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

$P \to Q$

Assertions

```
P ->> Q

Definition assert_implies (P Q : Assertion) : Prop :=
  ∀st, P st → Q st.
```

Assertions

```
P ->> Q

Definition assert_implies (P Q : Assertion) : Prop :=
  ∀st, P st → Q st.

Notation "P ->> Q" :=
  (assert_implies P Q) (at level 80) : hoare_spec_scope.
Open Scope hoare_spec_scope.

Notation "P <<->> Q" :=
  (P ->> Q ∧ Q ->> P) (at level 80) : hoare_spec_scope.
```

Hoare Triples

Hoare Triples

```
{P} c {Q}.
```

Hoare Triples

```
{P} c {Q}.

Definition hoare_triple
           (P:Assertion) (c:com) (Q:Assertion) : Prop :=
  ∀st st',
       c / st ⇓ st' →
       P st →
       Q st'.

Notation "{ P } c { Q }" :=
  (hoare_triple P c Q) (at level 90, c at next level)
  : 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 ∧ X = 3} X ::= 5 {X = 0}

3) {True} SKIP {False}

Examples

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

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

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

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

Examples

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

2) {X = 2 ∧ X = 3} X ::= 5 {X = 0}

3) {True} SKIP {False}

4) {False} SKIP {True}

5) {True} WHILE True DO SKIP END {False}

Examples

Examples

```
Theorem hoare_post_true : ∀(P Q : Assertion) c,
  (∀st, Q st) →
  {P} c {Q}.
```

□

```
Theorem hoare_pre_false : ∀(P Q : Assertion) c,
  (∀st, ~(P st)) →
  {P} c {Q}.
```

□

SKIP

SKIP

$$\frac{}{\{\ P\ \}\ \texttt{SKIP}\ \{\ P\ \}}\ \text{(hoare\_skip)}$$

```
Theorem hoare_skip : ∀P,
     {P} SKIP {P}.
```

□

Assignment

Assignment

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

Assignment

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

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

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

$$\{ (0 \leq X \wedge X \leq 5)\ [X \mapsto 3] \}$$

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).
```

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

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

□

Rules of Consequence

Rules of Consequence

```
{(X = 3) [X ↦ 3]} X ::= 3 {X = 3},

{True} X ::= 3 {X = 3}.
```

Rules of Consequence

```
{(X = 3) [X ↦ 3]} X ::= 3 {X = 3},

{True} X ::= 3 {X = 3}.
```

$$\frac{\{P'\}\ c\ \{Q\} \qquad P \to P'}{\{P\}\ c\ \{Q\}}\ \text{(hoare\_consequence\_pre)} \qquad \frac{\{P\}\ c\ \{Q'\} \qquad Q' \to Q}{\{P\}\ c\ \{Q\}}\ \text{(hoare\_consequence\_post)}$$

Rules of Consequence

```
{(X = 3) [X ↦ 3]} X ::= 3 {X = 3},

{True} X ::= 3 {X = 3}.
```

$$\frac{\{P'\}\ c\ \{Q\} \qquad P \to P'}{\{P\}\ c\ \{Q\}}\ \text{(hoare\_consequence\_pre)} \qquad \frac{\{P\}\ c\ \{Q'\} \qquad Q' \to Q}{\{P\}\ c\ \{Q\}}\ \text{(hoare\_consequence\_post)}$$

```
Theorem hoare_consequence_pre : ∀(P P' Q : Assertion) c,
  {P'} c {Q} →
  P ->> P' →
  {P} c {Q}.
```

□

```
Theorem hoare_consequence_post : ∀(P Q Q' : Assertion) c,
  {P} c {Q'} →
  Q' ->> Q →
  {P} c {Q}.
```

□

Sequencing

$$\frac{}{\{\ P\ \}\ c1;;c2\ \{\ R\ \}} \quad \text{(hoare\_seq)}$$

Sequencing

$$\frac{\{\ P\ \}\ c1\ \{\ Q\ \} \qquad \{\ Q\ \}\ c2\ \{\ R\ \}}{\{\ P\ \}\ c1;;c2\ \{\ R\ \}}\ \text{(hoare\_seq)}$$

Sequencing

$$\frac{\{\ P\ \}\ c1\ \{\ Q\ \} \qquad \{\ Q\ \}\ c2\ \{\ R\ \}}{\{\ P\ \}\ c1;;c2\ \{\ R\ \}}\ \text{(hoare\_seq)}$$

Example

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

Sequencing

$$\frac{\{\ P\ \}\ c1\ \{\ Q\ \} \qquad \{\ Q\ \}\ c2\ \{\ R\ \}}{\{\ P\ \}\ c1;;c2\ \{\ R\ \}}\ \text{(hoare\_seq)}$$

Example

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

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

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

Sequencing

$$\frac{\{\ P\ \}\ c1\ \{\ Q\ \} \qquad \{\ Q\ \}\ c2\ \{\ R\ \}}{\{\ P\ \}\ c1;;c2\ \{\ R\ \}}\ \text{(hoare\_seq)}$$

