Technische Universität München
Institut für Informatik
Prof. Tobias Nipkow, Ph.D.
Fabian Huch, Kevin Kappelmann

WS 23/24
Feb 6

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* $\Rightarrow$ *val set*" **where**
"γ *None* = {}" |
"γ *Neg* = {*i*. *i* < *0*}" |
"γ *Pos0* = {*i*. *i* $\geq$ *0*}" |
"γ *Any* = *UNIV*"

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

fun *inv_plus'* :: "*sign* $\Rightarrow$ *sign* $\Rightarrow$ *sign* $\Rightarrow$ *sign* $*$ *sign*"
lemma
"⟦ *inv_plus' a a1 a2* = (*a1'*,*a2'*); *i1* $\in$ γ *a1*; *i2* $\in$ γ *a2*; *i1*+*i2* $\in$ γ *a* ⟧
$\Longrightarrow$ *i1* $\in$ γ *a1'* $\wedge$ *i2* $\in$ γ *a2'* "
fun *inv_less'* :: "*bool* $\Rightarrow$ *sign* $\Rightarrow$ *sign* $\Rightarrow$ *sign* $*$ *sign*"
lemma
"⟦ *inv_less' bv a1 a2* = (*a1'*,*a2'*); *i1* $\in$ γ *a1*; *i2* $\in$ γ *a2*; (*i1*<*i2*) = *bv* ⟧
$\Longrightarrow$ *i1* $\in$ γ *a1'* $\wedge$ *i2* $\in$ γ *a2'*"