Generation of Verification Conditions

Andreas Podelski

November 15, 2011

mechanization of correctness proof

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

mechanization of correctness proof

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  a derivation is a 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:
- construct a derivation *assuming* that side conditions hold,
- and then check side conditions
  "discharge the verification condition"

mechanization of correctness proof

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  a derivation is a 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:
- construct a derivation *assuming* that side conditions hold,
- and then check side conditions
  "discharge the verification condition"
- if check does not succeed: try another derivation

mechanization of correctness proof

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  a derivation is a 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:
- construct a derivation *assuming* that side conditions hold,
- and then check side conditions
  "discharge the verification condition"
- if check does not succeed: try another derivation
- next:
  deterministic strategy to construct *unique* derivation

System $\mathcal{H}$ (1)

- Hoare triple $\{\phi\}\ C\ \{\psi\}$ derivable in $\mathcal{H}$ if
  exists a derivation using the axioms and inference rules of $\mathcal{H}$

System $\mathcal{H}$ (1)

- Hoare triple $\{\phi\}\ C\ \{\psi\}$ derivable in $\mathcal{H}$ if exists a derivation using the axioms and inference rules of $\mathcal{H}$
- skip

$$\frac{}{\{\phi\}\ \textbf{skip}\ \{\phi\}}$$

System $\mathcal{H}$ (1)

- Hoare triple $\{\phi\}\ C\ \{\psi\}$ derivable in $\mathcal{H}$ if exists a derivation using the axioms and inference rules of $\mathcal{H}$
- skip

$$\frac{}{\{\phi\}\ \textbf{skip}\ \{\phi\}}$$

- assignment

$$\frac{}{\{\psi[e/x]\}\ x := e\ \{\psi\}}$$

System $\mathcal{H}$ (2)

- sequential command $C \equiv C_1 \; ; \; C_2$

$$\frac{\{\phi\}\; C_1\; \{\phi'\} \qquad \{\phi'\}\; C\; \{\psi\}}{\{\phi\}\; C\; \{\psi\}}$$

System $\mathcal{H}$ (2)

- sequential command $C \;\equiv\; C_1 \,;\, C_2$

$$\frac{\{\phi\}\ C_1\ \{\phi'\} \qquad \{\phi'\}\ C\ \{\psi\}}{\{\phi\}\ C\ \{\psi\}}$$

- conditional command $C \;\equiv\; \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2$

$$\frac{\{\phi \wedge b\}\ C_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ C\ \{\psi\}}{\{\phi\}\ C\ \{\psi\}}$$

System $\mathcal{H}$ (3)

- while command $C \equiv \textbf{while } b \textbf{ do } \{\theta\}\ C_0$

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ C\ \{\theta \wedge \neg b\}}$$

System $\mathcal{H}$ (3)

- while command $C \equiv \textbf{while } b \textbf{ do } \{\theta\}\ C_0$

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ C\ \{\theta \wedge \neg b\}}$$

- strengthen precondition, weaken postcondition

$$\frac{\{\phi\}\ C\ \{\psi\}}{\{\phi'\}\ C\ \{\psi'\}} \quad \text{if} \quad \phi' \to \phi \quad \text{and} \quad \psi \to \psi'$$

System $\mathcal{H}$ (3)

- while command $C \equiv \textbf{while } b \textbf{ do } \{\theta\}\ C_0$

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ C\ \{\theta \wedge \neg b\}}$$

- strengthen precondition, weaken postcondition

$$\frac{\{\phi\}\ C\ \{\psi\}}{\{\phi'\}\ C\ \{\psi'\}} \quad \text{if} \quad \phi' \rightarrow \phi \quad \text{and} \quad \psi \rightarrow \psi'$$

System $\mathcal{H}$ (3)

- while command $C \equiv \textbf{while } b \textbf{ do } \{\theta\}\ C_0$

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ C\ \{\theta \wedge \neg b\}}$$

- strengthen precondition, weaken postcondition

$$\frac{\{\phi\}\ C\ \{\psi\}}{\{\phi'\}\ C\ \{\psi'\}} \quad \text{if} \quad \phi' \to \phi \quad \text{and} \quad \psi \to \psi'$$