Example

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

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

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

Sequencing

$$\frac{\{ P \} \; c1 \; \{ Q \} \qquad \{ Q \} \; c2 \; \{ R \}}{\{ P \} \; c1;;c2 \; \{ R \}} \quad \text{(hoare\_seq)}$$

Example

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

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

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

Conditionals

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

Conditionals

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

Conditionals

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

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

Conditionals

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

$$\frac{\{\ \mathrm{True}\ \}\ Y ::= 2\ \{\ X \le Y\ \} \qquad \{\ \mathrm{True}\ \}\ Y ::= X + 1\ \{\ X \le Y\ \}}{\{\ \mathrm{True}\ \}\ \mathtt{IFB}\ X == 0\ \mathtt{THEN}\ Y ::= 2\ \mathtt{ELSE}\ Y ::= X + 1\ \{\ X \le Y\ \}}$$

Conditionals

$$\frac{\{P \wedge b\}\ c1\ \{Q\} \qquad \{P \wedge \sim b\}\ c2\ \{Q\}}{\{P\}\ \texttt{IFB}\ b\ \texttt{THEN}\ c1\ \texttt{ELSE}\ c2\ \{Q\}}$$

$$\frac{\{\ \mathit{True}\ \}\ Y ::= 2\ \{\ X \le Y\ \} \qquad \{\ \mathit{True}\ \}\ Y ::= X + 1\ \{\ X \le Y\ \}}{\{\ \mathit{True}\ \}\ \texttt{IFB}\ X == 0\ \texttt{THEN}\ Y ::= 2\ \texttt{ELSE}\ Y ::= X + 1\ \{\ X \le Y\ \}}$$

Conditionals

$$\frac{\{P \wedge b\}\ c1\ \{Q\} \qquad \{P \wedge \sim b\}\ c2\ \{Q\}}{\{P\}\ \mathtt{IFB}\ b\ \mathtt{THEN}\ c1\ \mathtt{ELSE}\ c2\ \{Q\}}$$

$$\frac{\{\ \mathrm{True}\ \}\ Y ::= 2\ \{\ X \le Y\ \} \qquad \{\ \mathrm{True}\ \}\ Y ::= X + 1\ \{\ X \le Y\ \}}{\{\ \mathrm{True}\ \}\ \mathtt{IFB}\ X == 0\ \mathtt{THEN}\ Y ::= 2\ \mathtt{ELSE}\ Y ::= X + 1\ \{\ X \le Y\ \}}$$

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

Conditionals

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

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

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

Theorem hoare_if : ∀P Q b c1 c2,
  {fun st ⇒ P st ∧ bassn b st} c1 {Q} →
  {fun st ⇒ P st ∧ ~(bassn b st)} c2 {Q} →
  {P} (IFB b THEN c1 ELSE c2 FI) {Q}.
```

□

Loops

$$\frac{}{\{P\}\ \texttt{WHILE b DO c END}\ \{Q\}}\ \text{(hoare\_while)}$$

Loops

$$\frac{\{P\}\ c\ \{P\}}{\{P\}\ \texttt{WHILE b DO c END}\ \{P\}}\ \text{(hoare\_while)}$$

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

Loops

$$\frac{\{P\}\ c\ \{P\}}{\{P\}\ \texttt{WHILE b DO c END}\ \{P \wedge \sim b\}}\ \text{(hoare\_while)}$$

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

Loops

$$\frac{\{P \wedge b\}\ c\ \{P\}}{\{P\}\ \texttt{WHILE}\ b\ \texttt{DO}\ c\ \texttt{END}\ \{P \wedge \sim b\}}\ \text{(hoare\_while)}$$

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

Loops

$$\frac{\{P \wedge b\}\ c\ \{P\}}{\{P\}\ \texttt{WHILE}\ b\ \texttt{DO}\ c\ \texttt{END}\ \{P \wedge \sim b\}}\ \text{(hoare\_while)}$$

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

`P` is the assertion `X = 0`

```
WHILE X = 2 DO X := 1 END
```

Loops

$$\frac{\{P \wedge b\}\ c\ \{P\}}{\{P\}\ \texttt{WHILE}\ b\ \texttt{DO}\ c\ \texttt{END}\ \{P \wedge \sim b\}}\ \text{(hoare\_while)}$$

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

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

$$\frac{}{\{\ P\ \}\ \text{SKIP}\ \{\ P\ \}}\ \text{(hoare\_skip)}$$

$$\frac{\{\ P\ \}\ c1\ \{\ Q\ \} \quad \{\ Q\ \}\ c2\ \{\ R\ \}}{\{\ P\ \}\ c1;;c2\ \{\ R\ \}}\ \text{(hoare\_seq)}$$

$$\frac{\{P \wedge\ \ b\}\ c1\ \{Q\} \quad \{P \wedge \sim b\}\ c2\ \{Q\}}{\{P\}\ \text{IFB b THEN c1 ELSE c2 FI}\ \{Q\}}\ \text{(hoare\_if)}$$

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

$$\frac{\{P'\}\ c\ \{Q'\} \quad P \rightarrow P' \quad Q' \rightarrow Q}{\{P\}\ c\ \{Q\}}\ \text{(hoare\_consequence)}$$