-valid, then provide a proof in the semantic argument method. If φ is not $\mathcal{T}_A$-valid, then provide a counter-example.

Besides the equality axioms, reflexivity, symmetry and transitivity, you have:

- $\forall a\, \forall i\, \forall j\ \big(i \doteq j \ \rightarrow\ a[i] \doteq a[j]\big)$ (array congruence)
- $\forall a\, \forall v\, \forall i\, \forall j\ \big(i \doteq j \ \rightarrow\ a\langle i \triangleleft v\rangle[j] \doteq v\big)$ (read-over-write 1)
- $\forall a\, \forall v\, \forall i\, \forall j\ \big(i \not\doteq j \ \rightarrow\ a\langle i \triangleleft v\rangle[j] \doteq a[j]\big)$ (read-over-write 2)

Please be precise. In a proof indicate exactly why proof lines follow from some other(s) and name the used rule. If you use derived rules you have to prove them. Recall that a counter-example has to satisfy all axioms and falsifies φ.

(10 points)

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

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

(i) Reconstruct φ from $\hat{\delta}(\varphi)$ using as few as possible connectives.

(ii) Prove the validity of φ 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!

(5 points)

3.)

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

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

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

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

(10 points)

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

while $x \neq y$ **do**
  if $x > y$ **then** $x := x - 1$ **else abort**
od

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;

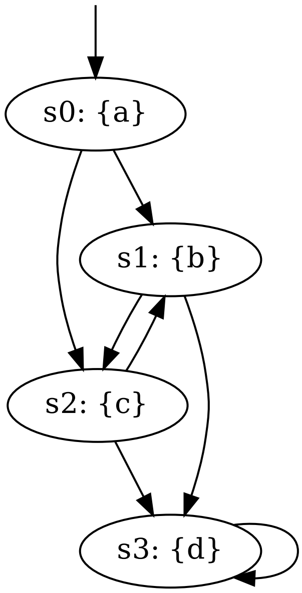
(iii) $[A]\ p\ [B]$ is valid.

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!

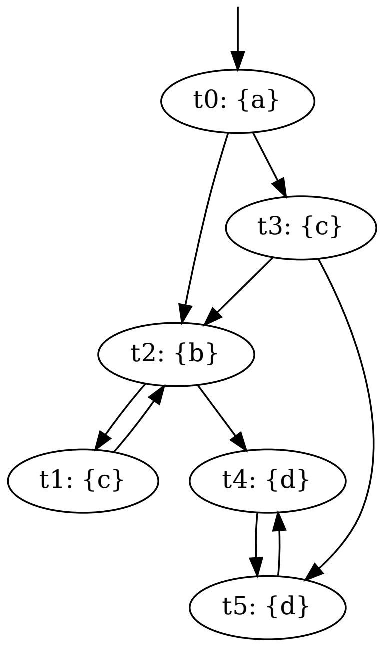
(5 points)

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:

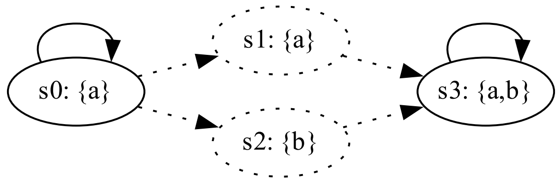


i. Check whether M_2 simulates M_1, i.e., provide a simulation relation that witnesses $M_1 \preceq M_2$, or briefly explain why M_2 does not simulate M_1.

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)

(b) Consider the following Kripke structure. Some of the states have been marked with dashed lines to indicate that they might be deleted (removed from the diagram, along with their corresponding edges) to yield a new Kripke structure.



For each of the following formulae φ,

i. indicate whether the formula is in CTL, LTL, and/or CTL*, and
ii. indicate for which of the following three cases (if any), the formula is true in state s_0, i.e., for which of the following Kripke structures M do we have $M, s_0 \models \varphi$?
   - The complete structure with neither s_1 nor s_2 deleted.
   - The one obtained by deleting only s_1.
   - The one obtained by deleting only s_2.

   (If φ is a path formula, check the mark if $M, s_0 \models \mathbf{A}\varphi$.)

φ	CTL	LTL	CTL*	keep both	delete s_1	delete s_2
$\mathbf{FG}\,a$	☐	☐	☐	☐	☐	☐
$\mathbf{AFAG}\,a$	☐	☐	☐	☐	☐	☐
$\mathbf{AFEG}\,a$	☐	☐	☐	☐	☐	☐
$\mathbf{AFEFG}\,a$	☐	☐	☐	☐	☐	☐
$\mathbf{X}\,b$	☐	☐	☐	☐	☐	☐

(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. $(\mathbf{G}(a \to \mathbf{F}b) \wedge \mathbf{G}(b \to \mathbf{F}a)) \Rightarrow (\mathbf{GF}a \wedge \mathbf{GF}b)$

ii. $(\mathbf{GF}a \wedge \mathbf{GF}b) \Rightarrow (\mathbf{G}(a \to \mathbf{F}b) \wedge \mathbf{G}(b \to \mathbf{F}a))$

(6 points)

Grading scheme: 0–25 nicht genügend, 26–31 genügend, 32–37 befriedigend, 38–43 gut, 44–50 sehr gut