Exercise	1.1	2.1	2.2	3.1	4.1	4.2	4.3	total
Points	15	5	10	15	5	5	5	60
reached								

6.0/4.0 VU Formale Methoden der Informatik
185.291 Oct., 19 2018

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

1 Foundations of complexity theory

Exercise 1.1

Consider the following decision problem: _____/ 15 p.

TRANSFORMED INPUT

INSTANCE: A tuple (Π_1, Π_2, I), where Π_1, Π_2 are programs and I is a string. Π_1 takes a string as input and outputs a string, and it is guaranteed that Π_1 terminates. Π_2 takes a string as input.

QUESTION: Does $\Pi_2(\Pi_1(I))$ hold, i.e. does Π_2 hold on the string that is delivered by Π_1 when called with string I?

1. By providing a suitable reduction from the **HALTING** problem, prove that the problem **TRANSFORMED INPUT** is undecidable.
2. Is **TRANSFORMED INPUT** semi-decidable? Explain your answer.

2 Satisfiability

Exercise 2.1

_____/5 p.

The topic of this exercise is *translation validation* (discussed in the fifth lecture of the second block). Given a statement in a source program of the form

$$z = (x_1 + y_1) * (x_2 + y_2) \tag{S}$$

and the result of the compiler of the form

$$u_1 = x_1 + y_1; \quad u_2 = x_2 + y_2; \quad z = u_1 * u_2\,. \tag{O}$$

The goal is to check the correctness of the translation.

1. Formulate the verification condition.

   _____ (VC)

2. Formulate the abstract verification condition (using uninterpreted functions).

   _____ (AVC)

3. Prove the correctness of the translation process (using the semantic proof method from the third lecture (on First-order Logc and Theories), or present a counter-example for (AVC).

Exercise 2.2

_____/ 10 p.

Prove: During the run of a SAT solver, the implication graph G_k at step k is acyclic.
Hints:

1. Perform a proof by induction on k.
2. Consider the following events that can occur:
   a) making a decision,
   b) unit propagation (one step of BCP),
   c) a clause is unsatisfiable,
   d) backtracking.

3 Deductive Verification of Programs

Exercise 3.1

_____/ 15 p.

Show that the following correctness assertion is true with respect to total correctness:

$$
\begin{array}{l}
\{F: \ x > 0 \ \wedge y > 0\} \\
\ r := y; \\
\ n := x; \\
\ \text{while } n > 0 \text{ do} \\
\quad\quad r := r + 2; \\
\quad\quad n := n - 1; \\
\text{od} \\
\quad \{G: \ r = 2 * x + y\}
\end{array}
$$

Use the formula $r = 2 * x + y - 2 * n \ \wedge 0 \leq n$ as loop invariant and choose an appropriate variant.

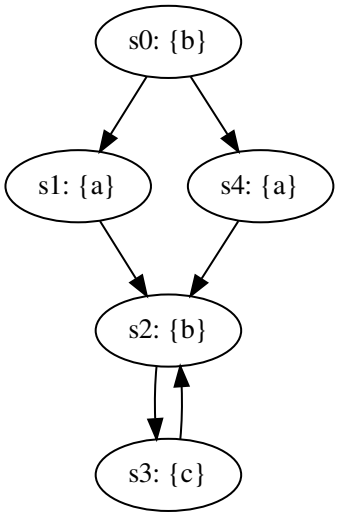
4 Model checking

Exercise 4.1

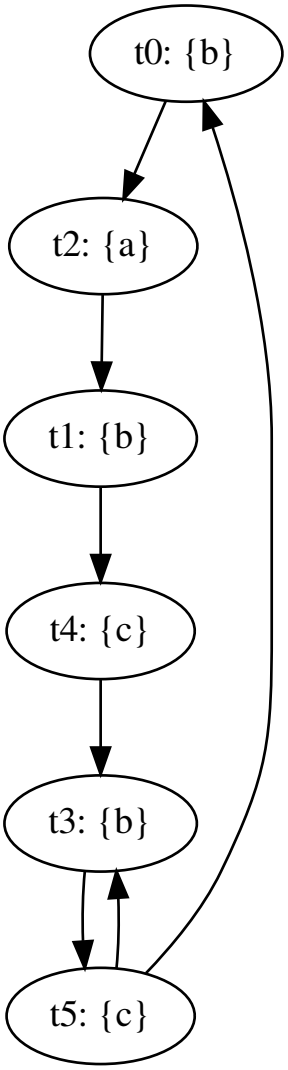
_____/5 p.

