1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik 185.291 January, 21 2022				
Kennzahl (study id)	Matrikelnummer (student id)	Familienname (family name)	Vorname (first name)	Gruppe (version) **A**

1.) Recall the **HALTING** problem which takes a program and a string as input, and consider the following variant thereof:

> **HALTING-EVEN**
>
> INSTANCE: A program Π that takes a string as input, a string I.
>
> QUESTION: Does Π terminate on I in an even number of computation steps.

(a) The following function f provides a polynomial-time many-one reduction from **HALTING** to **HALTING-EVEN**: for a program Π and a string I let $f(\Pi, I) = (\Pi', I')$ with $I' = I$ and Π' given as follows:

```
Π′(string S){
  call Π(S);
  call Π(S);
  return;
}
```

(Remark: We assume that calls and return-statements do not count as computation steps).

Show that (Π, I) is a yes-instance of **HALTING** $\iff$ (Π', I') is a yes-instance of **HALTING-EVEN**.

(9 points)

(b) Please answer the following questions and explain your answers

- Is **HALTING-EVEN** undecidable?
- Is **HALTING-EVEN** semi-decidable?

(6 points)

2.) (a) 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 $\neg z$).

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

(i) Reconstruct φ from $\hat{\delta}(\varphi)$.

(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!

(7 points)

(b) Let $\mathcal{T}_f^E$ be the theory containing all equality axioms (from $\mathcal{T}_E$) and the following two additional axioms.

- $\forall x \forall y\, (f(x) \doteq f(y) \;\rightarrow\; x \doteq y)$ (f-injectivity)
- $\forall x\, f(x) \doteq f(f(x))$ (f-idempotency)

Clarify the logical status of each of the following formulas. If one is $\mathcal{T}_f^E$-valid or $\mathcal{T}_f^E$-unsatisfiable, then prove it using the semantic argument method. If one is $\mathcal{T}_f^E$-satisfiable but not $\mathcal{T}_f^E$-valid, then present a satisfying and a falsifying interpretation. Argue formally that the formula evaluates to true resp. false under the constructed interpretations.

$$\varphi\colon \quad f(f(f(a))) \doteq f(b) \;\rightarrow\; a \doteq b$$
$$\psi\colon \quad f(f(f(a))) \not\doteq f(f(b)) \;\wedge\; a \doteq b$$

(8 points)

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

while $i < 10$ **do**
$x := x - 2 * i;$
$i := i + 1;$
$y := y + 2 * i;$
od

Give a loop invariant for the **while** loop in p and prove the validity of the total correctness triple $[i = 0 \wedge x = 100 \wedge y = 0]\ p\ [x + y = 120]$.

(10 points)

(b) Let p be the IMP program:

$$\textbf{if } 2 * x \geq y \textbf{ then } x := x + 2 \textbf{ else } y := y - 2$$

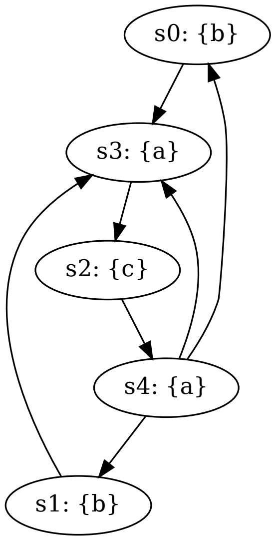
What is the $wlp(p, x = 4 \wedge y = 2)$? **(3 points)**

(c) Let p be an IMP program such that $[2 * x \geq y]\ p\ [x \neq y]$ is valid.
Is $[x = 2 \wedge y = 1]\ p\ [2 * y - 2 * x \neq 0]$ valid? If so, give a formal proof. Otherwise, give a counterexample.

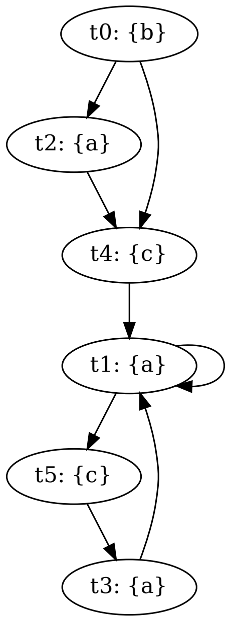
(2 points)

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:

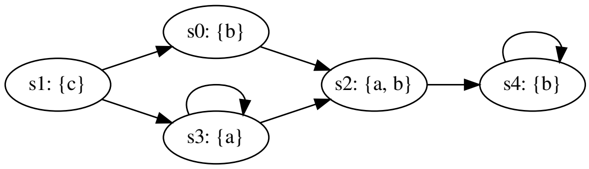


i. Briefly explain why M_2 does not simulate M_1.

ii. Add a minimal set of edges to M_2 such that the extended Kripke structure M_2' simulates M_1. Provide the additional edges and a non-empty simulation relation H that witnesses $M_1 \preceq M_2'$.

(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
$\mathbf{G}(b)$	☐	☐	☐	
$\mathbf{E}[(a)\ \mathbf{U}\ (b)]$	☐	☐	☐	
$\mathbf{X}(c)$	☐	☐	☐	
$\mathbf{EF}(b)$	☐	☐	☐	
$\mathbf{AF}(a \wedge b)$	☐	☐	☐	

(5 points)

(c) **LTL tautologies**

Prove that the following 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. $\mathbf{G}(a \Rightarrow \mathbf{F}b) \Rightarrow (\mathbf{GF}a) \wedge (\mathbf{GF}b)$

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

(6 points)