Interactive Software Verification SS 2013

https://www21.in.tum.de/teaching/isv/SS13

H. Gast, L. Noschinski

SHEET 4

Semantics & Simpl

Date: 29.5.2013
Hand-In: 5.6.2013, 08:30

Goals First steps in Simpl and concepts and rules of semantics and Hoare logic.

For the non-Isabelle exercises on this sheet, please answer each question in a complete sentence.

Exercise 1 [3] Basic notions

1. What is the idea of a *shallow embedding*?
2. Name some part of Simpl which is embedded shallowly and some part which is embedded deeply.
3. The *Soundness* of the Hoare logic for Simpl is expressed by the following theorem. Explain this proposition in a sentence.

$$\Gamma,\Theta \vdash P\ c\ Q,A \Longrightarrow \Gamma,\Theta \models P\ c\ Q\ ,A$$

Exercise 2 [4] Semantics

1. Explain how the following rules model a conditional expression:

$$[\![s \in b;\ \Gamma \vdash \langle c_1, \mathsf{Normal}\ s\rangle \Rightarrow t]\!] \implies \Gamma \vdash \langle \mathsf{Cond}\ b\ c_1\ c_2, \mathsf{Normal}\ s\rangle \Rightarrow t$$
$$[\![s \notin b;\ \Gamma \vdash \langle c_2, \mathsf{Normal}\ s\rangle \Rightarrow t]\!] \implies \Gamma \vdash \langle \mathsf{Cond}\ b\ c_1\ c_2, \mathsf{Normal}\ s\rangle \Rightarrow t$$

2. The Basic command encodes state updates. Explain the rule:

$$\Gamma \vdash \langle \mathsf{Basic}\ f, \mathsf{Normal}\ s\rangle \Rightarrow \mathsf{Normal}\ (f s)$$

3. How do the rules above rely on a shallow embedding-approach?
4. The Simpl state type is:

$$\texttt{datatype}\ \mathsf{xstate} = \mathsf{Normal}\ \mathit{state} \mid \mathsf{Abrupt}\ \mathit{state} \mid \mathsf{Fault} \mid \mathsf{Stuck}$$

How can the state Abrupt ever be reached? What is the meaning of this state?

Exercise 3 [3] Hoare Logic

1. The Hoare logic provides the following rule for state updates. Why does it match the semantic given above?

$$\Gamma,\Theta \vdash \{\!|s.\ f\ s \in Q|\!\}\ (\mathit{Basic} f)\ Q,A$$

2. For the branches of a conditional statement, one wants to have the test result as additional knowledge. How is this realized in each of the following rules?

$$[\![\Gamma,\Theta \vdash (P \cap b)\ c_1\ Q,A;\ \Gamma,\Theta \vdash (P \cap -b)\ c_2 Q,A]\!] \implies \Gamma,\Theta \vdash P\ (\mathsf{Cond}\ b\ c_1\ c_2)\ Q,A$$

$$\Gamma,\Theta \vdash (P \cap b)\ c\ P,A; \implies \Gamma,\Theta \vdash P\ (\mathsf{While}\ b\ c)\ (P \cap -b),A$$

3. The classic rule for While loops is stated below. Why is the usual name *invariant* for I a sensible choice?

$$[\![P \subseteq I;\ \ \Gamma,\Theta \vdash (I \cap b)\ c\ I,A;\ \ I \cap -b \subseteq Q]\!] \implies \Gamma,\Theta \vdash P\ (\mathsf{While}\ b\ c)\ Q$$

Exercise 4 [3] Getting Started with Simpl

For this and later exercises you need the Simpl package from the *Archive of Formal Proofs*. See the `Sheet04.thy` for the Simpl exercises.