- Hoare triple derivable in all logicals models in which implications in side condition are valid

backward construction of derivation

- given Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  "guess inference rule and guess assumptions"
  generate Hoare triples from which we could infer $\{\phi\}\ C\ \{\psi\}$
  ... and collect side conditions of inference rule (if any)

backward construction of derivation

- given Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  "guess inference rule and guess assumptions"
  generate Hoare triples from which we could infer $\{\phi\}\ C\ \{\psi\}$
  ... and collect side conditions of inference rule (if any)
- repeat on generated Hoare triples
  to generate new Hoare triples
  until every Hoare triple is an axiom

mechanize backward inference

- given Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  from what Hoare triples could we have inferred it?
  ... using what inference rule?

mechanize backward inference

- given Hoare triple $\{\phi\}\ C\ \{\psi\}$,
  from what Hoare triples could we have inferred it?
  ... using what inference rule?
- next:
  go through each form of command C
  (skip, update, seq, cond, while)

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$
- derivation can use what axiom and what inference rule?

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$
- derivation can use what axiom and what inference rule?
- axiom for skip

$$\frac{}{\{\phi\}\ \textbf{skip}\ \{\phi\}}$$

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$
- derivation can use what axiom and what inference rule?
- axiom for skip

$$\frac{}{\{\phi\}\ \textbf{skip}\ \{\phi\}}$$

- 'strengthen precondition, weaken postcondition' inference rule

$$\frac{\{\phi\}\ C\ \{\psi\}}{\{\phi'\}\ C\ \{\psi'\}}\quad \text{if}\quad \phi' \to \phi \quad \text{and} \quad \psi \to \psi'$$

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$
- possible derivation sequence: axiom for (skip), followed by weaking of postcondition

$$\frac{\overline{\{\phi\}\ \textbf{skip}\ \{\phi\}}}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$
- possible derivation sequence: axiom for (skip), followed by weaking of postcondition

$$\frac{\overline{\{\phi\}\ \textbf{skip}\ \{\phi\}}}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$

- side condition: $\phi \rightarrow \psi$

backward inference

- $$\frac{???}{\{\phi\}\ \mathbf{skip}\ \{\psi\}}$$
- possible derivation sequence: axiom for (skip), followed by weaking of postcondition

$$\frac{\overline{\{\phi\}\ \mathbf{skip}\ \{\phi\}}}{\{\phi\}\ \mathbf{skip}\ \{\psi\}}$$

- side condition: $\phi \to \psi$
- possible derivation sequence:
  axiom for (skip), followed by strengthening of precondition

$$\frac{\overline{\{\psi\}\ \mathbf{skip}\ \{\psi\}}}{\{\phi\}\ \mathbf{skip}\ \{\psi\}}$$

backward inference

- $$\frac{???}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$
- possible derivation sequence: axiom for (skip), followed by weaking of postcondition

$$\frac{\overline{\{\phi\}\ \textbf{skip}\ \{\phi\}}}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$

- side condition: $\phi \to \psi$
- possible derivation sequence:
  axiom for (skip), followed by strengthening of precondition

$$\frac{\overline{\{\psi\}\ \textbf{skip}\ \{\psi\}}}{\{\phi\}\ \textbf{skip}\ \{\psi\}}$$

- same side condition: $\phi \to \psi$

new axiom for skip

- $$\frac{}{\{\phi\}\ \textbf{skip}\ \{\psi\}} \quad \text{if} \quad \phi \to \psi$$

new axiom for skip

- $$\frac{}{\{\phi\}\ \textbf{skip}\ \{\psi\}} \quad \text{if} \quad \phi \to \psi$$
- old axiom & strengthening of precondition

new axiom for skip

- $$\frac{}{\{\phi\}\ \textbf{skip}\ \{\psi\}}\quad \text{if}\ \ \phi \to \psi$$
- old axiom & strengthening of precondition
- ϕ is a precondition for ψ under **skip**
  if and only if
  $\phi \to \psi$ is valid

