6.0/4.0 VU Formale Methoden der Informatik

185.291 **March, 28 2014**

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

1.) Consider the following decision problem:

LATIN-SQUARE

INSTANCE: A set $S = \{s_1, \ldots, s_n\}$ of n different symbols.

QUESTION: Can we fill an $n \times n$ matrix L with the n symbols of S, such that each symbol occurs exactly once in each row and exactly once in each column?

Example: A solution to **LATIN-SQUARE** with $S = \{A, B, C\}$ is presented below:

$$L_{3,3} = \begin{pmatrix} A & B & C \\ C & A & B \\ B & C & A \end{pmatrix}$$

Provide a polynomial time reduction from **LATIN-SQUARE** to **SAT** such that the resulting formula is in conjunctive normal form (CNF). Additionally explain the intuition of your reduction, i.e., explain the intended meaning of the propositional variables and of the clauses in the CNF formula.

(15 points)

2.) (a) First define the concept of a $\mathcal{T}$-interpretation. Then use it to define the following:

i. the $\mathcal{T}$-satisfiability of a formula;

ii. the $\mathcal{T}$-validity of a formula.

Additionally define the completeness of a theory $\mathcal{T}$ and give an example for a complete and an incomplete theory.

(5 points)

(b) Prove that the following formula φ is $\mathcal{T}^E_{cons}$-valid:

$$\varphi : \qquad \neg atom(x) \wedge car(x) \doteq y \wedge cdr(x) \doteq z \rightarrow x \doteq cons(y, z)$$

Hints: Recall the axiom of construction in $\mathcal{T}^E_{cons}$:

$$\neg atom(x) \rightarrow cons(car(x), cdr(x)) \doteq x$$

(10 points)

3.) Consider the following modified while-rule:

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

(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:

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

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

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

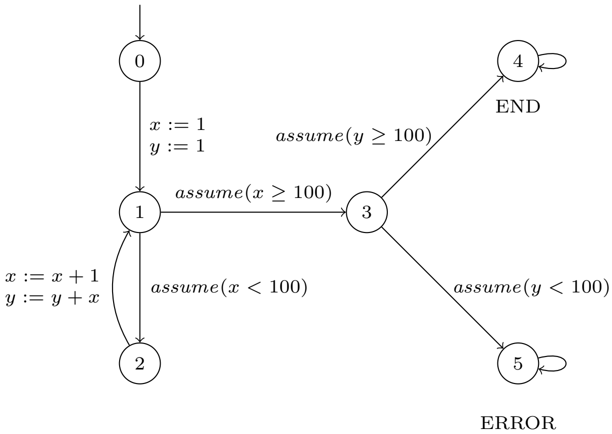
$$\frac{\{F\}\,p\,\{G\} \quad \{G\}\,q\,\{H\}}{\{F\}\,p;q\,\{H\}}$$

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

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

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

4.) Consider the following labeled transition system:



We model the labeled transition system as infinite Kripke structure $M = (S, I, R, L)$, where

- the set of atomic propositions is $AP = \{l_0, l_1, l_2, l_3, l_4, l_5\}$,
- $S = \{(c, x, y) \mid c \in [0, 5], x \in \mathbb{Z}, y \in \mathbb{Z}\}$,
- $I = \{(0, x, y) \mid x \in \mathbb{Z}, y \in \mathbb{Z}\}$,
- $R = \{((c, x, y), (c', x', y')) \mid$ there is a transition in the LTS from c to c' such that x, y go to $x', y'\}$, and
- $L(c, x, y) = l_c$

(a) i. Give an LTL formula stating that the error location is unreachable

ii. Give an LTL formula stating that if location 2 is visited, location 1 is visited in the next step

iii. Give an LTL formula stating that either location 3 is reached or location 1 is reached infinitely often

Hint: you can refer to program locations via the atomic propositions in AP.

(3 points)

(b) Provide an abstraction for the labeled transition system that uses the predicates AP (see above) for modeling the program counter and the predicates $x \geq 0$, $y \geq x$ and $x \geq 100$.

(5 points)

(c) Show that the abstraction (b) simulates the Kripke structure M.
Hint: Define a simulation relation H and show that H is indeed a simulation relation.

(5 points)

(d) Prove that M satisfies the LTL formulae from (a).
Hint: Show that the abstraction from (b) satisfies the formulae and apply a theorem from the lecture using the result from (c)

(2 points)