

Hoare Logic

door Nico Broeder

Type Theory & Coq
23 mei 2016



Assertions and Hoare Triples

Proof Rules



Assertions

Definition `Assertion := state → Prop.`



Assertions

`Definition Assertion := state → Prop.`

`Definition as1 : Assertion := fun st ⇒ st X = 3.`

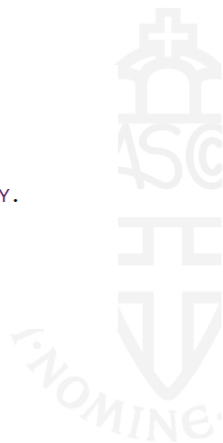


Assertions

`Definition Assertion := state → Prop.`

`Definition as1 : Assertion := fun st ⇒ st X = 3.`

`Definition as2 : Assertion := fun st ⇒ st X ≤ st Y.`

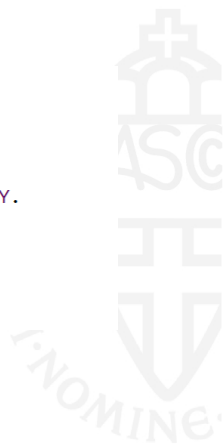


Assertions

Definition `Assertion := state → Prop.`

Definition `as1 : Assertion := fun st => st X = 3.`

Definition `as2 : Assertion := fun st => st X ≤ st Y.`

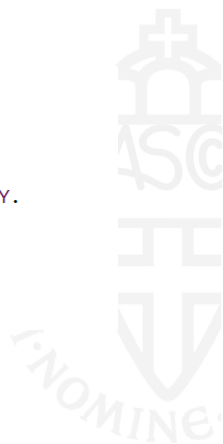


Assertions

Definition `Assertion := state → Prop.`

Definition `as1 : Assertion := fun st => st X = 3.`

Definition `as2 : Assertion := fun st => st X ≤ st Y.`



Assertions

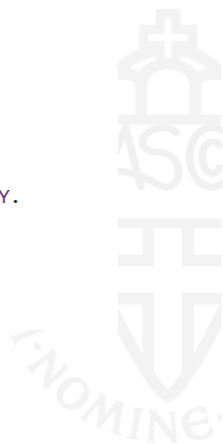
Definition `Assertion := state → Prop.`

Definition `as1 : Assertion := fun st => st X = 3.`

Definition `as2 : Assertion := fun st => st X ≤ st Y.`

`X = 3`

`X ≤ Y`



Assertions

$P \rightarrow Q$



Assertions

$P \rightarrow Q$

Definition `assert_implies` ($P\ Q : \text{Assertion}$) : `Prop` :=
 $\forall st, P\ st \rightarrow Q\ st.$



Assertions

$P \rightarrow Q$

Definition `assert_implies (P Q : Assertion) : Prop :=`
 `$\forall st, P \ st \rightarrow Q \ st.$`

Notation `"P \rightarrow Q" :=`
 `(assert_implies P Q) (at level 80) : hoare_spec_scope.`
Open Scope `hoare_spec_scope.`

Notation `"P \leftrightarrow Q" :=`
 `(P \rightarrow Q \wedge Q \rightarrow P) (at level 80) : hoare_spec_scope.`



Hoare Triples



Hoare Triples

$\{P\} c \{Q\}.$



Hoare Triples

$\{P\} c \{Q\}.$

Definition `hoare_triple`
 $(P:\text{Assertion}) (c:\text{com}) (Q:\text{Assertion}) : \text{Prop} :=$
 $\forall st\ st',$
 $c / st \Downarrow st' \rightarrow$
 $P\ st \rightarrow$
 $Q\ st'.$

Notation " $\{ P \} c \{ Q \}$ " :=
 $(\text{hoare_triple } P\ c\ Q)$ (at level 90, c at next level)
 $: \text{hoare_spec_scope}.$



