Floyd-Hoare Logic

Also called Axiomatic Semantics

- Based on formal logic (first order predicate calculus)
- Logical system built from axioms and inference rules
- Mainly suited to simple imperative programming languages
- Ideas applicable quite broadly

Goal: Derive statements of form

\[
\{ P \} \text{C} \{ Q \}
\]

- \(P, Q\) logical statements about state, \(P\) precondition, \(Q\) postcondition, \(C\) program
- Example:

\[
\{ x = 1 \} \ x := x + 1 \ { x = 2 } \]

Partial vs Total Correctness

- An expression \(\{ P \} \text{C} \{ Q \}\) is a partial correctness statement
- For total correctness must also prove that \(C\) terminates (i.e. doesn’t run forever)
  - Written: \([ P ] \text{C} [ Q ]\)
- Will only consider partial correctness here
Simple Imperative Language

- We will give rules for simple imperative language
  \[
  \langle \text{command} \rangle ::= \langle \text{variable} \rangle := \langle \text{term} \rangle \\
  | \langle \text{command} \rangle; \ldots; \langle \text{command} \rangle \\
  | \text{if} \langle \text{statement} \rangle \text{then} \langle \text{command} \rangle \text{else} \langle \text{command} \rangle \\
  | \text{while} \langle \text{statement} \rangle \text{do} \langle \text{command} \rangle
  \]
- Could add more features, like for-loops

Substitution

- Notation: \( P[e/v] \) (sometimes \( P[v \rightarrow e] \))
- Meaning: Replace every \( v \) in \( P \) by \( e \)
- Example:
  \[
  (x + 2)[y - 1/x] = ((y - 1) + 2)
  \]

The Assignment Rule

- \( \{ P[e/x] \} x := e \ {P} \)
- Example:
  \[
  \{ ? \} x := y \ {x = 2}
  \]

Examples:

\[
\{ y = 2 \} x := y \ {x = 2} \\
\{ y = 2 \} x := 2 \ {y = x} \\
\{ x + 1 = n + 1 \} x := x + 1 \ {x = n + 1} \\
\{ 2 = 2 \} x := 2 \ {x = 2}
\]
Which Inferences Are Correct?

\[
\begin{align*}
\{x > 0 \land x < 5\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x = 3\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x > 0 \land x < 5\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x \times x < 25\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x > 0 \land x < 5\} & \Rightarrow (x := x \times x \{x < 25\})
\end{align*}
\]

The Assignment Rule – Your Turn

- What is the weakest precondition of \( x := x + y \{x + y = wx\} \)?

\[
\begin{align*}
\{?\} & \Rightarrow (x := x + y \{x + y = wx\}) \\
\{x := x + y\} & \Rightarrow (x := x + y \{x + y = wx\})
\end{align*}
\]

Precondition Strengthening

\[
\begin{align*}
(P \Rightarrow P') & \Rightarrow (P \land C \{Q\}) \\
(P' \land C \{Q\}) & \Rightarrow (P \land C \{Q\})
\end{align*}
\]

- Meaning: If we can show that \( P \) implies \( P' \) (i.e. \( P \Rightarrow P' \)) and we can show that \( P' \land C \{Q\} \), then we know that \( P \land C \{Q\} \).

- \( P \) is stronger than \( P' \) means \( P \Rightarrow P' \).

Examples:

\[
\begin{align*}
(x = 3) & \Rightarrow (x < 7) \Rightarrow (x := x + 3 \{x < 10\}) \\
(x = 3) & \Rightarrow (x := x + 3 \{x < 10\}) \\
True & \Rightarrow (2 = 2) \Rightarrow (2 = 2) \Rightarrow (x := 2 \{x = 2\}) \\
(x = n) & \Rightarrow (x + 1 = n + 1) \Rightarrow (x := x + 1 \{x = n + 1\})
\end{align*}
\]

Which Inferences Are Correct?

