Prof. Dr. Andreas Podelski
Matthias Heizmann

30.11.2011
Submission: 6.12.2011
at the beginning of the lecture

Tutorials for Program Verification
Exercise sheet 6

Definition (propositional core) Let $\mathbf{qfForm}_{\mathcal{V}}$ be the set of quantifier-free formulas over the vocabulary $\mathcal{V}$. For a quantifier-free FOL formula ϕ the propositional core, denoted $propCore(\phi)$, is obtained by replacing each atomic formula of the form $P(t_1, \ldots, t_{ar(P)})$ by a propositional variable $X_{P(t_1,\ldots,t_{ar(P)})}$.
We formaly define the mapping $propCore(\phi) : \mathbf{qfForm}_{\mathcal{V}} \to \mathbf{Prop}$ recursively:

$$\begin{aligned} propCore(\bot) &= \bot \\ propCore(P(t_1, \ldots, t_{ar(P)})) &= X_{P(t_1,\ldots,t_{ar(P)})} \\ propCore(\neg\phi) &= \neg propCore(\phi) \\ propCore(\phi \odot \psi) &= propCore(\phi) \odot propCore(\psi) \end{aligned}$$

where $\odot \in \{\wedge, \vee, \to\}$.

Exercise 1: Propositional Core 2+1 points

(a) Prove that the following holds for each theory $\mathcal{T}$ and each quantifier-free formula ϕ.

If $propCore(\phi)$ is not satisfiable, then ϕ is not $\mathcal{T}$-satisfiable.

(Hint: Define a appropriate valuation ρ and prove by induction over the structure of quantifier-free formulas that for each $\mathcal{T}$-structure $\mathcal{M}$ and each assignment α the following propsition holds:$\mathcal{M}, \alpha \models \phi$ iff $\rho \models propCore(\phi)$)

(b) Does the opposite direction also hold? Prove or give a counterexample for the following proposition.

If ϕ is not $\mathcal{T}$-satisfiable then $propCore(\phi)$ is not satisfiable.

Definition (minimal unsatisfiable core) Let Γ be a finite set of formulas such that the conjunction $\bigwedge_{\phi\in\Gamma} \varphi$ is unsatisfiable. A subset $\Gamma' \subseteq \Gamma$ is called *unsatisfiable core* of Γ if $\bigwedge_{\phi\in\Gamma'} \varphi$ is also unsatisfiable. An unsatisfiable core Γ' is called *minimal unsatisfiable core* if for each proper subset Γ'' of Γ' the conjunction $\bigwedge_{\phi\in\Gamma''} \varphi$ is satisfiable.

Exercise 2: Minimal Unsatisfiable Core 1+1 points

(a) Give a minimal unsatisfiable core for the following set of formulas.

$$\{ \quad \neg(X \to \neg Z), \quad Y \to \neg U, \quad X \to Y, \quad X, \quad Z \to U \quad \}$$

(b) Is the minimal unsatisfiable core of set of formulas unique? (Are there sets of formulas $\Gamma, \Gamma_1, \Gamma_2$ such that $\Gamma_1 \neq \Gamma_2$ but both Γ_1 and Γ_2 are minimal unsatisfiable cores of Γ?)

Lets assume we have two tools. The first tool can decide satisfiability of propositional logic formulas. The second tool can decide $\mathcal{T}$-satisfiability for a conjunction of literals[1] and return a minimal unsatisfiable core if the conjunction is unsatisfiable. Then we can construct a third tool that can decide $\mathcal{T}$-satisfiability of quantifier free formulas by implementing the following algorithm.

Basic SMT Solving Algorithm

Input: quantifier-free formula ϕ_{input}

Output: Is ϕ_{input} satisfiable? Yes/No

$\phi := \phi_{\mathsf{input}}$

while(true) do {

  if $\mathit{propCore}(\phi)$ is unsatisfiable **return** No, ϕ_{input} is unsatisfiable

  Let ρ be a valuation such that $\mathcal{M}_\rho \models \mathit{propCore}(\phi)$

  Let $\{\psi_1, \dots, \psi_n\}$ be the set of atomic formulas that are subformulas of ϕ.