Examples

1) $\{X = 2\} X ::= X + 1 \{X = 3\}$



Examples

$$1) \{X = 2\} X ::= X + 1 \{X = 3\}$$

$$2) \{X = 2 \wedge X = 3\} X ::= 5 \{X = 0\}$$



Examples

1) $\{X = 2\} X ::= X + 1 \{X = 3\}$

2) $\{X = 2 \wedge X = 3\} X ::= 5 \{X = 0\}$

3) $\{\text{True}\} \text{SKIP} \{\text{False}\}$



Examples

1) $\{X = 2\} X ::= X + 1 \{X = 3\}$

2) $\{X = 2 \wedge X = 3\} X ::= 5 \{X = 0\}$

3) $\{\text{True}\} \text{SKIP} \{\text{False}\}$

4) $\{\text{False}\} \text{SKIP} \{\text{True}\}$



Examples

1) $\{X = 2\} X ::= X + 1 \{X = 3\}$

2) $\{X = 2 \wedge X = 3\} X ::= 5 \{X = 0\}$

3) $\{\text{True}\} \text{SKIP} \{\text{False}\}$

4) $\{\text{False}\} \text{SKIP} \{\text{True}\}$

5) $\{\text{True}\} \text{WHILE True DO SKIP END} \{\text{False}\}$



Examples



Examples

Theorem hoare_post_true : $\forall (P Q : \text{Assertion}) c,$
 $(\forall st, Q \ st) \rightarrow$
 $\{P\} c \{Q\}.$



Theorem hoare_pre_false : $\forall (P Q : \text{Assertion}) c,$
 $(\forall st, \sim(P \ st)) \rightarrow$
 $\{P\} c \{Q\}.$



SKIP



SKIP

$$\frac{}{\{ P \} \text{ SKIP } \{ P \}} \text{ (hoare_skip)}$$

Theorem `hoare_skip` : $\forall P,$
 $\{P\} \text{ SKIP } \{P\}.$

□



Assignment



Assignment

$\{ Y = 1 \} X ::= Y \{ X = 1 \}$



Assignment

$$\{ Y = 1 \} X ::= Y \{ X = 1 \}$$

$$\{ a = 1 \} X ::= a \{ X = 1 \}$$


Assignment

$$\{ Y = 1 \} X ::= Y \{ X = 1 \}$$

$$\{ a = 1 \} X ::= a \{ X = 1 \}$$

$$\{ Q [X \mapsto a] \} X ::= a \{ Q \}$$


Assignment

$$\{ Y = 1 \} X ::= Y \{ X = 1 \}$$

$$\{ a = 1 \} X ::= a \{ X = 1 \}$$

$$\{ Q [X \mapsto a] \} X ::= a \{ Q \}$$

Example

$$\{ (0 \leq X \wedge X \leq 5) [X \mapsto 3] \\ \text{i.e., } (0 \leq 3 \wedge 3 \leq 5) \}$$

$$X ::= 3$$

$$\{ 0 \leq X \wedge X \leq 5 \}$$


Assignment formalization

```

Definition assn_sub X a P : Assertion :=
  fun (st : state) =>
    P (update st X (aeval st a)).
    
```

```

Notation "P [ X |-> a ]" := (assn_sub X a P) (at level 10).
    
```



Assignment formalization

Definition `assn_sub X a P : Assertion :=`
`fun (st : state) =>`
`P (update st X (aeval st a)).`

Notation "`P [X |-> a]`" := (`assn_sub X a P`) (at level 10).

