1	2	3	4	Σ

6.0/4.0 VU Formale Methoden der Informatik (185.291)

March 24, 2023

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

1.) Recall the **3-COLORABILITY** problem from the lecture. Consider the following variant thereof. A graph $G = (V, E)$ is connected iff for each pair $s, t \in V$ there is a path from s to t in G, i.e., edges $(s, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n), (v_n, t)$.

> **CON-3-COL**
>
> INSTANCE: A **connected** graph $G = (V, E)$.
>
> QUESTION: Does there exist a valid 3-coloring for G, i.e., a function μ from vertices in V to values in $\{0, 1, 2\}$ such that $\mu(x) \neq \mu(y)$ for any edge $(x, y) \in E$.

(a) The following function f provides a polynomial-time many-one reduction from the problem **3-COLORABILITY** to **CON-3-COL**: for a graph $G = (V, E)$, let V_{uncon} be a set of fresh vertices, such that:

$$V_{uncon} = \{v_{x,y} \mid x, y \in V, \text{ there is no path in } G \text{ from } x \text{ to } y\}.$$

We define $f(G) = G'$ with $G' = (V', E')$, where

$$\begin{aligned} V' &= V \cup V_{uncon}, \\ E' &= E \cup \{(x, v_{x,y}), (y, v_{x,y}) \mid v_{x,y} \in V_{uncon}\}. \end{aligned}$$

Show the correctness of the reduction in (a), i.e., show that G is a positive instance of **3-COLORABILITY** if and only if $f(G)$ is a positive instance of **CON-3-COL**.

(9 points)

(b) 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 **3-COLORABILITY** is NP-complete. Recall also that **SATISFIABILITY** is NP-complete.

true	**false**	
○	○	The correctness of the reduction in (a) proves NP-hardness of **CON-3-COL**.
○	○	The correctness of the reduction in (a) proves NP-membership of the complement of **CON-3-COL**.
○	○	The correctness of the reduction in (a) proves undecidability of **CON-3-COL**.
○	○	If we can show **CON-3-COL** to be in P, we also would have shown P = NP.
○	○	The fact that **CON-3-COL** is a special case of **3-COLORABILITY** proves NP-membership of **CON-3-COL**.
○	○	The correctness of the reduction in (a) proves that there is a polynomial-time many-one reduction from **SATISFIABILITY** to **CON-3-COL**.

(6 points)

2.) (a) Translate the following formula φ^E:

$$\neg\big(a \doteq b \wedge a \neq c \rightarrow \big((a \doteq d \wedge e \neq f) \vee e \neq h \vee f \neq g \vee (b \neq c \wedge e \doteq h \wedge h \neq g)\big)\big)$$

into a propositional formula φ^p such that φ^E is E-satisfiable if and only if φ^p is satisfiable.

Recall that a formula is simplified before the propositional skeleton and the transitivity constraints are constructed. In the simplification steps, indicate the simple contradictory cycles and the pure literals. **(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.

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

- 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!

(3 points)

3.)

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

$$
\begin{array}{l}
\textbf{while } x < y \textbf{ do} \\
\quad x := 3 * x - 3 * y; \\
\quad y := 4 * y - 2 * x; \\
\textbf{od}
\end{array}
$$

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

- $I_1 : \quad x = y$
- $I_2 : \quad x + y = 2$
- $I_3 : \quad 3 * x + y = 4$

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.

(10 points)

(b) Consider the following rule in Hoare logic:

$$\frac{\{A \wedge b\}\ p\ \{B\}}{\{A\}\textbf{if } b \textbf{ then } p \textbf{ else abort } \{B\}}$$

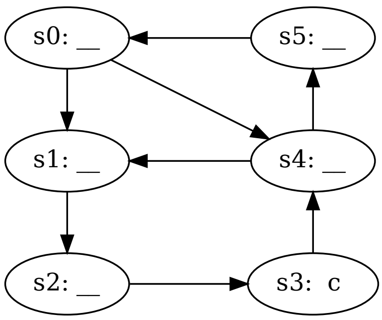
where A, B are assertions, b is a Boolen expression, and p is an IMP program.

Is this rule sound? If yes, give a formal proof. Otherwise, give a counterexample.

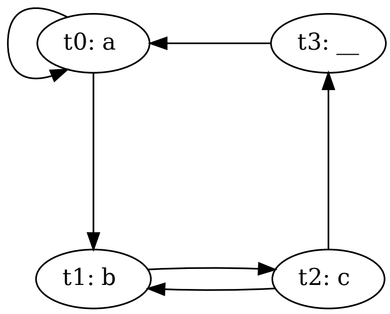
(5 points)

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. Some labels are given, for example state t_0 has label a. On the other hand most labels in M_1 as well as the label of t_3 in M_2 are missing. Assume that each state is labeled with a singular label a, b or c.

Kripke structure M_1:



Kripke structure M_2:

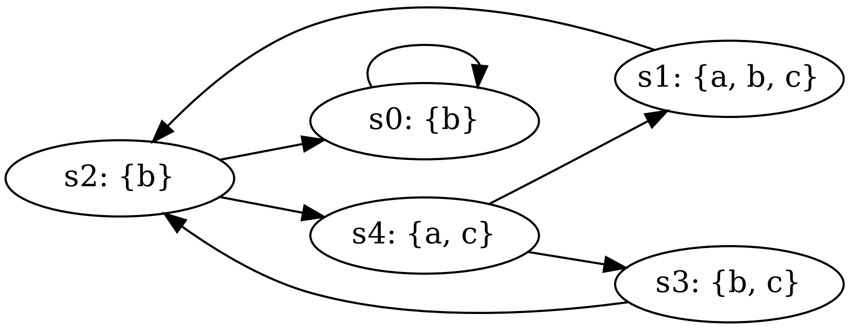


i. Fill in the missing labels such that M_2 simulates M_1. Is there more than one possible solution?

ii. Argue why it is not possible to fill the missing labels such that M_1 simulates 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 $M, s_i \models \varphi$?
(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
$\mathbf{F}(b \wedge c)$	☐	☐	☐	
$((b \wedge c)\ \mathbf{U}\ (a))$	☐	☐	☐	
$\mathbf{EG}(b)$	☐	☐	☐	
$\mathbf{EX}(a \wedge c)$	☐	☐	☐	
$\mathbf{E}[(b)\ \mathbf{U}\ (a)]$	☐	☐	☐	

(5 points)

(c) Prove that the following LTL-formulas are tautologies, i.e., they hold for every Kripke structure M and every path π in M, or find a Kripke structure M and path π in M, for which the formula does not hold and justify your answer.

i. $((\mathbf{F}a)\ \mathbf{U}\ b) \to \mathbf{F}(b \land \mathbf{F}a)$.

ii. $\mathbf{F}(b \land \mathbf{F}a) \to ((\mathbf{F}a)\ \mathbf{U}\ b)$.

(6 points)

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