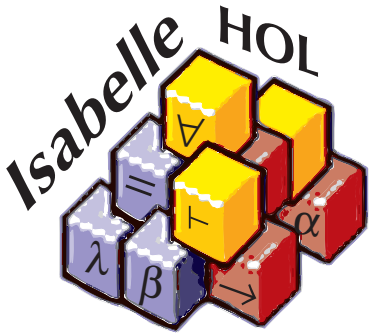
Hoare Logic for Mutual Recursion and Local Variables

David von Oheimb, TU München

DFG Project Bali

http://isabelle.in.tum.de/Bali/



Outline

Syntax and Semantics of IMP$_P$

Hoare Logic for IMP$_P$

- Auxiliary Variables
- Local Variables
- Rule of Consequence
- Mutual Recursion (2 Versions)

Soundness Proof

- Validity

Completeness Proof

- MGF approach
- Proof outline (3 Versions)

Conclusion

... Demo session with

Abstract Syntax of IMP_P

Statements (deep embedding)

$$\begin{aligned} com \;=\; & \texttt{SKIP} \mid com\texttt{;}\ com \mid vname\ \texttt{:=}\ aexp \\ & \mid \texttt{IF}\ bexp\ \texttt{THEN}\ com\ \texttt{ELSE}\ com \mid \texttt{WHILE}\ bexp\ \texttt{DO}\ com \\ & \mid \texttt{LOCAL}\ loc\ \texttt{:=}\ aexp\ \texttt{IN}\ com \\ & \mid vname\ \texttt{:=}\ \texttt{CALL}\ pname(aexp) \mid \texttt{BODY}\ pname \end{aligned}$$

Expressions $aexp = state \to val$ (shallow embedding)

Variables $vname =$ Glb $glb \mid$ Loc loc (strict separation!)

Procedure declarations body :: $pname \to com$

Finitely many procedures: via finite type $pname$

Operational Semantics for IMP_P

Judgment Form $\langle c, \sigma\rangle \longrightarrow \sigma'$

Rules

$$Local\ \frac{\langle c, \sigma_0[a\ \sigma_0/X]\rangle \longrightarrow \sigma_1}{\langle \texttt{LOCAL}\ X\ \texttt{:=}\ a\ \texttt{IN}\ c, \sigma_0\rangle \longrightarrow \sigma_1[\sigma_0\langle X\rangle/X]}$$

$$Call\ \frac{\langle \texttt{BODY}\ p, (\mathsf{setlocs}\ \sigma_0\ \mathsf{newlocs})[a\ \sigma_0/\texttt{Arg}]\rangle \longrightarrow \sigma_1}{\langle X\texttt{:=CALL}\ p(a), \sigma_0\rangle \longrightarrow (\mathsf{setlocs}\ \sigma_1\ (\mathsf{getlocs}\ \sigma_0))[X\texttt{:=}\sigma_1\langle \texttt{Res}\rangle]}$$

$$Body\ \frac{\langle \mathsf{body}\ p, \sigma_0\rangle \longrightarrow \sigma_1}{\langle \texttt{BODY}\ p, \sigma_0\rangle \longrightarrow \sigma_1}$$

Extensions to Hoare Triples

Assertions (first approach) $assn = state \to bool$ (shallow embedding)

Auxiliary Variables $\vdash \{X{=}Z\}\ c\ \{X{=}Z\}$

intended meaning: $\vdash \forall Z.\ \{\lambda\sigma.\ \sigma\langle X\rangle{=}Z\}\ c\ \{\lambda\sigma.\ \sigma\langle X\rangle{=}Z\}$

Problem: assumptions $\{\{X{=}Z\}\ \texttt{BODY}\ F\ \{X{=}Z\}\} \vdash \{P\}\ c\ \{Q\}$

Assertions (revised version) $\alpha\ assn = \alpha \to state \to bool$

Hoare Triples $\alpha\ triple = \{\alpha\ assn\}\ com\ \{\alpha\ assn\}$

Validity (wrt. Partial Correctness, preliminary definition)

$\models\{P\}\ c\ \{Q\} \equiv \forall Z\ \sigma\ \sigma'.\ P\ Z\ \sigma \Longrightarrow \langle c,\sigma\rangle \longrightarrow \sigma' \Longrightarrow Q\ Z\ \sigma'$

Non-Procedure Rules

Judgments (preliminary) $\vdash _ :: \alpha\ triple \to bool$

Rules

$$Ass\ \frac{}{\vdash \{\lambda Z\,\sigma.\ P\ Z\,(\sigma[a\,\sigma/X])\}\ X{:=}a\ \{P\}}$$

$$Local\ \frac{\vdash \{P\}\ c\ \{\lambda Z\,\sigma.\ Q\ Z\,(\sigma[\sigma_0\ \langle X\rangle/X])\}}{\vdash \{\lambda Z\,\sigma.\ \sigma_0{=}\sigma \wedge P\ Z\,(\sigma[a\,\sigma/X])\}\ \texttt{LOCAL}\ X{:=}a\ \texttt{IN}\ c\ \{Q\}}$$

$$Local\ \frac{\vdash \{P\}\ c\ \{Q[old\ X/X]\}}{\vdash \{P[a/X]\}\ \texttt{LOCAL}\ X{:=}a\ \texttt{IN}\ c\ \{Q\}}$$

