Hoare Triple

{ \{ P \} S \{ Q \} }

Precondition    Statement    Postcondition
Hoare Triple

\{
  x=3
\} \ x*=2 \ { x>0 \}
Hoare Triple

\{ x=3 \} \quad x^* = 2 \quad \{ \quad \}

Strongest Postcondition: \( X = 6 \)
Hoare Triple

\{ \quad \} \quad x^* = 2 \quad \{ \quad x > 0 \quad \}

Weakest Precondition: \( X > 0 \)
Weakest Precondition

Weakest precondition \( P_{\text{weak}} = \text{wp}(S, Q) \)

(1) \( \{ P_{\text{weak}} \} S \{ Q \} \) is valid and

(2) \( P \Rightarrow P_{\text{weak}} \) for all \( P \) such that \( \{ P \} S \{ Q \} \)
Deterministic Language

Step 1:  
No-operation  
Abort computation  
Assignment  
Conditional  
While loop  

Step 2:  
Probabilistic Choice  
Nondeterministic Choice  

S::=

  skip
  fail
  x = e
  if (b) then S1 else S2
  while (b) S
  S1 [p] S2
  S1 [ ] S2
Weakest Precondition Analysis

\{ _____ \}  \ x^* = 2 \ \ { x > 0 \}
Weakest Precondition Analysis

\{ \quad \} \quad S \quad \{ \quad Q \quad \}
Weakest Precondition Analysis

\{ \text{wp}(S, Q) \} \quad S \quad \{ Q \}
Weakest Precondition Analysis for Deterministic Programs

Program: Predicate Transformer

Predicate: \( Q \in \mathbb{Q}: \{States\} \rightarrow \{True, False\} \)

Analysis: \( wp: Stmt \times \mathbb{Q} \rightarrow \mathbb{Q} \)

\[
wp \ (\text{skip}, Q) = Q
\]
\[
wp \ (\text{fail}, Q) = false
\]
\[
wp \ (x = e, Q) = Q[x/E]
\]

Substitutes the variable \( x \) with the expression \( E \) in the predicate \( Q \)
\[
\begin{array}{c}
\{ \quad \{ ?? \} \quad \}
\end{array}
\]

\[
x = y + 2
\]

\[
\begin{array}{c}
\{ \quad x > 0 \quad \}
\end{array}
\]
\[
\{ (x>0)[(x/y)+2] \} \\
x = y + 2 \\
\{ x>0 \}
\]
\[
\begin{align*}
\{ y + 2 & > 0 \} \\
\{ x & = y + 2 \} \\
\{ x & > 0 \}
\end{align*}
\]
\{ \text{??} \}

\textbf{x} = \textbf{x} + 2

\{ \textbf{x} \geq 0 \}
\{ x+2 > 0 \}

x = x + 2

\{ x \geq 0 \}
Weakest Precondition Analysis for Deterministic Programs

\[
\begin{align*}
\text{wp } (\text{skip}, Q) &= Q \\
\text{wp } (\text{fail}, Q) &= \text{false} \\
\text{wp } (x = e, Q) &= Q \left[ x/E \right] \\
\text{wp } (s_1; s_2, Q) &= \text{wp } (s_1, \text{wp } (s_2, Q)) \\
\text{wp } (\text{if } b \text{ then } S_1 \text{ else } S_2, Q) &= (b \Rightarrow \text{wp } (S_1, Q)) \land \\
&\quad (\neg b \Rightarrow \text{wp } (S_2, Q))
\end{align*}
\]

(We will discuss loops later)
Example

\{
(\text{True}) \land (\text{True})\}

x = 2;
\{
(x > 0 \Rightarrow 2 \cdot x > 3) \land (x \leq 0 \Rightarrow -2 \cdot x > 3)\}

y = 0;
\{
(x > 0 \Rightarrow 2 \cdot x > 3) \land (x \leq 0 \Rightarrow -2 \cdot x > 3)\}

if (x > 0) y = x;
else y = -x
\{
2 \cdot y > 3\}

z = 2 \cdot y;

\text{Postcondition: } \{ z > 3 \}
Probabilistic Analysis

**Expectation** \( \mathbb{E} : \{ProgramStates\} \rightarrow [0, +\infty) \)

Intuitively, adds weights to Boolean predicates
Embeds Boolean predicates numerically \([Q] \rightarrow \{0, 1\}\)

Probabilistic Analysis

**Expectation Transformer** \( WP : Stmt \times \mathbb{E} \rightarrow \mathbb{E} \)

Allows for both probabilistic choice \( S_1 \ [p] \ S_2 \) and nondeterministic choice \( S_1 \ [] \ S_2 \)

**Meaning of expectation predicates:**

*The probability* that program will establish \( \{ \text{Postcondition} \} \) is at least \( p \).

