

CS 511: Formal Methods in Security and Privacy

Non-interference and RHL

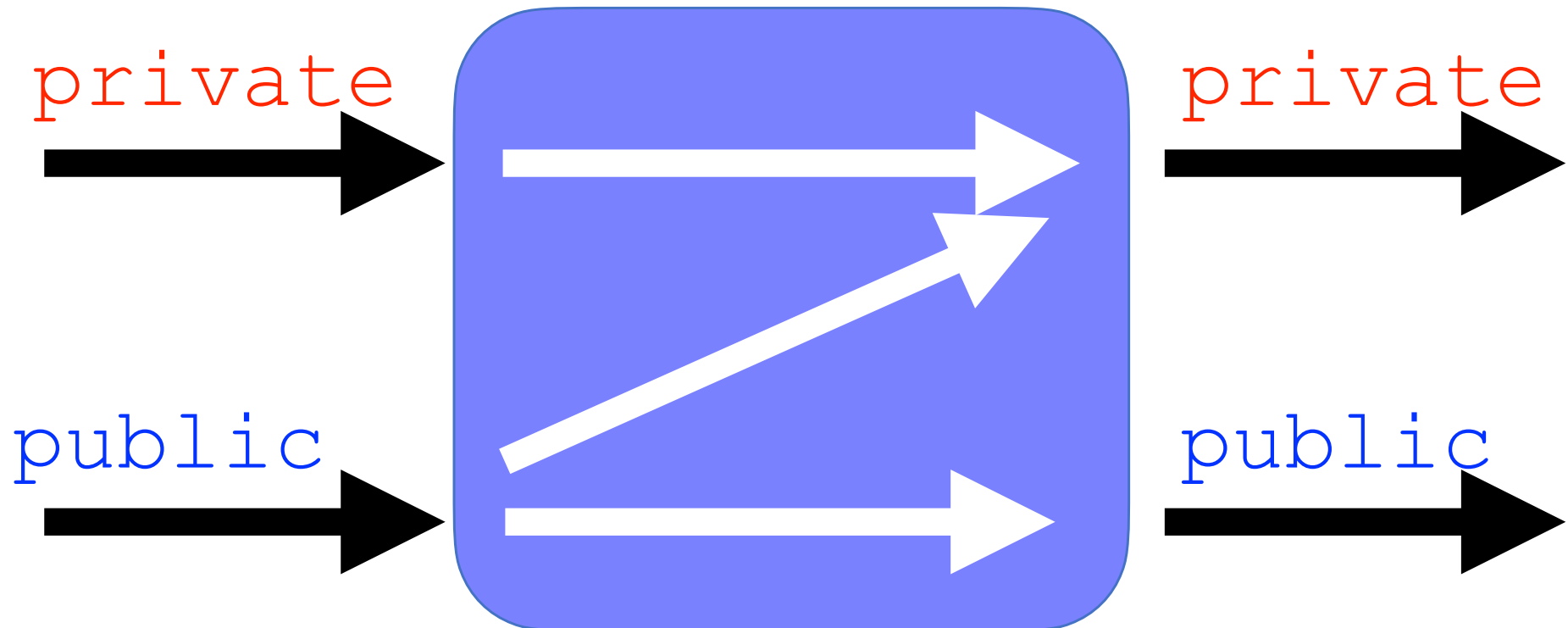
Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu

From the previous classes

Information Flow Control

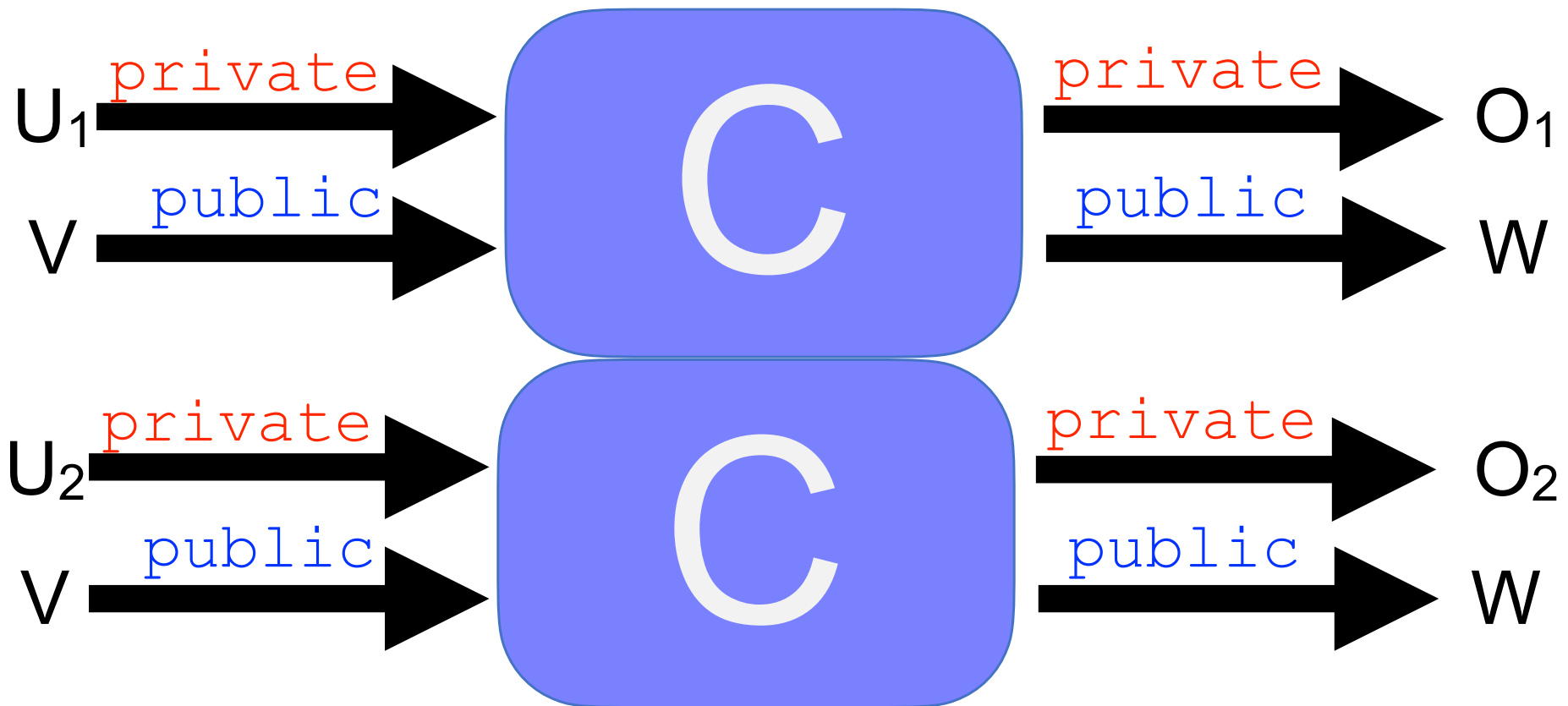
We want to guarantee that **confidential information** do not flow in what is considered **nonconfidential**.