\[
\begin{align*}
\{x > 0 \land x < 5\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x = 3\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x > 0 \land x < 5\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x \times x < 25\} & \Rightarrow (x := x \times x \{x < 25\}) \\
\{x > 0 \land x < 5\} & \Rightarrow (x := x \times x \{x < 25\})
\end{align*}
\]

The Assignment Rule – Your Turn

- What is the weakest precondition of \( x := x + y \{x + y = wx\} \)?

\[
\begin{align*}
\{(x + y) + y = w(x + y)\} & \Rightarrow (x := x + y \{x + y = wx\}) \\
\{x := x + y\} & \Rightarrow (x := x + y \{x + y = wx\})
\end{align*}
\]
Then

February 23, 2018 15 / 41

February 23, 2018 17 / 41

Else Rule suffices to show:

February 23, 2018 16 / 41

February 23, 2018 14 / 41

Rule of Consequence

Post Condition Weakening

Sequencing

If Then Else

Which Inferences Are Correct?

\[
\begin{align*}
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \quad \text{YES} \\
\{x = 3\} \ x := \ x \times \ x \ (x < 25) & \\
\{x = 3\} \ x := \ x \times \ x \ (x < 25) & \quad \text{NO} \\
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \\
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \quad \text{YES} \\
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \\
\end{align*}
\]

Which Inferences Are Correct?

\[
\begin{align*}
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \quad \text{YES} \\
\{x = 3\} \ x := \ x \times \ x \ (x < 25) & \quad \text{YES} \\
\{x = 3\} \ x := \ x \times \ x \ (x < 25) & \quad \text{NO} \\
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \quad \text{YES} \\
\{x > 0 \land x < 5\} \ x := \ x \times \ x \ (x < 25) & \\
\end{align*}
\]

Post Condition Weakening

\[
\frac{(P) \ C \ \{Q'\} \ Q' \Rightarrow Q}{(P) \ C \ \{Q\}}
\]

- Example:

\[
\begin{align*}
\{x + y = 5\} \ x := \ x + y \ (x = 5) & \quad (x = 5) \Rightarrow (x < 10) \\
\{x + y = 5\} \ x := \ x + y \ (x < 10) & \\
\end{align*}
\]

Rule of Consequence

\[
\begin{align*}
P & \Rightarrow P' \\
\frac{(P') \ C \ \{Q'\} \ Q' \Rightarrow Q}{(P) \ C \ \{Q\}}
\end{align*}
\]

- Logically equivalent to the combination of Precondition Strengthening and Postcondition Weakening
- Uses \(P \Rightarrow P\) and \(Q \Rightarrow Q\)

Sequencing

\[
\frac{(P) \ G_1 \ \{Q\} \ C_1 \ (R)}{(P) \ C_1; \ C_2 \ (R)}
\]

- Example:

\[
\begin{align*}
\{z = z \land z = z\} \ x := \ {z = z \land z = z} \\
\{x = z \land z = z\} \ y := \ {x = z \land y = z} & \\
\{z = z \land z = z\} \ x := z; \ y := z \ (x = z \land y = z) & \\
\end{align*}
\]

If Then Else

\[
\frac{(P \land B) \ C_1 \ \{Q\} \ (P \land \neg B) \ C_2 \ \{Q\}}{(P) \ if \ B \ then \ C_1 \ else \ C - 2 \ (Q)}
\]

- Example:

\[
\begin{align*}
\{y = a\} \ if \ x < 0 \ then \ y := y - x \ else \ y := y + x \ (y = a + |x|) \\
\end{align*}
\]

By If, Then, Else Rule suffices to show:

- (1) \(y = a \land x < 0\) \(y := y - x \ (y = a + |x|)\) and
- (4) \(y = a \land \neg(x < 0)\) \(y := y + x \ (y = a + |x|)\)
We need a rule to be able to make assertions about while loops.