`{Q [X ↦ a]} X ::= a {Q}` (hoare_asgn)

Theorem `hoare_asgn : ∀Q X a,`
`{Q [X ↦ a]} (X ::= a) {Q}.`

□



Rules of Consequence



Rules of Consequence

$\{(X = 3) \ [X \mapsto 3]\} X ::= 3 \ \{X = 3\},$

$\{\text{True}\} X ::= 3 \ \{X = 3\}.$



Rules of Consequence

$$\{\{X = 3\} [X \mapsto 3]\} X ::= 3 \{X = 3\},$$

$$\{\text{True}\} X ::= 3 \{X = 3\}.$$

$$\frac{\{\{P'\} c \{Q'\}\} \quad P \rightarrow P'}{\{\{P\} c \{Q\}\}} \quad (\text{hoare_consequence_pre}) \qquad \frac{\{\{P\} c \{Q'\}\} \quad Q' \rightarrow Q}{\{\{P\} c \{Q\}\}} \quad (\text{hoare_consequence_post})$$





Rules of Consequence

$$\{\{X = 3\} [X \mapsto 3]\} X ::= 3 \{X = 3\},$$

$$\{\text{True}\} X ::= 3 \{X = 3\}.$$

$$\frac{\{\{P'\} c \{Q\}\} \quad P \rightarrow P'}{\{\{P\} c \{Q\}\}} \quad (\text{hoare_consequence_pre}) \qquad \frac{\{\{P\} c \{Q'\}\} \quad Q' \rightarrow Q}{\{\{P\} c \{Q\}\}} \quad (\text{hoare_consequence_post})$$

Theorem `hoare_consequence_pre` : $\forall (P P' Q : \text{Assertion}) c,$
 $\{\{P'\} c \{Q\}\} \rightarrow$
 $P \rightarrow P' \rightarrow$
 $\{\{P\} c \{Q\}\}.$

□

Theorem `hoare_consequence_post` : $\forall (P Q Q' : \text{Assertion}) c,$
 $\{\{P\} c \{Q'\}\} \rightarrow$
 $Q' \rightarrow Q \rightarrow$
 $\{\{P\} c \{Q\}\}.$

□

Sequencing

$$\frac{}{\{\{ P \} \} c1;;c2 \{\{ R \} \}} \text{ (hoare_seq)}$$



Sequencing

$$\frac{\begin{array}{l} \{ P \} c1 \{ Q \} \\ \{ Q \} c2 \{ R \} \end{array}}{\{ P \} c1;;c2 \{ R \}} \quad (\text{hoare_seq})$$



Sequencing

$$\frac{\begin{array}{l} \{ P \} c1 \{ Q \} \\ \{ Q \} c2 \{ R \} \end{array}}{\{ P \} c1;;c2 \{ R \}} \text{ (hoare_seq)}$$

Example

$\{ \text{True} \} X ::= 1;; Y ::= 2 \{ X = 1 \wedge Y = 2 \}$



Sequencing

$$\frac{\begin{array}{l} \{ P \} c1 \{ Q \} \\ \{ Q \} c2 \{ R \} \end{array}}{\{ P \} c1;;c2 \{ R \}} \quad (\text{hoare_seq})$$

Example

$\{ \text{True} \} X ::= 1;; Y ::= 2 \quad \{ X = 1 \wedge Y = 2 \}$

$\{ 1 = 1 \} X ::= 1 \quad \{ X = 1 \}$

$\{ X = 1 \wedge 2 = 2 \} Y ::= 2 \quad \{ X = 1 \wedge Y = 2 \}$



Sequencing

$$\frac{\begin{array}{l} \{ P \} c1 \{ Q \} \\ \{ Q \} c2 \{ R \} \end{array}}{\{ P \} c1;;c2 \{ R \}} \quad (\text{hoare_seq})$$

Example

$\{ \text{True} \} X ::= 1;; Y ::= 2 \quad \{ X = 1 \wedge Y = 2 \}$

$\{ \text{True} \} X ::= 1 \quad \{ X = 1 \}$

$\{ X = 1 \wedge 2 = 2 \} Y ::= 2 \quad \{ X = 1 \wedge Y = 2 \}$



Sequencing

$$\frac{\begin{array}{l} \{ P \} c1 \{ Q \} \\ \{ Q \} c2 \{ R \} \end{array}}{\{ P \} c1;;c2 \{ R \}} \quad (\text{hoare_seq})$$

