1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik

185.291 **January, 29 2021**

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

1.) Recall the NP-complete problem **SAT** and its specialization **3SAT** which is also NP-complete:

> **3SAT**
>
> INSTANCE: A propositional formula φ in 3-CNF, i.e. of the form $\bigwedge_{i=1}^{n}(l_{i1} \lor l_{i2} \lor l_{i3})$.
>
> QUESTION: Does there exists a truth assignment T that makes φ true?

Now consider the following further restriction:

> **3SATX**
>
> INSTANCE: A propositional formula φ in 3-CNF, where each variable occurs negatively at most two times (i.e., at most two times in the scope of negation).
>
> QUESTION: Does there exists a truth assignment T that makes φ true?

(a) The following function f provides a polynomial-time many-one reduction from **3SAT** to **3SATX**: for a formula $\varphi = \bigwedge_{i=1}^{n}(l_{i1} \lor l_{i2} \lor l_{i3})$ over variables V let

$$f(\varphi) = \Big(\bigwedge_{v \in V} \big((\neg v \lor \neg v \lor \neg \bar{v}) \land (v \lor v \lor \bar{v}) \big) \land \bigwedge_{i=1}^{n} (l^*_{i1} \lor l^*_{i2} \lor l^*_{i3}) \Big)$$

where $l^*_{ij} = v$ if $l_{ij} = v$ and $l^*_{ij} = \bar{v}$ if $l_{ij} = \neg v$ (i.e., we replace each literal $\neg v$ in φ by $\bar{v}$ for all $v \in V$).

It can be shown that φ is a yes-instance of **3SAT** $\Longleftrightarrow$ $f(\varphi)$ is a yes-instance of **3SATX**. Provide a proof for the $\Longrightarrow$ direction.

(9 points)

(b) Tick the correct statements (for ticking a correct statement a certain number of points is given; ticking an incorrect statement results in a substraction of the same amount; you cannot go below 0 points):

- ○ Since **3SAT** is NP-hard, our reduction from (a) shows that **3SATX** is in NP.
- ○ Since **3SAT** is NP-hard, our reduction from (a) shows that **3SATX** is NP-hard.
- ○ Since **3SAT** is in NP, our reduction from (a) shows that **3SATX** is NP-hard.
- ○ Since **3SATX** is a special case of **SAT**, **3SATX** must be contained in NP.
- ○ Since **3SATX** is a special case of **3SAT**, **3SATX** must be contained in NP.
- ○ Since **3SATX** is a special case of **3SAT**, **3SATX** must be NP-hard.

(6 points)

2.) (a) We consider the theory $\mathcal{T}_A$ of arrays from the lecture.

i. What is the signature of this theory?
ii. What kinds of axioms are available in this theory? Please name them.
iii. Consider a $\mathcal{T}_A$-formula ψ and suppose that ψ is not valid. What is a counter-example to $\mathcal{T}_A$-validity of ψ and what properties has this counter-example to satisfy?

(4 points)

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

$$\varphi : \quad \big(\forall j \; a[j] \doteq b\langle i \triangleleft v\rangle[j]\big) \rightarrow a[i] \doteq v \ .$$

If φ is $\mathcal{T}_A$-valid, then provide a proof in the semantic argument method (similarly to the proofs in the lecture and on the extra sheets). If φ is not $\mathcal{T}_A$-valid, then provide a counter-example.

Besides the equality axioms reflexivity, symmetry and transitivity, you have the following ones for arrays.

- $\forall a, i, j \; \big(i \doteq j \rightarrow a[i] \doteq a[j]\big)$ (array congruence)
- $\forall a, v, i, j \; \big(i \doteq j \rightarrow a\langle i \triangleleft v\rangle[j] \doteq v\big)$ (read-over-write 1)
- $\forall a, v, i, j \; \big(i \neq j \rightarrow a\langle i \triangleleft v\rangle[j] \doteq a[j]\big)$ (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. **(11 points)**

3.) (a) Let p be the following program:

$$
\begin{array}{l}
x := 0; z := 0; y := 0; \\
\textbf{while } y < n \textbf{ do} \\
\quad x := x + 2; \\
\quad z := z + 5; \\
\quad y := y + 1 \\
\textbf{od}
\end{array}
$$

Give a loop invariant for the **while** loop in p and prove the validity of the partial correctness triple $\{n > 1\}\ p\ \{z - x = 3 * n\}$.

