| 1 | 2 | 3 | 4 | Σ | Grade |
|---|---|---|---|---|---|
| | | | | | |

# 6.0/4.0 VU Formale Methoden der Informatik

**185.291** **January, 24 2023**

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

**1.)** For this exercise assume that every instance of **3-COLORABILITY** has **at least one edge** (the problem remains NP-complete with this constraint).

A 5-star is any graph that is isomorphic to $G_{Star5} = (V_5, E_5)$ with $V_5 = \{1, 2, 3, 4, 5, 6\}$, $E_5 = \{(1, 2), (1, 3), (1, 4), (1, 5), (1, 6)\}$, i.e., a graph with one "center" vertex that has an edge to each of the five "outer" vertices.

Consider the following problem.

> **5-STAR-3-COL**
>
> INSTANCE: A graph $G = (V, E)$ that contains a 5-star as a sub-graph.
>
> QUESTION: Does there exist a valid 3-coloring for $G$, i.e., a function $\mu$ 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** (with at least one edge) to **5-STAR-3-COL**: for a graph $G = (V, E)$ with $E \neq \emptyset$, let $(a, b) \in E$ be an arbitrary edge of $G$. We define $f(G) = G'$ with $G' = (V', E')$, where

$$V' = V \cup \{a_1, a_2, a_3, a_4\}$$
$$E' = E \cup \{(a, a_1), (b, a_1), (a_1, a_2), (a_1, a_3), (a_1, a_4)\}$$

for fresh vertices $a_1, a_2, a_3, a_4$.

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 **5-STAR-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** (where every instance has at least one edge) is NP-complete.

| **true** | **false** | |
|---|---|---|
| ○ | ○ | The correctness of the reduction in (a) proves NP-hardness of **5-STAR-3-COL**. |
| ○ | ○ | The correctness of the reduction in (a) proves coNP-membership of **5-STAR-3-COL**. |
| ○ | ○ | The correctness of the reduction in (a) proves undecidability of **5-STAR-3-COL**. |
| ○ | ○ | If we can show **5-STAR-3-COL** to be in P, we also would have shown P = NP. |
| ○ | ○ | A polynomial-time many-one reduction from **5-STAR-3-COL** to **3-COLORABILITY**would show NP-membership for **5-STAR-3-COL**. |
| ○ | ○ | A polynomial-time many-one reduction from **5-STAR-3-COL** to **3-COLORABILITY**would show P-membership for **5-STAR-3-COL**. |

**(6 points)**

**2.)** (a) Consider Peano arithmetic $PA$ with signature $\Sigma_{PA} = \big\{\{0, 1, +, \cdot\}, \{\doteq\}\big\}$. Here we need only the induction axiom scheme from $PA$ and four additional axioms:

$$F[0] \land \big(\forall x\ (F[x] \rightarrow F[x+1])\big) \rightarrow \forall x\ F[x] \qquad \text{(induction)}$$
$$\forall x\ (x^0 \doteq 1) \qquad \text{(exp zero)}$$
$$\forall x\ \forall y\ (x^{y+1} \doteq x^y \cdot x) \qquad \text{(exp succ)}$$
$$\forall x\ \forall z\ (exp_3(x, 0, z) \doteq z) \qquad (exp_3 \text{ zero})$$
$$\forall x\ \forall y\ \forall z\ \big(exp_3(x, y+1, z) \doteq exp_3(x, y, x \cdot z)\big) \qquad (exp_3 \text{ succ})$$

The extended theory is called $\mathcal{T}_{PA}^{+}$. Show the following:

$$\forall x \forall y \forall z\ (exp_3(x, y, z) \doteq x^y \cdot z) \quad \text{is } \mathcal{T}_{PA}^{+}\text{-valid.}$$

**Hints:** Use $F[y]\colon \forall x \forall z\ \big(exp_3(x, y, z) \doteq x^y \cdot z\big)$ and perform induction on $y$.

i. Base case: Formally prove $F[0]$ using the semantic argument method.
ii. State precisely the induction hypothesis.
iii. Perform the step case. Again use the semantic argument method.

In order to simplify the proofs, you may use the formulas $(L)\colon \forall x\ (1 \cdot x \doteq x)$ and $(A)\colon \forall x \forall y \forall z\ \big((x \cdot y) \cdot z \doteq x \cdot (y \cdot z)\big)$ as additional lemmas.

