Formal Methods for Java

Lecture 19: Proofs in Jahob

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Jan 8, 2013

Static Checking vs. Theorem Proving

Goal:

- finds bugs at compile-time,
- proves that there is no violation.

Static Checking:

- e. g. Jahob and ESC/Java
- fully automatic (after annotation)
- can only verify simple properties

Theorem Proving:

- Needs lot of manual interaction
- complete calculus, can verify any property.

The Jahob Proof Language

Goals

- Improve the strength of the provable properties.
- Still fully automatic (after annotation).
- Have intermediate proof steps in annotation.

Paper:

- Karen Zee, Viktor Kuncak, and Martin Rinard. An integrated proof language for imperative programs. In ACM Conf. Programming Language Design and Implementation (PLDI), 2009.

Note command

We already know one command

$$\text{note } \ell : F$$

which abbreviates

$$\text{assert } \ell : F; \text{assume } \ell : F$$

- ℓ is a label (or name) for the formula F
- When F cannot be proven Jahob tells that the check for ℓ failed.
- ℓ can also be used to tell the Jahob which formulas are relevant:

$$\text{assert } G \text{ from } \ell$$

Why is this rule correct?

Correctness of Proof Commands

An incorrect program must not be verified succesfully.

If $P \rightarrow wp(S_1; \text{note } F; S_2, Q)$
then $P \rightarrow wp(S_1; S_2, Q)$

This is the case if we can proof that for all H

$$wp(\text{note } F, H) \rightarrow H$$

The note F command is correct:

$$\begin{aligned} wp(\text{note } F, H) &\leftrightarrow wp(\text{assert } F; \text{assume } F, H) \\ &\leftrightarrow F \wedge (F \rightarrow H) \\ &\leftrightarrow F \wedge H \\ &\rightarrow H \end{aligned}$$

Proving implications

Suppose you want to argue that F implies G by a implication chain

$$F \to F_1 \to F_2 \to G.$$

In Jahob there is a special syntax:

$$\begin{array}{ll} \text{assuming } F \text{ in} & \\ (& \text{note } F_1 \\ & \text{note } F_2 \\ & \text{note } G) \end{array}$$

This command adds the assumption

$$\text{assume } F \to G$$

General syntax of assuming

The general syntax is

$$\begin{array}{l} \text{assuming } F \text{ in} \\ (\quad \vdots \\ \quad\;\; \text{note } G) \end{array}$$

This is an abbreviation for

$$\begin{array}{ll} (& \text{assume } F \\ & \vdots \\ & \text{assert } G \\ & \text{assume false} \\ \square & \\ & \text{assume } F \rightarrow G \\ ) & \end{array}$$

- $\vdots$ stands for arbitrary proof statements

Correctness of assuming statement

The implication rule is correct, provided the proof statements used in between are correct.

$$
\begin{aligned}
& wp((\text{assume } F; p; \text{assert } G; \text{assume false} \,\square\, \text{assume } F \rightarrow G, H) \\
& \quad \equiv (F \rightarrow wp(p, G)) \wedge ((F \rightarrow G) \rightarrow H) \\
& \quad \rightarrow [\text{assuming that proof statements } p \text{ are correct}] \\
& \qquad (F \rightarrow G) \wedge ((F \rightarrow G) \rightarrow H) \\
& \quad \rightarrow H
\end{aligned}
$$

Case Splits

One can split cases, e. g.

$$\text{cases } x \geq 0, x < 0 \text{ for } abs(x) \geq 0$$

$$\text{cases } F_1, \ldots, F_n \text{ for } G$$

is an abbreviation for

$$\begin{aligned}&\text{assert } F_1 \vee \cdots \vee F_n;\\&\text{assert } F_1 \rightarrow G; \ldots\\&\text{assert } F_n \rightarrow G;\\&\text{assume } G\end{aligned}$$

- Proof that $F_1, \ldots, F_n$ are all possible cases.
- Proof for each case G separately.
- Assume G holds.

Proving Universal Quantifiers

To prove a universal quantified formula the syntax is

$$\begin{array}{l} \text{pickAny } x \\ \vdots \\ \text{note } F \end{array}$$

This is an abbreviation for

$$\begin{array}{ll} (& \text{havoc } x \\ & \vdots \\ & \text{assert } F[x] \\ & \text{assume false} \\ \Box & \\ & \text{assume } \forall x.F[x] \\ ) & \end{array}$$

Removing Universal Quantifiers

The inverse operation removes universal quantifiers:

$$\text{instantiate } \forall x.F[x] \text{ with } t$$

This is an abbreviation for

$$\begin{array}{l}\text{assert } \forall x.F[x] \\ \text{assume } F[t]\end{array}$$

Proving Existential Quantifiers

To prove an existential quantified formula the syntax is

$$\text{witness } t \text{ for } \exists x.F[x]$$

This is an abbreviation for

$$\begin{array}{l}\text{assert } F[t] \\ \text{assume } \exists x.F[x]\end{array}$$

Removing Existential Quantifiers

The syntax is

$$\begin{array}{ll} \text{pickWitness } x \text{ for } F[x] & \\ \vdots & \qquad\qquad \text{where } x \text{ does not occur in } G \\ \text{note } G & \end{array}$$

This is an abbreviation for

$$\begin{array}{ll} (& \text{assert } \exists x. F[x] \\ & \text{havoc } x \\ & \text{assume } F[x] \\ & \vdots \\ & \text{assert } G \\ & \text{assume false} \\ \Box & \\ & \text{assume } G \\ ) & \end{array}$$