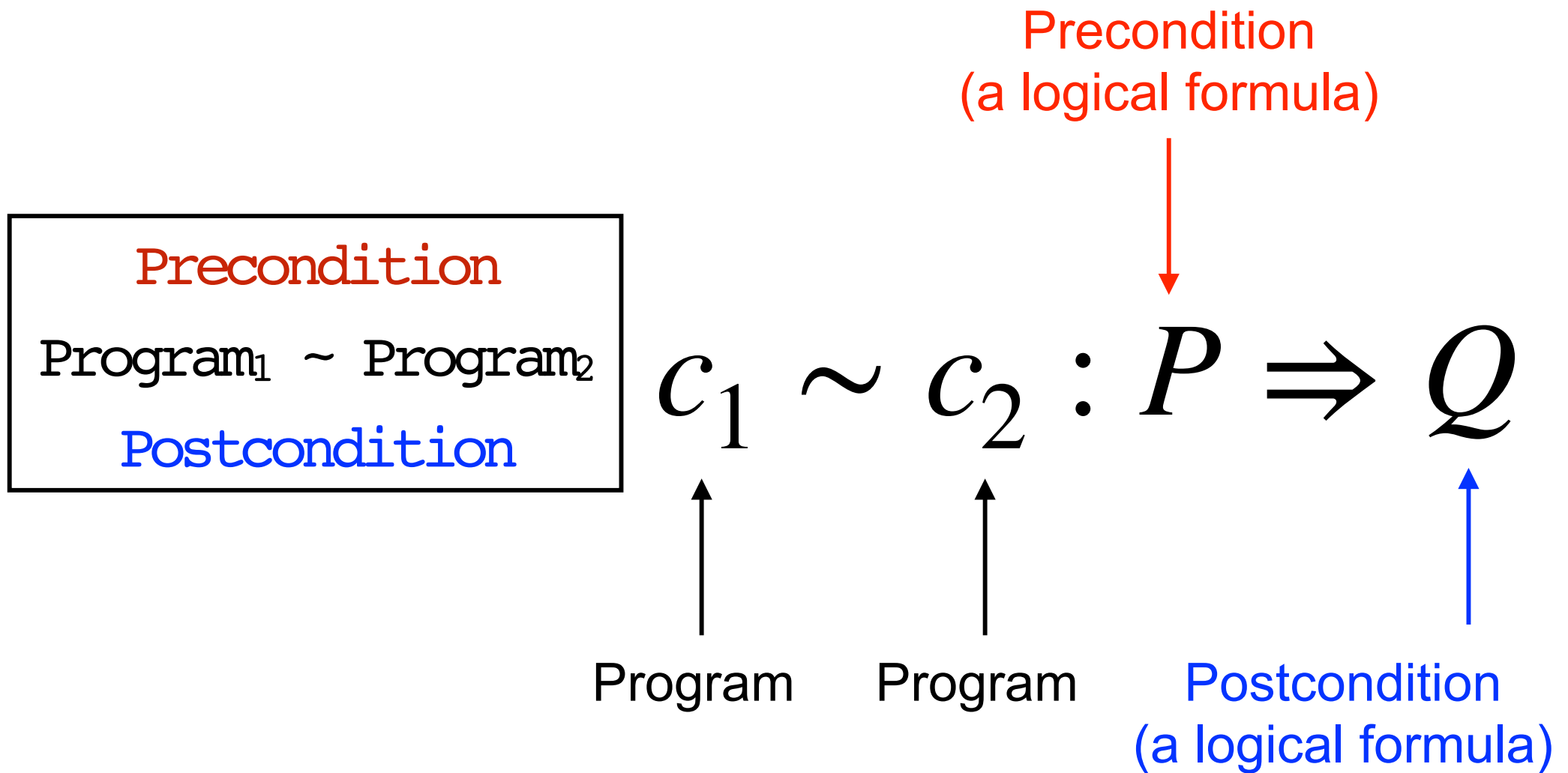
NonInterference

In symbols, c is **noninterferent** if and only if for every $m_1 \sim_{\text{low}} m_2$:

- 1) $\{c\}_{m_1} = \perp$ iff $\{c\}_{m_2} = \perp$
- 2) $\{c\}_{m_1} = m_1'$ and $\{c\}_{m_2} = m_2'$ implies $m_1' \sim_{\text{low}} m_2'$



Relational Hoare Logic - RHL



Validity of Hoare quadruple

We say that the quadruple $c_1 \sim c_2 : P \Rightarrow Q$ is **valid** if and only if for every pair of memories m_1, m_2 such that $P(m_1, m_2)$ we have:

- 1) $\{c_1\}_{m_1} = \perp$ iff $\{c_2\}_{m_2} = \perp$
- 2) $\{c_1\}_{m_1} = m_1'$ and $\{c_2\}_{m_2} = m_2'$ implies $Q(m_1', m_2')$.

Some Rules of Relational Hoare Logic

$$\frac{}{\vdash \text{skip} \sim \text{skip} : P \Rightarrow P}$$

$$\frac{}{\vdash \text{abort} \sim \text{abort} : \text{true} \Rightarrow \text{false}}$$

$$\vdash x_1 := e_1 \sim x_2 := e_2 :$$

$$P[e_1 \langle 1 \rangle / x_1 \langle 1 \rangle, e_2 \langle 2 \rangle / x_2 \langle 2 \rangle] \Rightarrow P$$

$$\vdash c_1 \sim c_2 : P \Rightarrow R \quad \vdash c_1' \sim c_2' : R \Rightarrow S$$

$$\frac{}{\vdash c_1 ; c_1' \sim c_2 ; c_2' : P \Rightarrow S}$$

$$\frac{P \Rightarrow S \quad \vdash c_1 \sim c_2 : S \Rightarrow R \quad R \Rightarrow Q}{\vdash c_1 \sim c_2 : P \Rightarrow Q}$$