Provide a 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:



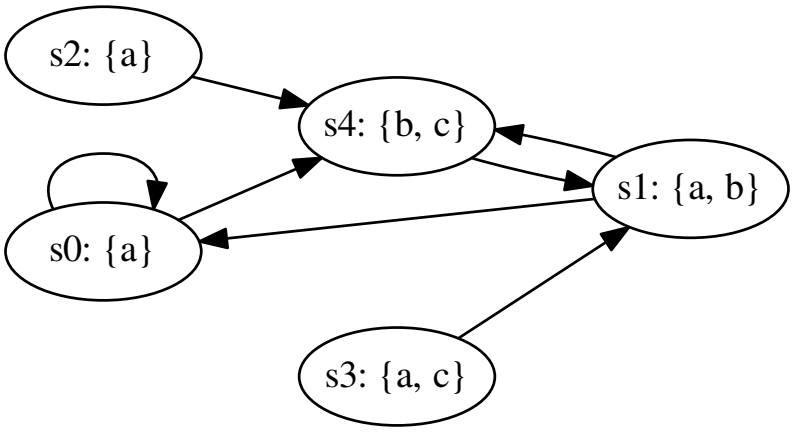
Kripke structure M_2:



Exercise 4.2

_____/5 p.

Consider the following Kripke structure M:



For each of the following formulae φ,

1. check the respective box if the formula is in CTL, LTL, and/or CTL*, and
2. list the states s_i on which the formula φ holds; i.e. for which states s_i do we have $M, s_i \models \varphi$?

Note that by a CTL* formula, we here mean a CTL* *state* formula *or* a CTL* *path* formula. Also recall that for an LTL formula φ we have $M, s \models \varphi$ if and only if $\pi \models \varphi$ for *all* paths in M that start at s.

φ	CTL	LTL	CTL*	States s_i
$\mathbf{G}(a)$	☐	☐	☐	
$\mathbf{G}(b)$	☐	☐	☐	
$\mathbf{G}(c)$	☐	☐	☐	
$\mathbf{G}(a \wedge b)$	☐	☐	☐	
$\mathbf{G}(a \wedge c)$	☐	☐	☐	
$\mathbf{G}(b \wedge c)$	☐	☐	☐	
$\mathbf{G}(a \wedge b \wedge c)$	☐	☐	☐	
$\mathbf{F}(a)$	☐	☐	☐	

$\mathbf{F}(b)$	☐	☐	☐
$\mathbf{F}(c)$	☐	☐	☐
$\mathbf{F}(a \wedge b)$	☐	☐	☐
$\mathbf{F}(a \wedge c)$	☐	☐	☐
$\mathbf{F}(b \wedge c)$	☐	☐	☐
$\mathbf{F}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{X}(a)$	☐	☐	☐
$\mathbf{X}(b)$	☐	☐	☐
$\mathbf{X}(c)$	☐	☐	☐
$\mathbf{X}(a \wedge b)$	☐	☐	☐
$\mathbf{X}(a \wedge c)$	☐	☐	☐
$\mathbf{X}(b \wedge c)$	☐	☐	☐
$\mathbf{X}(a \wedge b \wedge c)$	☐	☐	☐
$((a)\ \mathbf{U}\ (a))$	☐	☐	☐
$((b)\ \mathbf{U}\ (c))$	☐	☐	☐
$((c)\ \mathbf{U}\ (a))$	☐	☐	☐
$((a \wedge b)\ \mathbf{U}\ (c))$	☐	☐	☐
$((a \wedge c)\ \mathbf{U}\ (c))$	☐	☐	☐
$((b \wedge c)\ \mathbf{U}\ (c))$	☐	☐	☐
$((a \wedge b \wedge c)\ \mathbf{U}\ (b))$	☐	☐	☐
$\mathbf{AG}(a)$	☐	☐	☐
$\mathbf{AG}(b)$	☐	☐	☐
$\mathbf{AG}(c)$	☐	☐	☐
$\mathbf{AG}(a \wedge b)$	☐	☐	☐
$\mathbf{AG}(a \wedge c)$	☐	☐	☐
$\mathbf{AG}(b \wedge c)$	☐	☐	☐
$\mathbf{AG}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{AF}(a)$	☐	☐	☐
$\mathbf{AF}(b)$	☐	☐	☐
$\mathbf{AF}(c)$	☐	☐	☐
$\mathbf{AF}(a \wedge b)$	☐	☐	☐
$\mathbf{AF}(a \wedge c)$	☐	☐	☐
$\mathbf{AF}(b \wedge c)$	☐	☐	☐