Example

$\{ \text{True} \} X ::= 1;; Y ::= 2 \quad \{ X = 1 \wedge Y = 2 \}$

$\{ \text{True} \} X ::= 1 \quad \{ X = 1 \wedge 2 = 2 \}$

$\{ X = 1 \wedge 2 = 2 \} Y ::= 2 \quad \{ X = 1 \wedge Y = 2 \}$



Conditionals

$$\frac{}{\{P\} \text{ IFB } b \text{ THEN } c1 \text{ ELSE } c2 \{Q\}}$$


Conditionals

$$\frac{\begin{array}{l} \{P\} \ c1 \ \{Q\} \\ \{P\} \ c2 \ \{Q\} \end{array}}{\{P\} \ \text{IFB } b \ \text{THEN } c1 \ \text{ELSE } c2 \ \{Q\}}$$



Conditionals

$$\frac{\begin{array}{l} \{P\} c1 \{Q\} \\ \{P\} c2 \{Q\} \end{array}}{\{P\} \text{IFB } b \text{ THEN } c1 \text{ ELSE } c2 \{Q\}}$$

$\{ \text{True} \} \text{IFB } X == 0 \text{ THEN } Y ::= 2 \text{ ELSE } Y ::= X + 1 \{ X \leq Y \}$



Conditionals

$$\frac{
 \begin{array}{c}
 \{P\} \ c1 \ \{Q\} \\
 \{P\} \ c2 \ \{Q\}
 \end{array}
 }{
 \{P\} \ \text{IFB } b \ \text{THEN } c1 \ \text{ELSE } c2 \ \{Q\}
 }$$

$$\frac{
 \begin{array}{c}
 \{ \text{True} \} \ Y ::= 2 \ \{ X \leq Y \} \\
 \{ \text{True} \} \ Y ::= X + 1 \ \{ X \leq Y \}
 \end{array}
 }{
 \{ \text{True} \} \ \text{IFB } X == 0 \ \text{THEN } Y ::= 2 \ \text{ELSE } Y ::= X + 1 \ \{ X \leq Y \}
 }$$



Conditionals

$$\frac{\begin{array}{l} \{P \wedge b\} c1 \{Q\} \\ \{P \wedge \sim b\} c2 \{Q\} \end{array}}{\{P\} \text{IFB } b \text{ THEN } c1 \text{ ELSE } c2 \{Q\}}$$

$$\frac{\begin{array}{l} \{ \text{True} \} Y ::= 2 \{ X \leq Y \} \\ \{ \text{True} \} Y ::= X + 1 \{ X \leq Y \} \end{array}}{\{ \text{True} \} \text{IFB } X == 0 \text{ THEN } Y ::= 2 \text{ ELSE } Y ::= X + 1 \{ X \leq Y \}}$$



Conditionals

$$\frac{\begin{array}{l} \{P \wedge b\} c1 \{Q\} \\ \{P \wedge \sim b\} c2 \{Q\} \end{array}}{\{P\} \text{IFB } b \text{ THEN } c1 \text{ ELSE } c2 \{Q\}}$$

$$\frac{\begin{array}{l} \{ \text{True} \} Y ::= 2 \{ X \leq Y \} \\ \{ \text{True} \} Y ::= X + 1 \{ X \leq Y \} \end{array}}{\{ \text{True} \} \text{IFB } X == 0 \text{ THEN } Y ::= 2 \text{ ELSE } Y ::= X + 1 \{ X \leq Y \}}$$

Definition `bassn b : Assertion :=
 fun st => (beval st b = true).`



Conditionals

$$\frac{\begin{array}{l} \{P \wedge b\} c1 \{Q\} \\ \{P \wedge \sim b\} c2 \{Q\} \end{array}}{\{P\} \text{IFB } b \text{ THEN } c1 \text{ ELSE } c2 \{Q\}}$$

$$\frac{\begin{array}{l} \{ \text{True} \} Y ::= 2 \{ X \leq Y \} \\ \{ \text{True} \} Y ::= X + 1 \{ X \leq Y \} \end{array}}{\{ \text{True} \} \text{IFB } X == 0 \text{ THEN } Y ::= 2 \text{ ELSE } Y ::= X + 1 \{ X \leq Y \}}$$

