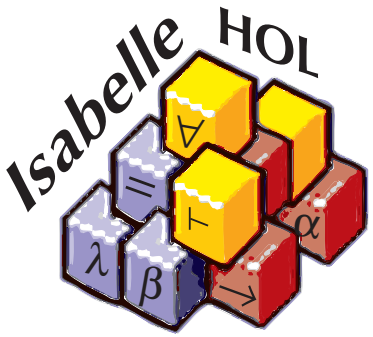
Axiomatic Semantics for Java^{light} in Isabelle/HOL

David von Oheimb[1], TU München

http://www.in.tum.de/~oheimb/



[1]Research funded by the Project BALI

State of the Art

Motivation

Object-oriented languages like Java widely used
Demand for verification (e.g. Smart Cards)
Classical approach: Hoare Logic
New challenges (e.g. dynamic binding)

Aims

- Soundness
- Usability
- Language Coverage
- Completeness

Related Work

- Arnd Poetzsch-Heffter et al.
- Bart Jacobs et al.
- Martin Wirsing et al.
- . . .

Assertions

Shallow embedding into HOL: Predicates on the state
$\leadsto$ trivial expressiveness, relative completeness (in the sense of Cook)

Auxiliary variables for relating pre- and post-states, like in $\{X{=}Z\}\ cmd\ \{X{=}Z\}$
avoiding rules of adaptation

Result stack of anonymous intermediate results (instead of meta variables)
used for handling side-effecting expressions first-class

Assertion type $\alpha\ assn = res\ list \times state \to \alpha \to bool$

Peeking at the state: e.g. Normal $P \equiv \lambda(Y,\sigma)\ Z.\ P\ (Y,\sigma)\ Z \wedge$ fst $\sigma =$ None

Pushing a result onto the stack: $P{\uparrow}:v \equiv \lambda(Y,\sigma)\ Z.\ P\ (v:Y,\sigma)\ Z$

Dynamic Binding

Dependency problem: code depends on dynamically computed value D

- D passed as a special result value
- universally quantified value bound in the precondition to D

Range problem: D should be limited to be a subtype of the type rt

- restriction on D supplied to the user as the precondition $\Gamma \vdash mode \rightarrow D \preceq rt$
- meta-level proof of correctness within soundness proof
- $\rightsquigarrow$ type-safety plays a crucial role

$$\frac{\begin{array}{c}\Gamma \vdash \{\text{Normal } P\}\ e\ \{Q\} \\ \Gamma \vdash \{Q\}\ args\ \{\ldots \text{ let } D = \ldots \text{ in } R\uparrow : \text{DynT } D \ldots\} \\ \forall D.\ \Gamma \vdash \{R\uparrow : \text{DynT } D \wedge \ldots\ \Gamma \vdash mode \rightarrow D \preceq rt\}\ \text{Body } D\ (mn, pTs)\ \{\ldots\}\end{array}}{\Gamma \vdash \{\text{Normal } P\}\ \{rt, \tau, mode\} e.mn(\{pTs\} args)\ \{S\}}$$

Soundness & Completeness

Goal wf_prog $\Gamma \longrightarrow \Gamma{\vdash}\{P\}\ t{\succ}\ \{Q\} = \Gamma{\models}\{P\}\ t{\succ}\ \{Q\}$

Soundness proof by rule induction on the derivation of triples

- using well-typedness and conformance (as preconditions) plus type-safety
- for method calls and loops: auxiliary inductions on the recursive depth

Completenss proof by structural induction with the MGF approach

$\{\lambda(Y,\sigma)\ Z.\ (Y,\sigma){=}Z\}\ t{\succ}\ \{\lambda(Y',\sigma')\ (Y,\sigma).\ \ldots\ \wedge\ \Gamma{\vdash}\sigma\ {-}t{\rightarrow}\ (v,\sigma')\}$

- with auxiliary induction on the number of classes already initialized
- with outer induction on the number of methods already verified, exploiting well-typedness to ensure finiteness of the number of methods

Conclusion

Achievements

- First sound & (relatively) complete Hoare logic for a Java-style language
- Insights into the role of type-safety
- One of the major applications of Isabelle/HOL

Inherent complexity leads to . . .

- extensions of the classical Hoare calculus
- challenging proof of completeness
- tedious program verification

Theorem prover . . .

- enforces fully formal treatment.
- assists with all the details

Axiomatic Semantics, applied to OO . . .

- retains its typical flavor
- is at least feasible