$\mathbf{AF}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{AX}(a)$	☐	☐	☐
$\mathbf{AX}(b)$	☐	☐	☐
$\mathbf{AX}(c)$	☐	☐	☐
$\mathbf{AX}(a \wedge b)$	☐	☐	☐
$\mathbf{AX}(a \wedge c)$	☐	☐	☐
$\mathbf{AX}(b \wedge c)$	☐	☐	☐
$\mathbf{AX}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{A}[(a)\ \mathbf{U}\ (c)]$	☐	☐	☐
$\mathbf{A}[(b)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{A}[(c)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{A}[(a \wedge b)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{A}[(a \wedge c)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{A}[(b \wedge c)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{A}[(a \wedge b \wedge c)\ \mathbf{U}\ (c)]$	☐	☐	☐
$\mathbf{EG}(a)$	☐	☐	☐
$\mathbf{EG}(b)$	☐	☐	☐
$\mathbf{EG}(c)$	☐	☐	☐
$\mathbf{EG}(a \wedge b)$	☐	☐	☐
$\mathbf{EG}(a \wedge c)$	☐	☐	☐
$\mathbf{EG}(b \wedge c)$	☐	☐	☐
$\mathbf{EG}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{EF}(a)$	☐	☐	☐
$\mathbf{EF}(b)$	☐	☐	☐
$\mathbf{EF}(c)$	☐	☐	☐
$\mathbf{EF}(a \wedge b)$	☐	☐	☐
$\mathbf{EF}(a \wedge c)$	☐	☐	☐
$\mathbf{EF}(b \wedge c)$	☐	☐	☐
$\mathbf{EF}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{EX}(a)$	☐	☐	☐
$\mathbf{EX}(b)$	☐	☐	☐
$\mathbf{EX}(c)$	☐	☐	☐
$\mathbf{EX}(a \wedge b)$	☐	☐	☐

$\mathbf{EX}(a \wedge c)$	☐	☐	☐
$\mathbf{EX}(b \wedge c)$	☐	☐	☐
$\mathbf{EX}(a \wedge b \wedge c)$	☐	☐	☐
$\mathbf{E}[(a)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{E}[(b)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{E}[(c)\ \mathbf{U}\ (c)]$	☐	☐	☐
$\mathbf{E}[(a \wedge b)\ \mathbf{U}\ (c)]$	☐	☐	☐
$\mathbf{E}[(a \wedge c)\ \mathbf{U}\ (a)]$	☐	☐	☐
$\mathbf{E}[(b \wedge c)\ \mathbf{U}\ (c)]$	☐	☐	☐
$\mathbf{E}[(a \wedge b \wedge c)\ \mathbf{U}\ (b)]$	☐	☐	☐

Exercise 4.3

_____/5 p.

LTL tautologies

Prove or disprove that the following formulas are tautologies, i.e., they hold for every Kripke structure M:

1. $$(\mathbf{G}p)\ \mathbf{U}\ (p \wedge q) \rightarrow \mathbf{F}(q\ \mathbf{U}\ p)$$

2. $$\mathbf{G}p \wedge \neg\mathbf{G}q \rightarrow p\ \mathbf{U}\ \neg q$$