Definition `bassn b : Assertion :=`
`fun st => (beval st b = true).`

Theorem `hoare_if` : $\forall P Q b c1 c2,$
`{fun st => P st \wedge bassn b st} c1 {Q} \rightarrow`
`{fun st => P st \wedge \sim (bassn b st)} c2 {Q} \rightarrow`
`{P} (IFB b THEN c1 ELSE c2 FI) {Q}.`

□

Loops

$$\frac{}{\{P\} \text{ WHILE } b \text{ DO } c \text{ END } \{Q\}} \quad (\text{hoare_while})$$


Loops

$$\frac{\{\!P\!\} c \{\!P\!\}}{\{\!P\!\} \text{ WHILE } b \text{ DO } c \text{ END } \{\!P\!\}} \quad (\text{hoare_while})$$

The proposition P is called an *invariant* of the loop.



Loops

$$\frac{\{\!P\!\} c \{\!P\!\}}{\{\!P\!\} \text{ WHILE } b \text{ DO } c \text{ END } \{\!P \wedge \sim b\!\}} \quad (\text{hoare_while})$$

The proposition P is called an *invariant* of the loop.



Loops

$$\frac{\{\!P \wedge b\!\} c \{\!P\!\}}{\{\!P\!\} \text{ WHILE } b \text{ DO } c \text{ END } \{\!P \wedge \sim b\!\}} \quad (\text{hoare_while})$$

The proposition P is called an *invariant* of the loop.



Loops

$$\frac{\{\!P \wedge b\!\} c \{\!P\!\}}{\{\!P\!\} \text{WHILE } b \text{ DO } c \text{ END } \{\!P \wedge \sim b\!\}} \quad (\text{hoare_while})$$

The proposition P is called an *invariant* of the loop.

P is the assertion $X = 0$
`WHILE X = 2 DO X := 1 END`



Loops

$$\frac{\{\!P \wedge b\!\} c \{\!P\!\}}{\{\!P\!\} \text{WHILE } b \text{ DO } c \text{ END } \{\!P \wedge \sim b\!\}} \quad (\text{hoare_while})$$

The proposition P is called an *invariant* of the loop.

P is the assertion $X = 0$
`WHILE X = 2 DO X := 1 END`
 $\{\!P \wedge b\!\} c \{\!P\!\}$
 but *not* $\{\!P\!\} c \{\!P\!\}$



Summary





Summary

$$\frac{}{\{Q \ [X \mapsto a]\} \ X ::= a \ \{Q\}} \quad (\text{hoare_asgn})$$

$$\frac{}{\{P\} \ \text{SKIP} \ \{P\}} \quad (\text{hoare_skip})$$

$$\frac{\begin{array}{l} \{P\} \ c1 \ \{Q\} \\ \{Q\} \ c2 \ \{R\} \end{array}}{\{P\} \ c1;;c2 \ \{R\}} \quad (\text{hoare_seq})$$

$$\frac{\begin{array}{l} \{P \wedge b\} \ c1 \ \{Q\} \\ \{P \wedge \sim b\} \ c2 \ \{Q\} \end{array}}{\{P\} \ \text{IFB } b \ \text{THEN } c1 \ \text{ELSE } c2 \ \text{FI} \ \{Q\}} \quad (\text{hoare_if})$$

$$\frac{\{P \wedge b\} \ c \ \{P\}}{\{P\} \ \text{WHILE } b \ \text{DO } c \ \text{END} \ \{P \wedge \sim b\}} \quad (\text{hoare_while})$$

$$\frac{\begin{array}{l} \{P'\} \ c \ \{Q'\} \\ P \rightarrow P' \\ Q' \rightarrow Q \end{array}}{\{P\} \ c \ \{Q\}} \quad (\text{hoare_consequence})$$