- Inference rule because we can only draw conclusions if we know something about the body
- Lets start with:

\[
\{ \ ? \} \ C \{ \ ? \} \\
\{ \ ? \} \text{ if } \{ \ ? \} \text{ then } y := y - x \text{ else } y := y + x \{ y = a + |x| \}
\]

by the If.Then.Else Rule
While

- Always know $\neg B$ when while loop finishes
- Final While rule:
  \[
  \{P \land B\} \quad C \quad \{P\}
  \]
  \[
  \{P\} \quad \text{while} \quad B \quad \text{do} \quad C \quad \{P \land \neg B\}
  \]

Example

- Need to find $P$ that is true before and after loop is executed, such that
  \[
  (P \land \neg (x < n)) \Rightarrow y = n \ast n
  \]

- First attempt:
  \[
  y = x \ast x
  \]

  Motivation:
  - Want $y = n \ast n$
  - $x$ counts up to $n$
  - **Guess**: Each pass of loop calculates next square
Problem with (2)

- Want \((y = x * x \land \neg(x < n)) \Rightarrow (y = n * n)\)
- From \(\neg(x < n)\) have \(x \geq n\)
- Need \(x = n\)
- Don’t know this; from this could have \(x > n\)
- Need stronger invariant
- Try ading \(x < n\)
- Then have \(((x \leq n) \land \neg(x < n)) \Rightarrow (x = n)\)
- Then have \(x = n\) when loop done

Example

By Post-condition Weakening, suffices to show:

1. \(\{n \geq 0\}
   \begin{align*}
   x &:= 0; y := 0; \\
   \text{while } x < n \text{ do} \\
   y &:= y + ((2 * x) + 1); x := x + 1 \\
   \{y = x * x \land \neg(x < n)\}
   \end{align*}

and

2. \(y = x * x \land \neg(x < n) \Rightarrow (y = n * n)\)

Example

Second attempt:

\[P = ((y = x * x) \land (x \leq n))\]

Again by Post-condition Weakening, sufices to show:

1. \(\{n \geq 0\}
   \begin{align*}
   x &:= 0; y := 0; \\
   \text{while } x < n \text{ do} \\
   y &:= y + ((2 * x) + 1); x := x + 1 \\
   \{y = x * x \land (x \leq n) \land \neg(x < n)\}
   \end{align*}

and

2. \(((y = x * x) \land (x \leq n) \land \neg(x < n)) \Rightarrow (y = n * n)\)

Example

- For (1), set up While Rule using Sequencing Rule
- By Sequencing Rule, sufices to show

3. \(\{n \geq 0\}
   \begin{align*}
   x &:= 0; y := 0 \quad \{y = x * x \land (x \leq n)\}
   \end{align*}

and

4. \(\{y = x * x \land (x \leq n)\}
   \begin{align*}
   \text{while } x < n \text{ do} \\
   y &:= y + ((2 * x) + 1); x := x + 1 \\
   \{y = x * x \land (x \leq n) \land \neg(x < n)\}
   \end{align*}

Proof of (2)

- \(\neg(x < n) \Rightarrow (x \geq n)\)
- \(((x \geq n) \land (x \leq n)) \Rightarrow (x = n)\)
- \(((x = n) \land (y = x * x)) \Rightarrow (y = n * n)\)

Proof of (4)

By While Rule

\begin{align*}
(5) \quad \{(y = x * x \land (x \leq n) \land (x < n))\} \\
y &:= y + ((2 * x) + 1); x := x + 1 \\
\{y = x * x \land (x \leq n)\}
\end{align*}

\begin{align*}
\text{while } x < n \text{ do} \\
y &:= y + ((2 * x) + 1); x := x + 1 \\
\{y = x * x \land (x \leq n) \land \neg(x < n)\}
\end{align*}
Proof of (5)

By Sequencing Rule

\[(6)\] \\
\[\{ y = x \times x \} \land (x \leq n) \land ((x + 1) \leq n) \]
\[\land ((x + 1) \leq n) \]
\[y := y + ((2 \times x) + 1) \]
\[x := x + 1 \]
\[\{ y = x \times x \} \land (x \leq n)\]

(7) holds by Assignment Axiom

\[
\begin{align*}
(5) & \land (x < n) \Rightarrow ((x + 1) \leq n) \\
& \land ((x + 1) \leq n) \\
y & := y + ((2 \times x) + 1) \\
x & := x + 1 \\
\{ y = x \times x \} \land (x \leq n)\end{align*}
\]

