Generation of Verification Conditions (cont'd)

Andreas Podelski

November 21, 2011

mechanization of correctness proof

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,

mechanization of correctness proof

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- construct a *backwards* derivation

mechanization of correctness proof

- given a Hoare triple $\{\phi\}$ C $\{\psi\}$,
- construct a *backwards* derivation
- derivation $=$ sequence of Hoare triples,
  each Hoare triple is an axiom (skip, update)
  or it is inferred by one of the inference rules (seq, cond, while)

mechanization of correctness proof

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- construct a *backwards* derivation
- derivation $=$ sequence of Hoare triples,
  each Hoare triple is an axiom (skip, update)
  or it is inferred by one of the inference rules (seq, cond, while)
- Hoare triple uses given postcondition and *weakest precondition*
- derivation *unique*

mechanization of correctness proof

- given a Hoare triple $\{\phi\}$ C $\{\psi\}$,
- construct a *backwards* derivation
- derivation $=$ sequence of Hoare triples,
  each Hoare triple is an axiom (skip, update)
  or it is inferred by one of the inference rules (seq, cond, while)
- Hoare triple uses given postcondition and *weakest precondition*
- derivation *unique*
- verification condition $=$ set of side conditions

weakest precondition wp(C, ψ)

- wp(**skip**, ψ) $= \psi$

weakest precondition wp(C, ψ)

- wp(**skip**, ψ) $= \psi$
- wp($x := e, \psi$) $= \psi[e/x]$

weakest precondition $\mathrm{wp}(C, \psi)$

- $\mathrm{wp}(\textbf{skip}, \psi) = \psi$
- $\mathrm{wp}(x := e, \psi) = \psi[e/x]$
- $\mathrm{wp}(C_1 \; ; \; C_2, \psi) = \mathrm{wp}(C_1, \mathrm{wp}(C_2, \psi))$

weakest precondition $\mathsf{wp}(C, \psi)$

- $\mathsf{wp}(\textbf{skip}, \psi) = \psi$
- $\mathsf{wp}(x := e, \psi) = \psi[e/x]$
- $\mathsf{wp}(C_1 \ ; \ C_2, \psi) = \mathsf{wp}(C_1, \mathsf{wp}(C_2, \psi))$
- $\mathsf{wp}(\textbf{if } b \textbf{ then } C_1 \textbf{ else } C_2, \psi) = (\neg b \vee \phi_1) \wedge (b \vee \phi_2)$
  where
  $$\phi_1 = \mathsf{wp}(C_1, \psi)$$
  $$\phi_2 = \mathsf{wp}(C_2, \psi)$$

weakest precondition wp(C, ψ)

- wp(**skip**, ψ) $= \psi$
- wp$(x := e, \psi) = \psi[e/x]$
- wp$(C_1 \; ; \; C_2, \psi) = $ wp$(C_1, $ wp$(C_2, \psi))$
- wp(**if** b **then** C_1 **else** C_2, ψ) $= (\neg b \vee \phi_1) \wedge (b \vee \phi_2)$
  where
  $$\phi_1 = \mathrm{wp}(C_1, \psi)$$
  $$\phi_2 = \mathrm{wp}(C_2, \psi)$$
- wp(**while** b **do** $\{\theta\}$ C_0, ψ) $= \theta$

verification condition for $\{\phi\}$ C $\{\psi\}$

- for command C of form: skip, update, seq, cond,

verification condition for $\{\phi\}\ C\ \{\psi\}$

- for command C of form: skip, update, seq, cond,
- add one implication:

$$\phi \to \mathsf{wp}(C, \psi)$$

verification condition for $\{\phi\}\ C\ \{\psi\}$

- for command C of form: skip, update, seq, cond,
- add one implication:

$$\phi \rightarrow \mathrm{wp}(C, \psi)$$

- for command C of form: **while** b **do** $\{\theta\}\ C_0$,

verification condition for $\{\phi\}$ C $\{\psi\}$

- for command C of form: skip, update, seq, cond,
- add one implication:

$$\phi \rightarrow \mathrm{wp}(C, \psi)$$

- for command C of form: **while** b **do** $\{\theta\}$ C_0 ,
- add two implications:

$$\begin{array}{l} \phi \rightarrow \theta \\ \theta \wedge \neg b \rightarrow \psi \end{array}$$

and add verification condition for Hoare triple $\{\theta \wedge b\}$ C_0 $\{\theta\}$

Adequacy of Verification Condition

- let Φ be the verification condition for $\{\phi\}$ C $\{\psi\}$

Adequacy of Verification Condition

- let Φ be the verification condition for $\{\phi\}\ C\ \{\psi\}$
- let Γ be a set of assertions
  (e.g., axioms for bounded integer arithmetic,
  axioms for factorial function, . . .)

Adequacy of Verification Condition

- let Φ be the verification condition for $\{\phi\}\ C\ \{\psi\}$
- let Γ be a set of assertions
  (e.g., axioms for bounded integer arithmetic,
  axioms for factorial function, ...)
- $$\Gamma \models \Phi \quad \text{iff} \quad \Gamma \vdash \{\phi\}\ C\ \{\psi\}$$