  Let $\{\psi_1^\rho, \dots, \psi_n^\rho\}$ be the set of formulas such that $\psi_i^\rho = \begin{cases} \psi_i & \text{if } \mathit{propCore}(\psi_i) \in \mathcal{M}_\rho \\ \neg\psi_i & \text{otherwise} \end{cases}$

  if $\psi_1^\rho \wedge \dots \wedge \psi_n^\rho$ is satisfiable **return** Yes, ϕ_{input} is satisfiable

  Let Γ be a minimal unsatisfiable core of $\{\psi_1^\rho, \dots, \psi_n^\rho\}$

  $\phi := \phi \wedge \neg(\bigwedge_{\psi \in \Gamma} \psi)$

}

Exercise 3: Basic SMT Solving Algorithm 3 points

Use the Basic SMT Solving Algorithm to determine $\mathcal{T}_E$- satisfiability[2] of the following formula.

$$x = y \quad \wedge \quad y = z \quad \wedge \quad (f(x) \neq f(z) \ \vee \ (P(x) \wedge \neg P(z)))$$

Denote all your steps.

- If a propositional logical formula is satisfiable, give a satisfying valuation. If a propositional logical formula is unsatisfiable you may write down your proof, but you don't have to.

[1] A literal is an atomic formulas or a negated atomic formula

[2] $\mathcal{T}_E$ denotes the theory of equality

- If a conjunction of atomic FOL formulas is satisfiable, give a satisfying assignment. If a conjunction of atomic FOL formulas is unsatisfiable, you may write down your proof, but a explanation is also sufficient.

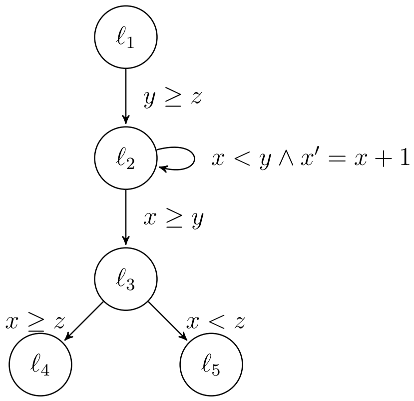
Exercise 4: Inductive Invariants 1+2 points

Consider the following program

$$Prog = (V, pc, \varphi_{init}, \mathcal{R}, \varphi_{err})$$

where the tuple of program variables V is (pc, x, y, z), the inital condition φ_{init} is $pc = \ell_1$, the error condition φ_{err} is $pc = \ell_5$, and the set of transition relations $\mathcal{R}$ contains the following transitions.

$$\begin{aligned}
\rho_1 &= (move(\ell_1, \ell_2) \wedge y \geq z \wedge skip(x, y, z)) \\
\rho_2 &= (move(\ell_2, \ell_2) \wedge x + 1 \leq y \wedge x' = x + 1 \wedge skip(y, z)) \\
\rho_3 &= (move(\ell_2, \ell_3) \wedge x \geq y \wedge skip(x, y, z)) \\
\rho_4 &= (move(\ell_3, \ell_4) \wedge x \geq z \wedge skip(x, y, z)) \\
\rho_5 &= (move(\ell_3, \ell_5) \wedge x + 1 \leq z \wedge skip(x, y, z))
\end{aligned}$$



(a) Is the complement of ρ_5 an inductive invariant[3]? If not, state a counterexample.

(b) What is the weakest[4] inductive invariant that is contained in the complement of φ_{err} (i.e., disjoint from φ_{err})?

Exercise 5: Construction of Weakest Inductive Invariant 2 bonus points

Define a (possibly non-terminating) algorithm to construct the weakest inductive invariant that is contained in the complement of φ_{err}.

(Idea: eliminate states that can reach an error state.)

[3]Note that here, the term inductive invariant refers to the inductive invariant of a program (defined in the lecture on 28th November), not to the inductive invariant of a while loop (defined in the lecture on 8th November).

[4]We say that the formula ϕ is weaker than the formula ψ if ψ implies ϕ. An inductive invariant ϕ is the weakest inductive invariant if ϕ is implied by all other inductive invariants.