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

# 6.0/4.0 VU Formale Methoden der Informatik

**185.291 October 31, 2023**

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

**1.)** Recall from the lecture the NP-complete problem **SAT** and its specialization **3-SAT**, that is also NP-complete:

> **SAT**
>
> INSTANCE: A propositional formula $\varphi$.
>
> QUESTION: Is $\varphi$ satisfiable?

> **3-SAT**
>
> INSTANCE: A propositional formula $\varphi$ in 3-CNF, i.e., of the form $\bigwedge_{i=1}^{n}(l_{i1} \vee l_{i2} \vee l_{i3})$.
>
> QUESTION: Is $\varphi$ satisfiable?

For this exercise, assume that instances of **3-SAT** are restricted to those in which no variable occurs twice in the same clause (the problem remains NP-complete under this restriction).

Consider now the following variant of **SAT**.

> **($\leq$3,3)-SAT**
>
> INSTANCE: A propositional formula $\varphi$ in CNF, where each clause consists of at most 3 literals over pairwise distinct variables and each variable has at most 3 occurrences.
>
> QUESTION: Is $\varphi$ satisfiable?

(This page contains no exercise, answer problems (a) and (b) on the following pages.)

(a) The following describes a polynomial-time many-one reduction from **3-SAT** to **(≤3,3)-SAT**: Consider $\varphi = \bigwedge_{i=1}^{n}(l_{i1} \vee l_{i2} \vee l_{i3})$ over variables $V$. Let $V' \subseteq V$ be the set of all variables that occur more than 3 times in $\varphi$. For each $x \in V'$, we do the following. Let $k$ be the number of occurrences of $x$ in $\varphi$:

**Step 1:** Introduce $k$ *new* variables $x_1, \ldots, x_k$, and replace the $i$th occurrence of $x$ in $\varphi$ with $x_i$, for all $i = 1, \ldots, k$.

**Step 2:** Append clauses $(x_i \vee \neg x_{i+1})$, $i = 1, \ldots, k-1$, as well as $(x_k \vee \neg x_1)$ to the resulting formula of Step 2.

Let $\varphi'$ be the formula obtained from $\varphi$ by applying the two steps listed above, for each $x \in V'$.

It holds that $\varphi$ is a positive instance of **3-SAT** $\iff$ $\varphi'$ is a positive instance of **(≤3,3)-SAT**. Show the $\Longrightarrow$ direction of the claim.

**(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 both **3-SAT** and **SAT** are NP-complete problems.

| **true** | **false** | |
|---|---|---|
| ○ | ○ | The correctness of the reduction in (a) proves that **($\leq$3,3)-SAT** is NP-hard. |
| ○ | ○ | The correctness of the reduction in (a) proves that **($\leq$3,3)-SAT** is in NP. |
| ○ | ○ | Every instance of **($\leq$3,3)-SAT** is an instance of **3-SAT**. |
| ○ | ○ | Every instance of **($\leq$3,3)-SAT** is an instance of **SAT**. |
| ○ | ○ | If we can show **($\leq$3,3)-SAT** to be in P, we would also show P=NP. |
| ○ | ○ | Any problem that can be reduced to **($\leq$3,3)-SAT** in polynomial time is in NP. |

**(6 points)**

**2.)** (a) Consider the function M, defined as follows.

**Input:** $x$, $y$, two *positive* integers
**Output:** The computed positive integer value for $x$, $y$
**if** $x == 1$ **then**
  **return** $2y$;
**end**
**else if** $y == 1$ **then**
  **return** $x$;
**end**
**else return** $\mathrm{M}(x-1, \mathrm{M}(x, y-1))$;

**Algorithm 1:** The function M

Let $\mathbb{N}$ denote the natural numbers *without* 0. Use well-founded induction to show

$$\forall x \, \forall y \, \big((x \in \mathbb{N} \wedge y \in \mathbb{N}) \;\rightarrow\; \mathrm{M}(x, y) \geq 2y\big).$$

**(11 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.

- 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!