Proof of (6)

By Precondition Strengthening

\[(8)\] \\
\[\{ y = x \times x \} \land (x < n) \Rightarrow ((x + 1) \leq n) \]
\[\land ((x + 1) \leq n) \]
\[y := y + ((2 \times x) + 1) \]
\[\{ y = x \times x \} \land (x < n) \Rightarrow ((x + 1) \leq n) \]
\[\land ((x + 1) \leq n) \]

(7) holds by Assignment Axiom

\[
\begin{align*}
(5) & \land (x < n) \Rightarrow ((x + 1) \leq n) \\
& \land ((x + 1) \leq n) \\
y & := y + ((2 \times x) + 1) \\
x & := x + 1 \\
\{ y = x \times x \} \land (x < n) \Rightarrow ((x + 1) \leq n) \\
& \land ((x + 1) \leq n) \]

Have (9) by Assignment Axiom

Proof of (7)

By Precondition Strengthening

\[(9)\] \\
\[\{ y = (x + 1) \times (x + 1) \} \land ((x + 1) \leq n) \]
\[\land ((x + 1) \leq n) \]
\[y := y + ((2 \times x) + 1) \]
\[\{ y = (x + 1) \times (x + 1) \} \land ((x + 1) \leq n) \]

(7) holds by Assignment Axiom

\[
\begin{align*}
(5) & \land (x < n) \Rightarrow ((x + 1) \leq n) \\
& \land ((x + 1) \leq n) \\
y & := y + ((2 \times x) + 1) \\
x & := x + 1 \\
\{ y = (x + 1) \times (x + 1) \} \land ((x + 1) \leq n) \]

Have (9) by Assignment Axiom

Proof of (8)

(10) \\
\[\{n \geq 0\} \land x := 0 \Rightarrow \{y = x \times x\} \land \{y \leq n\}\]

(11) \\
\[\{n \geq 0\} \land y := 0 \Rightarrow \{y = x \times x\} \land \{y \leq n\}\]

\[\{n \geq 0\} \land x := 0; y := 0 \Rightarrow \{y = x \times x\} \land \{y \leq n\}\]

Have (11) by Assignment Axiom

Proof of (9)

By Sequencing

\[(10)\] \\
\[\{ n \geq 0 \} \quad \{ (0 = x \times x) \land (x \leq n) \} \]
\[x := 0 \quad y := 0 \]
\[\{ (0 = x \times x) \land (x \leq n) \} \land \{ (0 = x \times x) \land (x \leq n) \} \]

\[\{ n \geq 0 \} \land x := 0; y := 0 \Rightarrow \{ (0 = x \times x) \land (x \leq n) \} \land \{ (0 = x \times x) \land (x \leq n) \} \]

Have (11) by Assignment Axiom

Proof of (10)

By Precondition Strengthening

\[(13)\] \\
\[\{0 = 0 \times 0\} \land (0 \leq n) \]
\[x := 0 \]
\[\{0 = x \times x\} \land (x \leq n) \]
\[\{n \geq 0\} \land x := 0; y := 0 \Rightarrow \{0 = x \times x\} \land (x \leq n) \]

\[\{n \geq 0\} \land x := 0; y := 0 \Rightarrow \{0 = x \times x\} \land (x \leq n) \]

(12) \\
\[\{ n \geq 0 \} \Rightarrow \{ (0 = 0 \times 0) \land (0 \leq n) \} \]
\[\{ (0 = x \times x) \land (x \leq n) \} \land \{ (0 = x \times x) \land (x \leq n) \} \]

\[\{n \geq 0\} \land x := 0; y := 0 \Rightarrow \{0 = x \times x\} \land (x \leq n) \]

For (12), \(0 = 0 \times 0\) and \((n \geq 0) \Rightarrow (0 \leq n)\)

Have (13) by Assignment Axiom

Finishes (10), thus (3), thus (1)