Technische Universität München
Institut für Informatik
Prof. Tobias Nipkow, Ph.D.
Dr. Peter Lammich

WS 2015/16
25. 1. 2016

Semantics of Programming Languages

Exercise Sheet 14

Exercise 14.1 Inverse Analysis

Consider a simple sign analysis based on this abstract domain:

datatype *sign* = *None* | *Neg* | *Pos0* | *Any*

fun γ :: *"sign ⇒ val set"* **where**
"γ None = {}" |
"γ Neg = {i. i < 0}" |
"γ Pos0 = {i. i ≥ 0}" |
"γ Any = UNIV"

Define inverse analyses for "+" and "<" and prove the required correctness properties:

fun *inv_plus'* :: *"sign ⇒ sign ⇒ sign ⇒ sign * sign"*
lemma
"⟦ inv_plus' a a1 a2 = (a1',a2'); i1 ∈ γ a1; i2 ∈ γ a2; i1+i2 ∈ γ a ⟧
⟹ i1 ∈ γ a1' ∧ i2 ∈ γ a2' "
fun *inv_less'* :: *"bool ⇒ sign ⇒ sign ⇒ sign * sign"*
lemma
"⟦ inv_less' bv a1 a2 = (a1',a2'); i1 ∈ γ a1; i2 ∈ γ a2; (i1<i2) = bv ⟧
⟹ i1 ∈ γ a1' ∧ i2 ∈ γ a2'"

Homework 14 Hoare-Logic

Submission until Tuesday, 2. 2 2016, 10:00am. (Pen & Paper)
The following exercises are typical exam problems. You are supposed to solve them on a sheet of paper, without using Isabelle/HOL.

We replace the assignment in IMP by a command *REL R* that performs an arbitrary state transition according to relation *R* :: (*state* × *state*) *set*.
In the big-step semantics, we remove the *assign*-rule, and add the following rule:

Rel: $(s,s') \in R \implies (REL\ R,s) \Rightarrow s'$

1. Is the semantics deterministic, i.e., does the following hold (proof or counterexample):
   $(c,s) \Rightarrow t \Longrightarrow (c,s) \Rightarrow t' \Longrightarrow t=t'$
2. What does the weakest precondition $wp\ (REL\ R)\ Q$ look like?
3. Specify a Hoare-rule for REL.
4. Prove: $\vdash \{wp\ (REL\ R)\ Q\}\ REL\ R\ \{Q\}$.

Hints

- Question 2: Recall the definition of the weakest precondition:
  $wp\ c\ Q\ =\ (\lambda s.\ \forall t.\ (c,s) \Rightarrow t \longrightarrow Q\ t)$
  Now we want an equation that shows how to expand wp syntactically, i.e., the right hand side should not contain the Big/Small-step semantics. You need **not** prove your equation here.
- Question 4: The main lemma in the completeness proof of Hoare logic is $\vdash \{wp\ c\ Q\}\ c\ \{Q\}$. Here you have to prove the case for the REL-command. Use your equation for wp from Question 2 here!

Homework 14 Collecting Semantics

Submission until Tuesday, 2. 2 2016, 10:00am. (Pen & Paper)

This question concerns the iterative computation of the collecting semantics of the following annotated command where `i` is some positive integer:

```
x := i {A0};
{A1}
WHILE 0 < x
DO {A2} x := x+1 {A3}
{A4}
```

1. Show how the annotations change with each application of the step function. Fill in this table to show the first 7 steps of the process:

	0	1	2	3	4	5	6	7
$A0$	$\{\}$	$\{i\}$						
$A1$	$\{\}$							
$A2$	$\{\}$							
$A3$	$\{\}$							
$A4$	$\{\}$							

For compactness abbreviate a state <x := k> by the value k of x when you fill in the table. Entries that do not change can be left blank.

2. What are the annotations $A0$, ..., $A4$ of the collecting semantics of the above annotated command, i.e. of the least fixpoint of function *step*?

Homework 14 Complete Lattices

Submission until Tuesday, 2. 2 2016, 10:00am. (Pen & Paper)

Let $'a$ be a complete lattice with ordering $\leq$ and let $f :: {'a} \Rightarrow {'a}$ be a monotone function.

Give a detailed prove for the following statement:

$$\bigsqcup (f \text{ ` } X) \leq f \ (\bigsqcup X)$$

Hints:

- The least upper bound satisfies the following properties
  - Upper bound: $x \in A \Longrightarrow x \leq \bigsqcup A$
  - Least upper bound: $(\forall x \in A.\ x \leq u) \Longrightarrow \bigsqcup A \leq u$
- $f \text{ ` } X$ is the function image: $f \text{ ` } X = \{y.\ \exists x{\in}X.\ f\ x = y\}$