Rule of Consequence

$$\frac{\forall Z\,\sigma.\ P\ Z\,\sigma \Longrightarrow P'\ Z\,\sigma \quad \vdash \{P'\}\ c\ \{Q'\} \quad \forall Z\,\sigma'.\ Q'\ Z\,\sigma' \Longrightarrow Q\ Z\,\sigma'}{\vdash \{P\}\ c\ \{Q\}}$$

$$\frac{\vdash \{P'\}c\{Q'\} \quad \forall Z\,\sigma.\ P\ Z\,\sigma \Longrightarrow \forall \sigma'.\ \exists Z'.P'\ Z'\ \sigma \wedge (Q'\ Z'\ \sigma' \Longrightarrow Q\ Z\,\sigma')}{\vdash \{P\}\ c\ \{Q\}}$$

$$conseq\ \frac{\begin{array}{l}\forall Z\,\sigma.\ P\ Z\,\sigma \Longrightarrow \exists P'\ Q'.\ \vdash \{P'\}\ c\ \{Q'\} \wedge \\ \qquad \forall \sigma'.\ \exists Z'.\ (P'\ Z'\ \sigma \Longrightarrow Q'\ Z'\ \sigma') \Longrightarrow Q\ Z\,\sigma'\end{array}}{\vdash \{P\}\ c\ \{Q\}}$$

Application, e.g.

$$disj\ \frac{\vdash \{P\}\ c\ \{Q\} \quad \vdash \{P'\}\ c\ \{Q'\}}{\vdash \{P \vee P'\}\ c\ \{Q \vee Q'\}}$$

Nested Body Rule

Judgments (revised) $_ \vdash _ :: \alpha\ triple\ set \to \alpha\ triple \to bool$

$$BodyN\ \frac{\{\{P\}\ \texttt{BODY}\ p\ \{Q\}\} \cup \Gamma\ \vdash\ \{P\}\ \mathsf{body}\ p\ \{Q\}}{\Gamma \vdash \{P\}\ \texttt{BODY}\ p\ \{Q\}} \qquad asm\ \frac{t \in \Gamma}{\Gamma \vdash t}$$

Example P calls Q and R, Q calls R, and R calls P and Q:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\{P,Q,R\} \vdash \texttt{BODY}\ P}\,asm \quad \dfrac{}{\{P,Q,R\} \vdash \texttt{BODY}\ Q}\,asm}{\vdots\ \{P,Q,R\} \vdash \text{(body of } R\text{)}\ \vdots}{\{P,Q\} \vdash \texttt{BODY}\ R}\,BodyN}{\vdots\ \{P,Q\} \vdash \text{(body of } Q\text{)}\ \vdots}{\{P\} \vdash \texttt{BODY}\ Q}\,BodyN \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\{P,Q,R\} \vdash \texttt{BODY}\ R}\,asm \quad \dfrac{}{\{P,R\} \vdash \texttt{BODY}\ P}\,asm}{\vdots\ \{P,Q,R\} \vdash \text{(body of } Q\text{)}\ \vdots}{\{P,R\} \vdash \texttt{BODY}\ Q}\,BodyN}{\vdots\ \{P,R\} \vdash \text{(body of } R\text{)}\ \vdots}{\{P\} \vdash \texttt{BODY}\ R}\,BodyN}{\vdots\ \{P\} \vdash \text{(body of } P\text{)}\ \vdots}{\emptyset \vdash \texttt{BODY}\ P}\,BodyN$$

Simultaneous Body Rule

Judgments (final) $_ \Vdash _ :: \alpha\ triple\ set \to \alpha\ triple\ set \to bool$

$$Body\ \frac{\Gamma \cup \{\{P_i\}\texttt{BODY}\ i\{Q_i\} \mid i \in ps\} \Vdash \{\{P_i\}\texttt{body}\ i\{Q_i\} \mid i \in ps\}}{\Gamma \Vdash \{\{P_i\}\ \texttt{BODY}\ i\{Q_i\}\} \mid i \in ps\}}$$

$$empty\ \frac{}{\Gamma \Vdash \emptyset} \qquad insert\ \frac{\Gamma \vdash t \quad \Gamma \Vdash ts}{\Gamma \Vdash \{t\} \cup ts} \qquad weaken\ \frac{\Gamma \Vdash ts' \quad ts \subseteq ts'}{\Gamma \Vdash ts}$$

