Strongest Postcondition

Andreas Podelski and Matthias Heizmann

May 31, 2017

correctness proof via forward derivation

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

correctness proof via forward derivation

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

correctness proof via forward derivation

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- construct a *forwards* 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)

correctness proof via forward derivation

- given a Hoare triple $\{\phi\}\ C\ \{\psi\}$,
- construct a *forwards* 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 triples with ψ and *strongest postcondition*
  for larger and larger program fragments

correctness proof via forward derivation

- given a Hoare triple $\{\phi\}$ C $\{\psi\}$,
- construct a *forwards* 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 triples with ψ and *strongest postcondition*
  for larger and larger program fragments
- verification condition:
  strongest postcondition of ϕ under C entails ψ
  ($+$ special treatment of while)

strongest postcondition post(C, ψ)

- post(**skip**, ϕ) $\equiv$

strongest postcondition post(C, ψ)

- post$(\textbf{skip}, \phi) \;\equiv\; \phi$
- post$(x := e, \phi) \;\equiv$

strongest postcondition post(C, ψ)

- post(**skip**, ϕ) $\equiv \phi$
- post($x := e, \phi$) $\equiv \phi[x_{old}/x] \wedge x = e[x_{old}/x]$
- post($C_1 \; ; \; C_2, \phi$) $\equiv$

strongest postcondition post(C, ψ)

- post(**skip**, ϕ) $\equiv$ ϕ
- post($x := e, \phi$) $\equiv$ $\phi[x_{old}/x] \wedge x = e[x_{old}/x]$
- post(C_1 ; C_2, ϕ) $\equiv$ post(C_2, post(C_1, ϕ))
- post(**if** b **then** C_1 **else** C_2, ϕ) $\equiv$

strongest postcondition post(C, ψ)

- post(**skip**, ϕ) $\equiv$ ϕ
- post($x := e, \phi$) $\equiv$ $\phi[x_{old}/x] \wedge x = e[x_{old}/x]$
- post($C_1 \; ; \; C_2, \phi$) $\equiv$ post(C_2, post(C_1, ϕ))
- post(**if** b **then** C_1 **else** C_2, ϕ) $\equiv$
  post($C_1, b \wedge \phi$) $\vee$ post($C_2, \neg b \wedge \phi$)
- post(**while** b **do** $\{\theta\}$ C_0, ϕ) $\equiv$

strongest postcondition post(C, ψ)

- post(**skip**, ϕ) $\equiv$ ϕ
- post($x := e, \phi$) $\equiv$ $\phi[x_{old}/x] \wedge x = e[x_{old}/x]$
- post(C_1 ; C_2, ϕ) $\equiv$ post(C_2, post(C_1, ϕ))
- post(**if** b **then** C_1 **else** C_2, ϕ) $\equiv$
  post($C_1, b \wedge \phi$) $\vee$ post($C_2, \neg b \wedge \phi$)
- post(**while** b **do** $\{\theta\}$ C_0, ϕ) $\equiv$ $\theta \wedge \neg b$

- next:
  static analysis constructs candidate for θ via forward analysis
  "reachability analysis"