Formal Verification – Inference Rules

① $$\frac{}{\{Q[E/x]\}\ x = E\ \{Q\}}$$ assignment

② $$\frac{P \to P' \qquad \{P'\}\ C\ \{Q\}}{\{P\}\ C\ \{Q\}}$$ "precondition strengthening" implied

③ $$\frac{\{P\}\ C\ \{Q'\} \qquad Q' \to Q}{\{P\}\ C\ \{Q\}}$$ "post condition weakening" implied

④ $$\frac{\{P\}\ C_1\ \{Q\} \qquad \{Q\}\ C_2\ \{R\}}{\{P\}\ C_1; C_2\ \{R\}}$$ composition

⑤ $$\frac{\{P \wedge B\}\ C_1\ \{Q\} \qquad \{P \wedge \neg B\}\ C_2\ \{Q\}}{\{P\}\ \text{if } (B)\ C_1 \text{ else } C_2\ \{Q\}}$$ if-then-else

⑥ $$\frac{\{P \wedge B\}\ C\ \{Q\} \qquad (P \wedge \neg B) \to Q}{\{P\}\ \text{if } (B)\ C\ \{Q\}}$$ if-then

⑦ $$\frac{\{(I \wedge B)\}\ C\ \{I\}}{\{I\}\ \text{while } (B)\ C\ \{(I \wedge (\neg B))\}}$$ partial-while

empty

Formal Verification

Assignments

Nov 14.

Complete the following annotations

①
$x = 2;$
$\{(x = 2)\}$

②
$x = 2;$
$\{(x = y)\}$

③
$x = 2;$
$\{(x = 0)\}$

④
$x = x + 1;$
$\{x = n + 1\}$

⑤
$x = y;$
$\{(2 \cdot x = x + y)\}$

The "assignment" inference rule

$\{Q[E/x]\}$ then Q must be true when replacing every x by E.

$x = E;$

$\{Q\}$ if Q is true after assigning the value of E to x.

empty

Assignments

Prove that the following program satisfies the given triple under partial correctness

① $\{((x = x_0) \wedge (y = y_0))\}$

```
t = x;
x = y;
y = t;
```

$\{((x = y_0) \wedge (y = x_0))\}$

② $\{true\}$

```
z = x;
z = z + y;
u = z;
```

$\{(u = x + y)\}$

Conditional Statement (if-then) & (if-then-else)

① "if-then"

⊲ P D

if (B) {

C

}

⊲ Q D

② "if-then-else"

⊲ P D

if (B) {

C_1

} else {

C_2

}

⊲ Q D

Conditional Statements (If-Then)

Prove that the following program satisfies the given triple under partial correctness

⟨ true ⟩

if (max < x) {

max = x;

}

⟨ (max ≥ x) ⟩

Conditional Statements (If-Then-Else)

Prove that the following program satisfies the given triple under partial correctness.

{ true }

if ($x > y$) {

$max = x$;

} else {

$max = y$;

}

{ $((x > y) \wedge (max = x)) \vee ((x \leq y) \wedge (max = y))$ }