Please be precise and indicate exactly why proof lines follow from some other(s). Moreover, recall that equality handling is performed using equality axioms.

**(12 points)**

(b) Consider the following ternary variant of the propositional resolution rule.

$$\frac{C \vee p \vee q \qquad D \vee \neg p \qquad E \vee \neg q}{C \vee D \vee E}$$

Show that every model of the rule's premise clauses is a model of the rule's conclusion clause. **(3 points)**

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

$$
\begin{array}{l}
x := 0; y := 4 * n; z := n; \\
\textbf{while } z > 0 \textbf{ do} \\
\quad x := x + 2; \\
\quad y := y - 4 * x; \\
\quad z := z - 1 \\
\textbf{od}
\end{array}
$$

Give a loop invariant and variant for the **while** loop in $p$ and prove the validity of the total correctness triple $[n > 1]\ p\ [y + x^2 = 0]$.

**Note:** Make sure that your invariant expresses equalities among $x, y, z$.

**(10 points)**

(b) Consider the partial correctness triple $\{x > 2 \wedge y > 1\}\ x = x + y\ \{x > 3\}$. Answer the following questions about this triple and justify your claims.

i. Is the triple provable in the Hoare calculus, that is

$$\vdash \{x > 2 \wedge y > 1\}\ x = x + y\ \{x > 3\} \quad ?$$

ii. Is the triple provable in Hoare calculus without the rule of consequence?

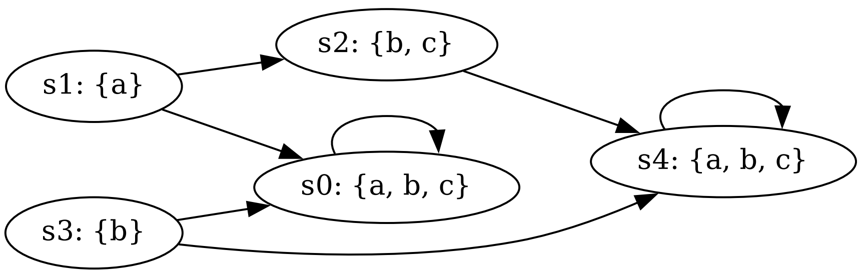
iii. Is the triple valid, that is

$$\models \{x > 2 \wedge y > 1\}\ x = x + y\ \{x > 3\} \quad ?$$

**(5 points)**

**4.)** (a) Find a Kripke structure $K$ with initial state $s_0$ that has the properties $\mathbf{AGEF}p$ and $\mathbf{A}\,(\mathbf{GF}p \Leftrightarrow \mathbf{GF}q)$ at state $s_0$, but not $\mathbf{AGAF}p$. Justify your choice. **(4 points)**

(b) Consider the following Kripke structure $M$:




For each of the following formulae $\varphi$,

i. indicate whether the formula is in CTL, LTL, and/or CTL*, and

ii. list the states $s_i$ on which the formula $\varphi$ holds; i.e. for which states $s_i$ do we have $M, s_i \models \varphi$?
(If $\varphi$ is a path formula, list the states $s_i$ such that $M, s_i \models \mathbf{A}\varphi$.)

| $\varphi$ | CTL | LTL | CTL* | States $s_i$ |
|---|---|---|---|---|
| $\mathbf{AX}\,a$ | ☐ | ☐ | ☐ | |
| $(b\ \mathbf{U}\ \neg a)$ | ☐ | ☐ | ☐ | |
| $\mathbf{X}(\neg a \wedge b)$ | ☐ | ☐ | ☐ | |
| $\mathbf{EG}(a \wedge b)$ | ☐ | ☐ | ☐ | |
| $\mathbf{A}[(\mathbf{EX}\,\neg b)\ \mathbf{U}\ c]$ | ☐ | ☐ | ☐ | |

**(5 points)**

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

i. $\mathbf{G}(p \Rightarrow \mathbf{X}(q)) \Rightarrow \mathbf{F}(p \Rightarrow \mathbf{F}(q))$

ii. $\mathbf{F}(p \Rightarrow \mathbf{F}(q)) \Rightarrow \mathbf{G}(p \Rightarrow \mathbf{X}(q))$

**(6 points)**

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