1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik
185.291 October, 28 2022

Kennzahl (study id)	Matrikelnummer (student id)	Familienname (family name)	Vorname (first name)	Gruppe (version)
				A

1.) Consider the following problem.

1-in-3 HITTING SET

INSTANCE: A collection $\mathcal{C}$ of sets of elements, where every $C \in \mathcal{C}$ has exactly 3 elements.

QUESTION: Does there exist a set S of elements, such that for each $C \in \mathcal{C}$, $|S \cap C| = 1$, i.e., each set in $\mathcal{C}$ contains exactly one element from S?

(a) The following function f provides a polynomial-time many-one reduction from the problem **1-in-3 HITTING SET** to **SATISFIABILITY**: for a collection $\mathcal{C}$ of sets of elements, where for every $C \in \mathcal{C}$, $|C| = 3$, let $f(\mathcal{C}) = \varphi$ with

$$\varphi = \bigwedge_{\{c_1,c_2,c_3\}\in\mathcal{C}} \Big((c_1 \vee c_2 \vee c_3) \wedge (\neg c_1 \vee \neg c_2) \wedge (\neg c_2 \vee \neg c_3) \wedge (\neg c_1 \vee \neg c_3)\Big)$$

where we use, for each element c_i in $\mathcal{C}$ (i.e., $c_i \in \bigcup_{C\in\mathcal{C}} C$), a propositional variable c_i.

Show the correctness of the reduction, i.e., show:
$\mathcal{C}$ is a yes-instance of **1-in-3 HITTING SET** $\iff$ $f(\mathcal{C})$ is a yes-instance of **SATISFIABILITY**.

(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 **SATISFIABILITY** is NP-complete.

true	**false**	
○	○	The correctness of the reduction in (a) proves NP-hardness of **1-in-3 HITTING SET**.
○	○	The correctness of the reduction in (a) proves NP-membership of **1-in-3 HITTING SET**.
○	○	The correctness of the reduction in (a) proves P-membership of **1-in-3 HITTING SET**.
○	○	If we can show **1-in-3-HITTING SET** to be in P, we also would have shown P $\neq$ NP.
○	○	Any problem that can be reduced to **1-in-3 HITTING SET** is in NP.
○	○	The problem **1-in-3 HITTING SET** is semi-decidable.

(6 points)

2.) (a) Let $\mathcal{T}_E^{di}$ be a first-order theory containing all axioms of the theory of equality $\mathcal{T}_E$ (including substitution axiom schemes for p and f) and the two axioms:

$$\forall x\, \forall y\, \Big(p(x,y) \rightarrow \big(p(x, f(x,y)) \wedge p(f(x,y), y)\big)\Big) \qquad \text{(p-density)}$$

$$\forall x\ \neg p(x,x) \qquad \text{(p-irreflexivity)}$$

Recall that the substitution axiom for the predicate symbol p is

$$\forall v \forall w \forall x \forall y\ \big((v \doteq w \wedge x \doteq y) \rightarrow (p(v,x) \leftrightarrow p(w,y))\big).$$

Use the semantic argument method to prove that the formula

$$p(a,b) \wedge \big(a \doteq f(a,b) \vee a \doteq b\big)$$

is $\mathcal{T}_E^{di}$-unsatisfiable. **(10 points)**

(b) Apply the Sparse Method including preprocessing to the E-formula φ to obtain an equi-satisfiable formula ψ in propositional logic.

$$\varphi : \quad \big[(x_1 \doteq x_5 \wedge x_5 \doteq x_3) \vee \neg(x_2 \doteq x_3 \rightarrow x_1 \doteq x_2)\big] \wedge (x_5 \doteq x_4 \rightarrow x_4 \not\doteq x_3)$$

Please indicate and justify briefly the steps in the translation! **(5 points)**

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

$$
\begin{array}{l}
x := 0; z := 0; \\
\textbf{while } x \neq y \textbf{ do} \\
\quad z := z + 2 * x; \\
\quad x := x + 1; \\
\textbf{od}
\end{array}
$$

Give a loop invariant and variant for the **while** loop in p and prove the validity of the total correctness triple $[y > 0]\ p\ [x^2 = z + y]$.

(10 points)

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

$$\textbf{if } x \neq y \textbf{ then } x := x + x \textbf{ else } x := x + y$$

Which of the following Hoare triples are correct? If the triple is correct, provide a short justification for your answer. If the triple is not correct, give a counterexample.

(i) $\{x = 2\}\ p\ \{x = 4\}$

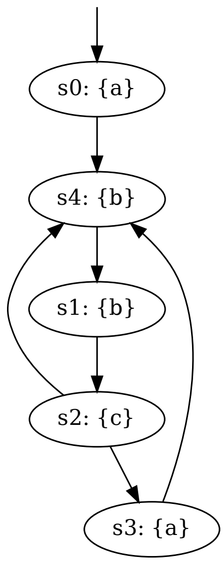
(ii) $\{x \geq 2\}\ p\ \{x = 4\}$

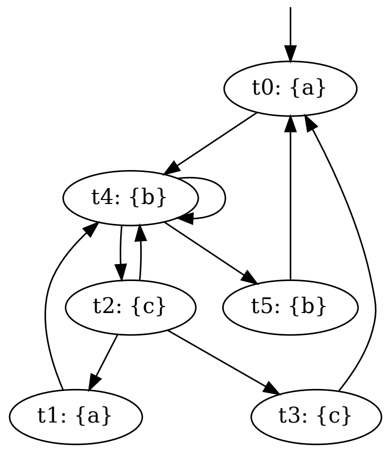
(iii) $\{x = 0\}\ p\ \{x > 0\}$

(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.

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) For each of the following formulas φ, provide a Kripke structure M for which $M \models \varphi$.

Note: Make sure to clearly mark initial states.

i. $\mathbf{AXEG}c \wedge \mathbf{E}(a\ \mathbf{U}\ \neg c)$

ii. $\mathbf{AG}(\mathbf{EF}p \wedge \mathbf{EF}\neg p)$

iii. $\mathbf{E}(\mathbf{G}c \wedge \mathbf{GF}b \wedge (a\ \mathbf{U}\ \neg b))$

(6 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. $((\neg a \wedge \neg b)\ \mathbf{U}\ (a \vee b)) \Rightarrow (\mathbf{GF}a \wedge \mathbf{GF}b)$

ii. $(\mathbf{GF}a \wedge \mathbf{GF}b) \Rightarrow ((\neg a \wedge \neg b)\ \mathbf{U}\ (a \vee b))$

(5 points)