Example

$$\dfrac{\dfrac{\dfrac{}{\{P,Q,R\} \vdash \texttt{BODY}\ P}\ asm \quad \dfrac{}{\{P,Q,R\} \vdash \texttt{BODY}\ Q}\ asm \quad \dfrac{}{\{P,Q,R\} \vdash \texttt{BODY}\ R}\ asm}{\dfrac{\vdots\ \{P,Q,R\} \Vdash (\text{bodies of } P,\ Q \text{ and } R)\ \vdots}{\dfrac{\emptyset \Vdash \{\texttt{BODY}\ P, \texttt{BODY}\ Q, \texttt{BODY}\ R\}}{\emptyset \vdash \texttt{BODY}\ P}\ weaken}\ Body}\ 2 \times insert, empty$$

Soundness Proof: Validity Revisited

Soundness goal $\emptyset \vdash t \Longrightarrow \emptyset \models t$

Actual proof $\Gamma \Vdash ts \Longrightarrow \Gamma \models\!\models ts$ by rule induction

Recursive Depth of evaluation $\langle c,\sigma_0\rangle -n\rightarrow \sigma_1$

Annotation for depth of procedure calls sufficient for execution of command

$$Body' \ \frac{\langle \text{body } p,\ \sigma_0\rangle - n \rightarrow \sigma_1}{\langle \texttt{BODY } p,\ \sigma_0\rangle - n{+}1 \rightarrow \sigma_1}$$

Validity $\models n{:}\{P\}\ c\ \{Q\} \equiv \forall Z\ \sigma\ \sigma'.\ P\ Z\ \sigma \Longrightarrow \langle c,\sigma\rangle - n \rightarrow \sigma' \Longrightarrow Q\ Z\ \sigma'$

Canonical extension to triple sets $\models\!\models n{:}ts \equiv \forall t \in ts.\ \models n{:}t$

Non-trivial extension to assumptions $\Gamma \models\!\models ts \equiv \forall n.\ \models\!\models n{:}\Gamma \Longrightarrow \models\!\models n{:}ts$

Connection to preliminary definition : $\emptyset \models\!\models ts \Longleftrightarrow \forall t \in ts.\ \models t$

(Relative) Completeness Proof: MGF Approach

Most General Triple $\mathtt{MGT}\ c \equiv \{\lambda Z\, \sigma_0.\ Z = \sigma_0\}\ c\ \{\lambda Z\, \sigma_1.\ \langle c, Z\rangle \longrightarrow \sigma_1\}$

MGF Corollary $\emptyset \vdash \mathtt{MGT}\ c \Longrightarrow \emptyset \models \{P\}\ c\ \{Q\} \Longrightarrow \emptyset \vdash \{P\}\ c\ \{Q\}$

Main Proof Obligation $\emptyset \vdash \mathtt{MGT}\ c$ (by structural/rule induction)

Version 1: Nested Structural Induction

MGT-lemma: $(\forall p.\ \Gamma \vdash \mathtt{MGT}\ (\mathtt{BODY}\ p)) \Longrightarrow \Gamma \vdash \mathtt{MGT}\ c$ (by Struct. Ind.)

Auxiliary induction on the number of procedures (strengthened goal), using 2×MGT-lemma, $BodyN$, asm, and finiteness

Version 2: Simultaneous Structural Induction

using 1×MGT-lemma, $Body$, $empty$, $insert$, asm, and finiteness

(Relative) Completeness Proof (cont'd)

Version 3: Rule Induction for proving

$$\forall \sigma_0\ \sigma_1.\ \langle c,\sigma_0\rangle \longrightarrow \sigma_1 \Longrightarrow \emptyset \vdash \{\lambda Z\ \sigma.\ \sigma = \sigma_0\}\ c\ \{\lambda Z\ \sigma.\ \sigma = \sigma_1\}$$

using a trivial version of $Body$ and an unfolding variant of the $Loop$ rule:

$$LoopT\ \frac{\Gamma \vdash \{P \wedge b\}\ c\ \{Q\} \quad \Gamma \vdash \{Q\}\ \texttt{WHILE}\ b\ \texttt{DO}\ c\ \{R\}}{\Gamma \vdash \{P \wedge b\}\ \texttt{WHILE}\ b\ \texttt{DO}\ c\ \{R\}}$$

MGF corollary requires $diverg\ \dfrac{}{\Gamma \vdash \{\lambda Z\ \sigma.\ \neg\exists \sigma'.\ \langle c,\ \sigma\rangle \longrightarrow \sigma'\}\ c\ \{Q\}}$

\+ simpler proof

\+ does not require assumptions nor auxiliary variables nor finiteness

– requires(?) two additional rules and strong conseq rule

– rather operational style (acceptable for meta theory only)

Conclusion

New approaches for old problems

- simple handling of local variables
- strong rule of consequence
- convenient rule for mutual recursion

Experience with meta-theoretical proofs

- Soundness is rather straightforward
- Completeness is feasible

Mechanical prover gives ...

- Relief from details
- Confidence in the results

Transfer to other languages

- Application to Java$_{light}$