new axiom for skip

- $$\frac{}{\{\phi\}\ \textbf{skip}\ \{\psi\}}\ \text{ if }\ \phi \to \psi$$
- old axiom & strengthening of precondition
- ϕ is a precondition for ψ under **skip**
  if and only if
  $\phi \to \psi$ is valid
- ψ is the weakest precondition for ψ under **skip**

new axiom for update

- $$\frac{}{\{\phi\}\ x := e\ \{\psi\}} \quad \text{if} \quad \phi \to \psi[e/x]$$

new axiom for update

- $$\frac{}{\{\phi\}\ x := e\ \{\psi\}}\quad \text{if}\ \ \phi \to \psi[e/x]$$
- old axiom & strengthening of precondition

new axiom for update

- $$\frac{}{\{\phi\}\ x := e\ \{\psi\}} \quad \text{if} \quad \phi \rightarrow \psi[e/x]$$
- old axiom & strengthening of precondition
- ϕ is a precondition for ψ under $x := e$
  if and only if
  $\phi \rightarrow \psi[e/x]$ is valid

new axiom for update

- $$\frac{}{\{\phi\}\ x := e\ \{\psi\}}\ \text{ if }\ \phi \to \psi[e/x]$$
- old axiom & strengthening of precondition
- ϕ is a precondition for ψ under $x := e$
  if and only if
  $\phi \to \psi[e/x]$ is valid
- $\psi[e/x]$ is the weakest precondition for ψ under $x := e$

new rule for seq

- old rule:

$$\frac{\{\phi\}\ C_1\ \{\theta\} \qquad \{\theta\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1 \ ; \ C_2\ \ \{\psi\}}$$

new rule for seq

- old rule:

$$\frac{\{\phi\}\ C_1\ \{\theta\} \qquad \{\theta\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\phi_2\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}\phi \to \phi_1$$

new rule for seq

- old rule:

$$\frac{\{\phi\}\ C_1\ \{\theta\} \qquad \{\theta\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\phi_2\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}\ \phi \to \phi_1$$

- let ϕ_2 be the weakest precondition of ψ under C_2 and let ϕ_1 be the weakest precondition of ϕ_2 under C_1

new rule for seq

- old rule:

$$\frac{\{\phi\}\ C_1\ \{\theta\} \qquad \{\theta\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\phi_2\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}\,\phi \to \phi_1$$

- let ϕ_2 be the weakest precondition of ψ under C_2 and let ϕ_1 be the weakest precondition of ϕ_2 under C_1
- ϕ is a precondition for ψ under $C_1\ ;\ C_2$
  if and only if
  $\phi \to \phi_1$ is valid

new rule for seq

- old rule:

$$\frac{\{\phi\}\ C_1\ \{\theta\} \qquad \{\theta\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\phi_2\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \ C_1\ ;\ C_2\ \ \{\psi\}}\ \phi \to \phi_1$$

- let ϕ_2 be the weakest precondition of ψ under C_2 and let ϕ_1 be the weakest precondition of ϕ_2 under C_1
- ϕ is a precondition for ψ under C_1 ; C_2
  if and only if
  $\phi \to \phi_1$ is valid
- the weakest precondition of ψ under C_1 ; C_2 is
  the weakest precondition of
  (the weakest precondition of ψ under C_2)
  under C_1

new rule for cond

- old rule:

$$\frac{\{\phi \wedge b\}\ C_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}}$$

new rule for cond

- old rule:

$$\frac{\{\phi \wedge b\}\ C_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\psi\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}} \quad \phi \to (\neg b \vee \phi_1) \ \text{ and } \ \phi \to (b \vee \phi_2)$$

new rule for cond

- old rule:

$$\frac{\{\phi \wedge b\}\ C_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\psi\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}} \quad \phi \to (\neg b \vee \phi_1) \ \text{ and } \ \phi \to (b \vee \phi_2)$$

