Probabilistic & **A**pproximate **C**omputing

Sasa Misailovic

UIUC

Hoare Triple

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

Precondition **Statement** **Postcondition**

Hoare Triple

{ x=3 } x*=2 { x>0 }

Hoare Triple

$$\{ x=3 \}\ \mathbf{x*=2}\ \{ \_\_\_\_ \}$$

Strongest Postcondition: **X = 6**

Hoare Triple

{ ______ } x*=2 { x>0 }

Weakest Precondition: **X > 0**

Weakest Precondition

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

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

(2) **$P \Rightarrow P_{weak}$** for all **P** such that **$\{P\}$ S $\{Q\}$**

Deterministic Language

Step 1:	`S::=`
No-operation	`skip`
Abort computation	`fail`
Assignment	`x = e`
Conditional	`if (b) then S1 else S2`
While loop	`while (b) S`
Step 2:	
Probabilistic Choice	`S1 [p] S2`
Nondeterministic Choice	`S1 [] S2`

Weakest Precondition Analysis

{ ________ } x*=2 { x>0 }

Weakest Precondition Analysis

{ ______________ } **S** { **Q** }

Weakest Precondition Analysis

$$\{\ wp(S, Q)\ \}\ \ S\ \ \{\ Q\ \}$$

Weakest Precondition Analysis for Deterministic Programs

Program: Predicate Transformer

Predicate: $\mathbf{Q} \in \mathbb{Q}: \{\boldsymbol{States}\} \rightarrow \{\boldsymbol{True}, \boldsymbol{False}\}$

Analysis: $\mathbf{wp}: \boldsymbol{Stmt} \times \mathbb{Q} \rightarrow \mathbb{Q}$

wp (skip, Q) = Q

wp (fail, Q) = false

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

Substitutes the variable x with the expression E in the predicate Q

$\{\ ??\ \}$

$$x = y + 2$$

$\{\ x>0\ \}$

$$\{\ (x>0)[x/y+2]\ \}$$

$$x = y + 2$$

$$\{\ x>0\ \}$$

$$\{ y+2>0 \}$$

$$x = y + 2$$

$$\{ x>0 \}$$

$$\{\ ??\ \}$$

$$x = x + 2$$

$$\{\ x>0\ \}$$

$$\{ x+2 > 0 \}$$

$$x = x + 2$$

$$\{ x>0 \}$$

Weakest Precondition Analysis for Deterministic Programs

wp (skip, Q) = Q

wp (fail, Q) = false

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

wp (s1; s2, Q) = wp (s1, wp(s2, Q))

wp (if b then S1else S2,Q) = (b ⇒ wp(S1, Q)) ∧
(¬b ⇒ wp(S2, Q))

(We will discuss loops later)

Example

$\{\ (True)\ \wedge\ (True)\ \}$

```
x = 2;
```

$\{\ (x > 0 \Rightarrow 2 \cdot x > 3)\ \wedge\ (x \leq 0 \Rightarrow -2 \cdot x > 3)\ \}$

```
y = 0;
```

$\{\ (x > 0 \Rightarrow 2 \cdot x > 3)\ \wedge\ (x \leq 0 \Rightarrow -2 \cdot x > 3)\ \}$

```
if ( x > 0 ) y = x;
else y = -x
```

$\{\ 2 \cdot y > 3\ \}$

```
z = 2 * y;
```

Postcondition: { z > 3 }

Probabilistic Analysis

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

Intuitively, adds weights to Boolean predicates

Embeds Boolean predicates numerically **[Q] -> {0, 1}**

Morgan, McIver, Seidel, Probabilistic Predicate Transformers TOPLAS Vol. 18.3, (1996)

Probabilistic Analysis

Expectation Transformer $WP: Stmt \times \mathbb{E} \rightarrow \mathbb{E}$

Allows for both probabilistic choice **S1 [p] S2**
and nondeterministic choice **S1 [] S2**

Meaning of expectation predicates:

The probability that program will establish {*Postcondition*}
is at least *p*.