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

**(4 points)**

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

$$
\begin{array}{l}
\textbf{while } x \neq x+1 \textbf{ do} \\
\quad x := x+1; \\
\quad y := y + 6 * x - 3; \\
\textbf{od}
\end{array}
$$

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

- $I_1: \quad y > x$
- $I_2: \quad y = 3 * x^2$
- $I_3: \quad y < x$

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 and justify your answer.

**(9 points)**

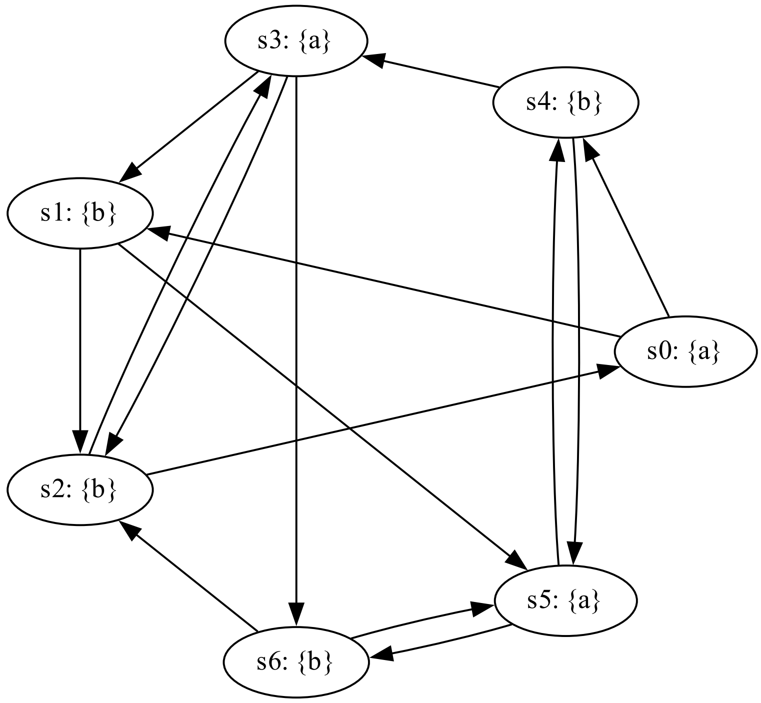
(b) Consider the following rule in Hoare logic:

$$\frac{\{A\}\ x := x + 1\ \{B\}}{\{A\}\ \textbf{skip};\ \textbf{if}\ \mathit{true}\ \textbf{then}\ x := x + 1\ \textbf{else skip}\ \{B\}}$$

where $A, B$ are assertions and $x$ is an integer-valued IMP program variable. Is this rule sound? If yes, give a formal proof. Otherwise, give a counterexample and justify your answer.

**(6 points)**

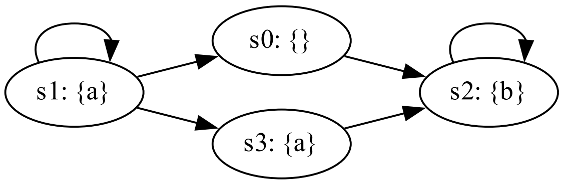
**4.)** (a) Consider the following Kripke structure $M$ with initial state $s_0$:




Give the smallest (i.e. having the minimal number of states) Kripke structure $K$ such that $M \equiv K$, i.e. there is a bisimulation between $M$ and $K$. Provide a bisimulation relation that witnesses $M \equiv K$.

**(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 $s_i$ |
|---|---|---|---|---|
| $a \vee b$ | ☐ | ☐ | ☐ | |
| $\mathbf{FG}(a \vee b)$ | ☐ | ☐ | ☐ | |
| $\mathbf{EFG}a$ | ☐ | ☐ | ☐ | |
| $\mathbf{EFAG}a$ | ☐ | ☐ | ☐ | |
| $a\ \mathbf{U}\ b$ | ☐ | ☐ | ☐ | |

**(5 points)**

(c) **CTL* tautologies**

Prove that the following formulas are tautologies, i.e., they hold for every Kripke structure $M$ and initial state $s$, or find a Kripke structure $M$ with an initial state $s$, for which the formula does not hold and justify your answer.

i. $\mathbf{AFG}a \Rightarrow \mathbf{AFAG}a$

ii. $\mathbf{AFAG}a \Rightarrow \mathbf{AFG}a$

**(6 points)**

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