(9 points)

(b) Let p be the following program:

$$
\begin{array}{l}
\textbf{while } a > 0 \wedge b > 0 \textbf{ do} \\
\quad \textbf{if } a > b \textbf{ then} \\
\quad\quad a := a - b; \\
\quad \textbf{else} \\
\quad\quad b := b - a \\
\textbf{od}
\end{array}
$$

Provide a loop variant t for the **while** loop in p strong enough to prove the validity of the total correctness triple $[a \geq 0 \wedge b \geq 0]\ p\ [a = 0 \vee b = 0]$. You may assume the invariant to be *true*.

You are **not** required to write a proof here, just state a suitable variant.

(2 points)

(c) Is the following theorem correct?

"For all assertions A, B and programs p, it holds that $\{A\}\ p\ \{B\}$ is valid if and only if $(VC(p, B)\ \wedge\ (A\ \Rightarrow\ wlp\,(p, B))\ )$. "

If it is, give an argument why. If not, what is wrong?

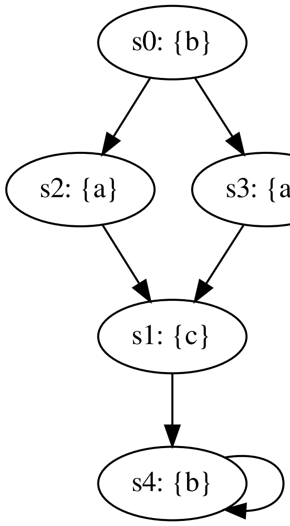
Be concise and write no more than 1-2 sentences. **(2 points)**

(d) Let n, m be integer-valued constants and A an assertion. Is there a state σ such that $\sigma \models [n \neq m]$ `abort` $[A]$? If so, provide such a state σ. If, not, explain why there exists no such σ.

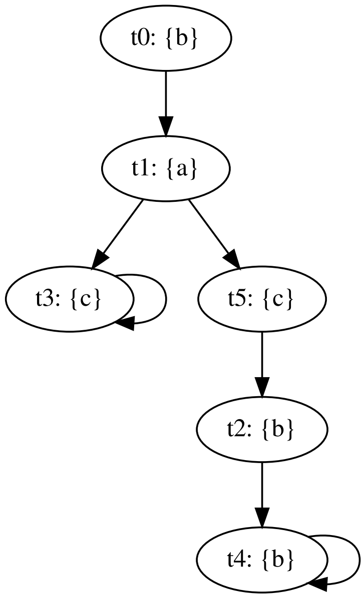
(2 points)

4.) (a) Provide a non-empty simulation relation H that witnesses $M_1 \leq M_2$, where M_1 and M_2 are shown below. The initial state of M_1 is s_0, the initial state of M_2 is t_0:

Kripke structure M_1:

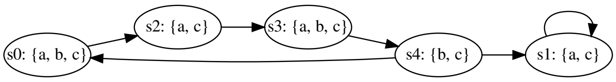


Kripke structure M_2:



(4 points)

(b) Consider the following Kripke structure M:



For each of the following formulae φ,

i. check the respective box if 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 $M, s_i \models \varphi$?
Hint: 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
$\mathbf{G}(a)$	☐	☐	☐	
$\mathbf{E}[(a)\ \mathbf{U}\ (b)]$	☐	☐	☐	
$\mathbf{F}(a \wedge b)$	☐	☐	☐	
$\mathbf{AF}(c)$	☐	☐	☐	
$\mathbf{X}(b)$	☐	☐	☐	

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

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

(6 points)