Morgan, McIver, Seidel, Probabilistic Predicate Transformers TOPLAS Vol. 18.3, (1996)

Weakest Precondition Analysis for Deterministic Programs

$wp\ (\text{skip}, Q) = Q$

$wp\ (\text{fail}, Q) = \text{false}$

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

$wp\ (s1; s2, Q) = wp\ (s1, wp(s2, Q))$

$wp\ (\text{if } b \text{ then } S1 \text{ else } S2, Q) = (b \Rightarrow wp(S1, Q)) \wedge$
$(\neg b \Rightarrow wp(S2, Q))$

Weakest Precondition Analysis for Probabilistic Programs

$wp(\text{skip}, Q) = Q$

$wp(\text{fail}, Q) = 0$

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

$wp(s1; s2, Q) = wp(s1, wp(s2, Q))$

$wp(\text{if } b \text{ then } S1 \text{ else } S2, Q) = [b]\, wp(S1, Q) + [\neg b]\, wp(S2, Q)$

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

$wp(s1\ [\,]\ s2, Q) = \min(wp(s1, Q), wp(s2, Q))$

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 · wp(s1, Q) + (1-p) · 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 · wp(s1, Q) + (1-p) · wp(s2, Q)

Example

Precondition (1): $\{ p \}$

Program: `x = 1 [p] x = 3;`

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

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

wp (s1 [p] s2, Q) = p · wp(s1, Q) + (1-p) · wp(s2, Q)

Example

Precondition (2): $\{\ \mathbf{1 - \boldsymbol{p}}\ \}$

Program: `x = 1 [p] x = 3;`

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

Example

Precondition (3): { **0** }

Program: `x = 1 [p] x = 3;`

Postcondition (3): { [x = 10] }

Example: Statement Sequence

Program:

$\{\ \boldsymbol{p}\ \}$

$\{\ \boldsymbol{p} \cdot [\mathbf{1} + \mathbf{1} = \mathbf{2}] + (\mathbf{1} - \boldsymbol{p}) \cdot [\mathbf{1} - \mathbf{1} = \mathbf{2}]\ \}$

```
x = 1;
```

$\{\ \boldsymbol{p} \cdot [\boldsymbol{x} + \mathbf{1} = \mathbf{2}] + (\mathbf{1} - \boldsymbol{p}) \cdot [\boldsymbol{x} - \mathbf{1} = \mathbf{2}]\ \}$

```
x = x + 1 [p] x = x - 1;
```

Postcondition: { [x = 2] }

Example: Probability and Nondeterminism

Program:

$\{ \ \mathbf{1} \ \}$

$\{ \ \mathbf{min}([\mathbf{3} + \mathbf{1} > \mathbf{0}], [\mathbf{3} - \mathbf{1} > \mathbf{0}]) \ \}$

```
x = 3;
```

$\{ \ \mathbf{min}([\boldsymbol{x} + \mathbf{1} > \mathbf{0}], [\boldsymbol{x} - \mathbf{1} > \mathbf{0}] \ \}$

```
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 [] ( x = x - 1 [p] fail );
```

Postcondition: { [x > 0] }

Example: Probability and Nondeterminism

Average and Worst-Case Analyses

Program (1):

$\{\ 2/3\ \}$

$\{\ \frac{1}{3}\cdot[1>1]+\frac{2}{3}\cdot\left(\frac{1}{2}\cdot[2>1]+\frac{1}{2}[3>1]\right)\ \}$

```
(x=1) [1/3] ( (x=2) [1/2] (x=3) )
```

Postcondition: $\{\ [x > 1]\ \}$

Program (2):

$\{\ 0\ \}$

$\{\ \min(\,[1>1],\min(\,[2>1],[3>1]\,)\,)\ \}$

```
(x=1) [] ( (x=2) [] (x=3) )
```

Postcondition: $\{\ [x > 1]\ \}$