Weakest Precondition Analysis for Deterministic Programs

\[ wp \left( \text{skip, } Q \right) = Q \]
\[ wp \left( \text{fail, } Q \right) = \text{false} \]
\[ wp \left( x = e, Q \right) = Q \left[ x/e \right] \]
\[ wp \left( s_1 ; s_2, Q \right) = wp \left( s_1, wp(s_2, Q) \right) \]
\[ wp \left( \text{if } b \text{ then } S_1 \text{ else } S_2, Q \right) = \left( b \Rightarrow wp(S_1, Q) \right) \land \left( \neg b \Rightarrow wp(S_2, Q) \right) \]
Weakest Precondition Analysis for Probabilistic Programs

\[ wp \text{ (skip, } Q) = Q \]
\[ wp \text{ (fail, } Q) = 0 \]
\[ wp \text{ (} x = e, Q \text{) } = Q \left[ x/e \right] \]
\[ wp \text{ (} s_1; s_2, Q \text{) } = wp \text{ (} s_1, wp(s_2, Q) \text{) } \]
\[ wp \text{ (if } b \text{ then } S_1 \text{ else } S_2, Q \text{) } = [b] \text{ wp(} S_1, Q \text{) } + [\neg b] \text{ wp(} S_2, Q \text{) } \]
\[ wp \text{ (} s_1 [p] s_2, Q \text{) } = p \cdot wp(s_1, Q) + (1-p) \cdot wp(s_2, Q) \]
\[ wp \text{ (} s_1 [] s_2, Q \text{) } = \min( \text{ wp(} s_1, Q \text{), wp(} s_2, Q \text{) } ) \]
Example

Precondition (1): \( \{ p \cdot [1 = 1] + (1 - p) \cdot [1 = 3] \} \)

Program: \( x = 1 \ [p] \ x = 3; \)

Postcondition (1): \( \{ [x = 1] \} \)

\[
wp \ (x = e, Q) = Q \ [x/e] \\
wp \ (s1 \ [p] \ s2, Q) = p \cdot \wp(s1, Q) + (1-p) \cdot \wp(s2, Q)
\]
Example

Precondition (1): \( \{ p \cdot [1 = 1] + (1 - p) \cdot [1 = 3] \} \)

Program: \( x = 1 \ [p] \ x = 3; \)

Postcondition (1): \( \{ [x = 1] \} \)

\[
wp\ (x = e, Q) = Q \ [x/e] \\
wp\ (s1 \ [p] \ s2, Q) = \ p \cdot wp(s1, Q) + (1-p) \cdot wp(s2, Q)
\]
Example

Precondition (1): \{ p \}

Program: \( x = 1 [p] x = 3; \)

Postcondition (1): \{ [x = 1] \}

\[
wp ( x = e, Q) = Q [x/e]
\]

\[
w p (s1 [p] s2, Q) = p \cdot wp(s1, Q) + (1-p) \cdot wp(s2, Q)
\]
Example

Precondition (2): \{ 1 - p \}

Program: \( x = 1 \ [p] \ x = 3; \)

Postcondition (2): \{ [x = 3] \}
Example

Precondition (3): \{ 0 \}

Program: \texttt{x = 1 [p] x = 3;}

Postcondition (3): \{ [x = 10] \}
Example: Statement Sequence

Program:

\[
\{ p \} \\
\{ p \cdot [1 + 1 = 2] + (1 - p) \cdot [1 - 1 = 2] \} \\
x = 1; \\
\{ p \cdot [x + 1 = 2] + (1 - p) \cdot [x - 1 = 2] \} \\
x = x + 1 \ [p] \\
\{ [x = 2] \} \\
x = x - 1;
\]

Postcondition: \{ [x = 2] \}
Example: Probability and Nondeterminism

Program:

\{
\ 1 \\
\}
\{
\ \text{min}([3 + 1 > 0], [3 - 1 > 0])
\}
x = 3;
\{
\ \text{min}([x + 1 > 0], [x - 1 > 0])
\}
x = x + 1 \ [ ] x = x - 1;

Postcondition: \{ [x > 0] \}
Example: Probability and Nondeterminism

Program:

\{ \ p \ \} \\
\{ \ \min([3 + 1 > 0],p \cdot [3 - 1 > 0]) \ \} \\
x = 3; \\
\{ \ \min([x + 1 > 0],p \cdot [x - 1 > 0] + (1 - p) \cdot [\text{false}] \ \} \\
x = x + 1 \ [\ p \] fail \\

Postcondition:  \ { \ [x > 0] \ }
Example: Probability and Nondeterminism

**Average and Worst-Case Analyses**

**Program (1):**

\[
\begin{align*}
\{ & \frac{2}{3} \} \\
\{ & \frac{1}{3} \cdot [1 > 1] + \frac{2}{3} \cdot \left( \frac{1}{2} \cdot [2 > 1] + \frac{1}{2} [3 > 1] \right) \}
\end{align*}
\]

\((x=1) \left\lceil \frac{1}{3} \right\rceil \ ( (x=2) \left\lceil \frac{1}{2} \right\rceil \ (x=3) )\)

**Postcondition:** \(\{ [x > 1] \}\)

**Program (2):**

\[
\begin{align*}
\{ & 0 \} \\
\{ & \text{min}( [1 > 1], \text{min}( [2 > 1], [3 > 1] ) ) \}
\end{align*}
\]

\((x=1) \left[ \right] \ ( (x=2) \left[ \right] \ (x=3) )\)

**Postcondition:** \(\{ [x > 1] \}\)