6.0/4.0 VU Formale Methoden der Informatik (185.291)

21 October 2016

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

1.) Consider the following problem:

> **LOOPS-HALTS**
>
> INSTANCE: A tuple (Π_1, Π_2, I_1, I_2), where I_1, I_2 are strings and Π_1, Π_2 are programs that take a string as input.
>
> QUESTION: Is it true that Π_1 does not halt on I_1 and Π_2 halts on I_2?

By providing a reduction from an undecidable problem, prove that **LOOPS-HALTS** is undecidable. Argue formally that your reduction is correct. **(15 points)**

2.) (a) Consider the clauses $C_1, \ldots, C_5$ in `dimacs` format (in this order, shown in the box) which are given as input to a SAT solver. Apply CDCL to solve the CNF using the following conventions:

- Decision variables are selected in increasing order with respect to their integer ID in the `dimacs` format. That is, `1` is selected before `2`, `2` before `3`, and so on.
- If a variable is assigned as a decision, then it is assigned 'false'.

```
1 5 0
-2 3 0
1 2 3 0
-3 -4 -5 0
-3 4 -5 0
```

Answer the following questions and justify your answers.

- Each time when a conflict occurs and after backtracking, draw the implication graph and mark the first UIP. Learn the asserting conflict clause that corresponds to the first UIP.
- Is the given CNF satisfiable, unsatisfiable, or valid?

(5 points)

(b) Let ϕ be a propositional formula in CNF. We interpret ϕ as a set of clauses and clauses as sets of literals.

- Let $C_1 \in \phi$ and $C_2 \in \phi$ be clauses such that $\ell \in C_1$ and $\neg\ell \in C_2$ for some literal ℓ.
- Let R denote the resolvent of C_1 and C_2 (i.e. R is the result of resolving upon the variable of ℓ).
- Assume that $R \subset C_1$ and consider the CNF $\phi' := (\phi \cup \{R\}) \setminus \{C_1\}$.

Do the following statements hold? Justify your answers by either providing a formal proof or a concrete counterexample.

- ϕ is satisfiable if and only if ϕ' is satisfiable.
- $\phi \equiv \phi'$.

(10 points)

3.) Consider the following modified while-rule:

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

(a) Show that this rule is admissible regarding partial correctness. **(5 points)**

(b) Show that the Hoare calculus for partial correctness is no longer complete, if we replace the regular while-rule by the modified one. **(10 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 $X_1, \ldots, X_n$ are valid formulas/partially correct assertions.

Hoare calculus for partial correctness:

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

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

$$\{\,F[v/e]\,\}\ v \leftarrow e\ \{\,F\,\}$$

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

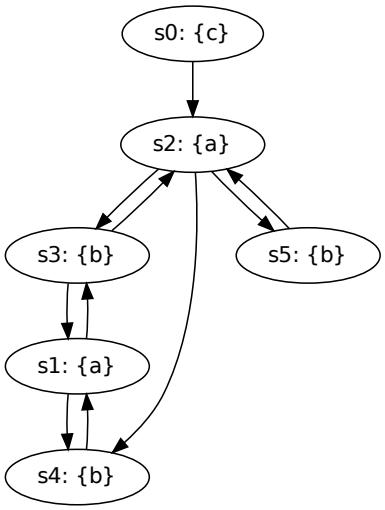
$$\frac{\{\,F \wedge e\,\}\,p\,\{\,G\,\} \quad \{\,F \wedge \neg e\,\}\,q\,\{\,G\,\}}{\{\,F\,\}\ \mathsf{if}\ e\ \mathsf{then}\ p\ \mathsf{else}\ q\ \mathsf{fi}\ \{\,G\,\}}$$

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

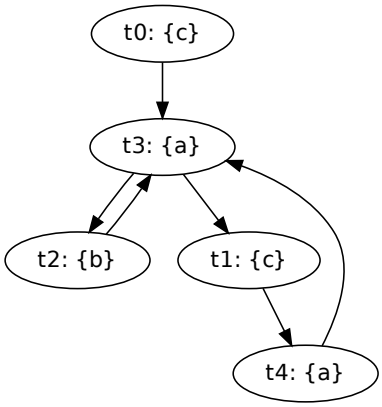
$$\frac{F \Rightarrow F' \quad \{\,F'\,\}\,p\,\{\,G'\,\} \quad G' \Rightarrow G}{\{\,F\,\}\,p\,\{\,G\,\}}$$

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:

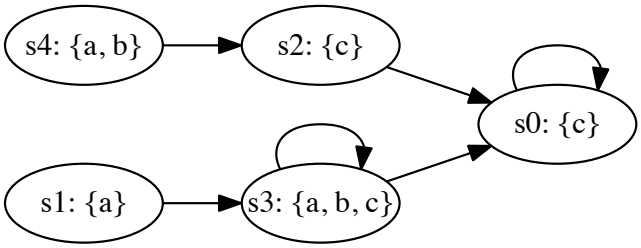


Kripke structure M_2:



(4 points)

(b) Consider the following Kripke structure M:



For each of the following formulae φ,

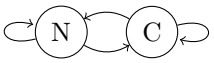
i. check the respective box if the formula is in CTL, LTL, and/or CTL*, and

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
$\mathbf{G}(c)$	☐	☐	☐	
$\mathbf{X}(b)$	☐	☐	☐	
$c\mathbf{U}b$	☐	☐	☐	
$\mathbf{AF}(a)$	☐	☐	☐	
$\mathbf{EG}(a)$	☐	☐	☐	

(5 points)

(c) **Background.** Consider the simple model of a process on the right: The process is either in state N or in state C.



Consider the system of N parallel processes P^N in which at most one process changes state at a time: We describe the system's state by counting the number of processes currently in N and C, respectively.

For example, in a system of three parallel processes P^3, if two processes are in state N, and one process is in state C, the corresponding configuration is $s := (n = 2, c = 1)$. Possible successors are $s'_1 := (n = 1, c = 2)$ and $s'_2 := (n = 3, c = 0)$.

Problem. We define the Kripke structure $M^N = \langle S_N, I_N, R_N, L_N \rangle$ over atomic propositions $AP = \{p\}$ corresponding to P^N:

- $S_N = I_N = \{(n, c) \mid n, c \in \{0, 1, \ldots, N\} \text{ and } n + c = N\}$
- $((n, c), (n', c')) \in R_n$ if and only if $n' = n + k, c' = c - k, k \in \{-1, 0, 1\}$ (at most one process moves at a time)
- $p \in L_N(s)$ if and only if $c > 0$.

We consider the systems of three and two parallel processes P^3 and P^2. We define $H \subseteq S_3 \times S_2$ as

$$H = \{((n_1, c_1), (n_2, c_2)) \mid \min(n_1, 1) = \min(n_2, 1) \wedge \min(c_1, 1) = \min(c_2, 1)\}$$

(H encodes the idea of observing if at last one process is in the respective state.)

Show that H witnesses $M^3 \leq M^2$.

(6 points)