- let ϕ_1 be the weakest precondition of ψ under C_1 and
  let ϕ_2 be the weakest precondition of ψ under C_2

new rule for cond

- old rule:

$$\frac{\{\phi \wedge b\}\ C_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\psi\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}} \quad \phi \to (\neg b \vee \phi_1)\ \text{ and }\ \phi \to (b \vee \phi_2)$$

- let ϕ_1 be the weakest precondition of ψ under C_1 and
  let ϕ_2 be the weakest precondition of ψ under C_2
- ϕ is a precondition for ψ under **if** b **then** C_1 **else** C_2
  if and only if
  $\phi \to ((\neg b \vee \phi_1) \wedge (b \vee \phi_2))$ is valid

new rule for cond

- old rule:

$$\frac{\{\phi \wedge b\}\ C_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}}$$

- new rule:

$$\frac{\{\phi_1\}\ C_1\ \{\psi\} \qquad \{\phi_2\}\ C_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \{\psi\}} \quad \phi \to (\neg b \vee \phi_1) \ \text{ and } \ \phi \to (b \vee \phi_2)$$

- let ϕ_1 be the weakest precondition of ψ under C_1 and
  let ϕ_2 be the weakest precondition of ψ under C_2
- ϕ is a precondition for ψ under **if** b **then** C_1 **else** C_2
  if and only if
  $\phi \to ((\neg b \vee \phi_1) \wedge (b \vee \phi_2))$ is valid
- the weakest precondition of ψ under **if** b **then** C_1 **else** C_2 is the conjunction of $\neg b \vee \phi_1$ and $b \vee \phi_2$

new rule for while

- old rule:

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\theta \wedge \neg b\}}$$

new rule for while

- old rule:

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\theta \wedge \neg b\}}$$

- new rule = old rule & strengthening & weakening

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\phi\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\psi\}} \quad \phi \rightarrow \theta \ \text{ and } \ \theta \wedge \neg b \rightarrow \psi$$

new rule for while

- old rule:
$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\theta \wedge \neg b\}}$$
- new rule = old rule & strengthening & weakening
$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\phi\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\psi\}} \quad \phi \to \theta \ \text{ and } \ \theta \wedge \neg b \to \psi$$
- ϕ is a precondition for ψ under **while** b **do** $\{\theta\}\ C_0$
if and only if
$\phi \to \theta$ and $\theta \wedge \neg b \to \psi$ are valid and $\{\theta \wedge b\}\ C_0\ \{\theta\}$

new rule for while

- old rule:

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\theta\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\theta \wedge \neg b\}}$$

- new rule = old rule & strengthening & weakening

$$\frac{\{\theta \wedge b\}\ C_0\ \{\theta\}}{\{\phi\}\ \ \textbf{while}\ b\ \textbf{do}\ \{\theta\}\ C_0\ \ \{\psi\}} \quad \phi \to \theta \ \text{ and } \ \theta \wedge \neg b \to \psi$$

- ϕ is a precondition for ψ under **while** b **do** $\{\theta\}\ C_0$
  if and only if
  $\phi \to \theta$ and $\theta \wedge \neg b \to \psi$ are valid and $\{\theta \wedge b\}\ C_0\ \{\theta\}$
- θ is the weakest precondition for ψ under **while** b **do** $\{\theta\}\ C_0$

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 wp(C, ψ)

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

weakest precondition wp(C, ψ)

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

verification condition

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

verification condition

- for command C of form: skip, update, seq, cond,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,

verification condition

- for command C of form: skip, update, seq, cond,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- check validity of verification condition

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

verification condition

- for command C of form: skip, update, seq, cond,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- check validity of verification condition

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

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

verification condition

- for command C of form: skip, update, seq, cond,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- check validity of verification condition

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

- for command C of form: **while** b **do** $\{\theta\}$ C_0 ,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,

verification condition

- for command C of form: skip, update, seq, cond,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- check validity of verification condition

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

- for command C of form: **while** b **do** $\{\theta\}\ C_0$,
- to check Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- check Hoare triple $\{\theta \wedge b\}\ C_0\ \{\theta\}$
  and check validity of two implications

$$\begin{aligned} &\phi \to \theta \\ &\theta \wedge \neg b \to \psi \end{aligned}$$