6.0/4.0 VU Formale Methoden der Informatik (185.291)

October 20, 2017

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

1.) We provide next a reduction from **2-COLORABILITY** to **2-SAT**. Let $G = (V, E)$ be an arbitrary undirected graph (i.e. an arbitrary instance of **2-COLORABILITY**), where $V = \{v_1, \ldots, v_n\}$. For the reduction we use propositional variables $x_1, \ldots, x_n$. Then the instance φ_G of **2-SAT** resulting from G is defined as follows:

$$\varphi_G = \bigwedge_{[v_i,v_j]\in E} (x_i \vee x_j) \wedge (\neg x_i \vee \neg x_j).$$

Task: Prove the "⇒" direction in the proof of correctness of the reduction, i.e. prove the following statement: if G is a positive instance of **2-COLORABILITY**, then φ_G is a positive instance of **2-SAT**.

(15 points)

2.) (a) Let φ^{EUF} be the following EUF-formula:

$$\varphi^{EUF} := x = y \wedge f(x) = g(y) \wedge z = g(f(y)) \wedge z \neq g(f(x)) \wedge P(g(f(y)), x)$$

where f and g denote uninterpreted functions and P denotes an uninterpreted predicate. Is φ^{EUF} E-satisfiable or E-unsatisfiable?
Either provide a concrete E-interpretation showing that φ^{EUF} is E-satisfiable or a detailed proof showing that φ^{EUF} is E-unsatisfiable.

(5 points)

(b) Consider the EUF-formula φ^{EUF} from above (Exercise 2a):

$$\varphi^{EUF} := x = y \wedge f(x) = g(y) \wedge z = g(f(y)) \wedge z \neq g(f(x)) \wedge P(g(f(y)), x)$$

Apply Ackermann's reduction to obtain an E-formula φ^E from φ^{EUF} so that φ^E is *E-satisfiable* if and only if φ^{EUF} is *E-satisfiable.*
(**Attention:** here we consider satisfiability-equivalence, and not validity-equivalence.)

(10 points)

3.) Consider the following modified if-rule:

$$\frac{\{\,F \wedge e\,\}\, p\, \{\,G\,\} \quad \{\,F\,\}\, q\, \{\,G\,\}}{\{\,F\,\}\ \mathsf{if}\ e\ \mathsf{then}\ p\ \mathsf{else}\ q\ \mathsf{fi}\ \{\,G\,\}}\ \mathrm{if}'$$

(a) Show that this rule is admissible regarding partial correctness. **(4 points)**

(b) Show that the Hoare calculus for partial correctness is no longer complete, if we replace the regular if-rule by the modified one. **(7 points)**

(c) Characterize all programs p that satisfy $\mathrm{wp}(p, \mathrm{true}) = \mathrm{true}$, i.e., specify a condition such that the equation holds exactly when p satisfies this condition. **(4 points)**

A rule $\frac{X_1 \cdots X_n}{\{\,F\,\}\,p\,\{\,G\,\}}$ is *admissible regarding partial correctness*, if the conclusion $\{\,F\,\}\,p\,\{\,G\,\}$ is partially correct whenever all premises $X_1, \dots, X_n$ are valid formulas/partially correct assertions.

Hoare calculus for partial correctness:

$$\{\,F\,\}\,\mathsf{skip}\,\{\,F\,\}$$

$$\{\,F\,\}\,\mathsf{abort}\,\{\,G\,\}$$

$$\{\,F[v/e]\,\}\,v := e\,\{\,F\,\}$$

$$\frac{\{\,F\,\}\,p\,\{\,G\,\} \quad \{\,G\,\}\,q\,\{\,H\,\}}{\{\,F\,\}\,p;q\,\{\,H\,\}}$$

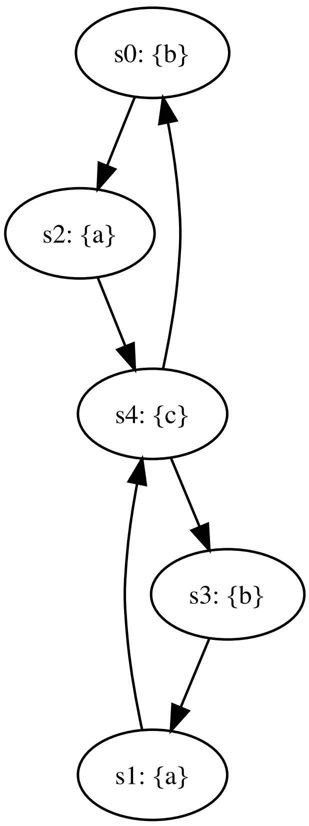
$$\frac{\{\,F \wedge e\,\}\,p\,\{\,G\,\} \quad \{\,F \wedge \neg e\,\}\,q\,\{\,G\,\}}{\{\,F\,\}\,\mathsf{if}\ e\ \mathsf{then}\ p\ \mathsf{else}\ q\ \mathsf{fi}\,\{\,G\,\}}$$

$$\frac{\{\,Inv \wedge e\,\}\,p\,\{\,Inv\,\}}{\{\,Inv\,\}\,\mathsf{while}\ e\ \mathsf{do}\ p\ \mathsf{od}\,\{\,Inv \wedge \neg e\,\}}$$

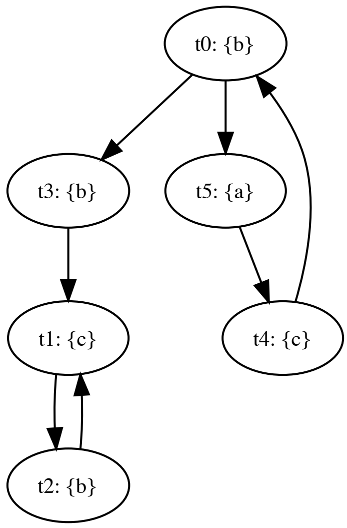
$$\frac{F \rightarrow F' \quad \{\,F'\,\}\,p\,\{\,G'\,\} \quad G' \rightarrow G}{\{\,F\,\}\,p\,\{\,G\,\}}$$

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:

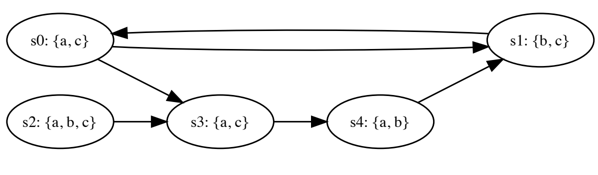


Kripke structure M_2:



(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 $M, s_i \models \varphi$?

φ	CTL	LTL	CTL*	States s_i
$\mathbf{F}(b \wedge c)$	☐	☐	☐	
$\mathbf{X}(a \wedge b \wedge c)$	☐	☐	☐	
$((b)\ \mathbf{U}\ (b))$	☐	☐	☐	
$\mathbf{EG}(c)$	☐	☐	☐	
$\mathbf{E}[(a \wedge b)\ \mathbf{U}\ (a)]$	☐	☐	☐	

(5 points)

(c) **CTL Model Checking Algorithm**

Let $K = (S, T, L)$ be a Kripke structure and let p be an atomic proposition. Give an algorithm that computes the set of all states $s \in S$ that satisfy $\mathbf{EG}p$.

(6 points)