Some Rules of Relational Hoare Logic

$$\vdash c_1 \sim c_2 : e_1 \langle 1 \rangle \wedge P \Rightarrow Q \quad P \Rightarrow e_1 \langle 1 \rangle = e_2 \langle 2 \rangle$$

$$\vdash c_1' \sim c_2' : \neg e_1 \langle 1 \rangle \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{l} \text{if } e_1 \text{ then } c_1 \text{ else } c_1' \\ \sim \\ \text{if } e_2 \text{ then } c_2 \text{ else } c_2' \end{array} : P \Rightarrow Q$$

$$\vdash c_1 \sim c_2 : e_1 \langle 1 \rangle \wedge P \Rightarrow P \quad P \Rightarrow e_1 \langle 1 \rangle = e_2 \langle 2 \rangle$$

$$\vdash \begin{array}{l} \text{while } e_1 \text{ do } c_1 \\ \sim \\ \text{while } e_2 \text{ do } c_2 \end{array} : P \Rightarrow P \wedge \neg e_1 \langle 1 \rangle$$

How can we prove this?

```
x:private  
y:public
```

```
y:=x  
y:=5
```

```
: =low ⇒ =low
```

How can we prove this?

```
x:private  
y:public
```

```
if y mod 3 = 0 then  
  x:=1  
else  
  x:=0
```

```
: =low  $\Rightarrow$  =low
```

How can we prove this?

```
x:private  
y:public
```

```
if x mod 3 = 0 then  
  y:=1  
else  
  y:=1
```

```
: =low  $\Rightarrow$  =low
```

How can we prove this?

```
x:private  
y:public
```

Can we prove it?

```
if x mod 3 = 0 then  
  y:=1  
else  
  y:=1
```

```
: =low  $\Rightarrow$  =low
```

Rules of Relational Hoare Logic

If then else

$$P \Rightarrow e_1 \langle 1 \rangle = e_2 \langle 2 \rangle$$

$$\vdash c_1 \sim c_2 : e_1 \langle 1 \rangle \wedge P \Rightarrow Q$$

$$\vdash c_1' \sim c_2' : \neg e_1 \langle 1 \rangle \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{l} \text{if } e_1 \text{ then } c_1 \text{ else } c_1' \\ \sim \\ \text{if } e_2 \text{ then } c_2 \text{ else } c_2' \end{array} : P \Rightarrow Q$$

Rules of Relational Hoare Logic

If then else - left

$$\vdash c_1 \sim c_2 : e < 1 > \wedge P \Rightarrow Q$$

$$\vdash c_1' \sim c_2 : \neg e < 1 > \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{c} \text{if } e \text{ then } c_1 \text{ else } c_1' \\ \sim \\ c_2 \end{array} : P \Rightarrow Q$$

Rules of Relational Hoare Logic

If then else - left

$$\vdash c_1 \sim c_2 : e < 2 > \wedge P \Rightarrow Q$$

$$\vdash c_1 \sim c_2' : \neg e < 2 > \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{c} c_1 \\ \sim \\ \text{if } e \text{ then } c_2 \text{ else } c_2' \end{array} : P \Rightarrow Q$$

How can we prove this?

```
x:private  
y:public
```

```
if x mod 3 = 0 then  
  y:=1  
else  
  y:=1
```

```
: =low  $\Rightarrow$  =low
```

How can we prove this?

```
x:public
z:private
y:private

y:=0
z:=0
if x=0 then z:=1;
if z=0 then y:=1

: =low ⇒ =low
```

How can we prove this?

```
s1:public
s2:private
r:private
i:public

proc Compare (s1:list[n] bool,s2:list[n] bool)
i:=0;
r:=0;
while i<n do
  if not(s1[i]=s2[i]) then
    r:=1
  i:=i+1

: n>0 /\ =low ⇒ =low
```

Rules of Relational Hoare-Logic

One-sided Rules

What do we do if our two programs have different forms? There are three pairs of *one-sided* rules.

$$\vdash \frac{\text{if } e \text{ then } c_1 \text{ else } c_1'}{\sim} : P \Rightarrow Q$$

c_2

Rules of Relational Hoare Logic

If-then-else — left

$$\vdash c_1 \sim c_2 : e < 1 > \wedge P \Rightarrow Q$$

$$\vdash c_1' \sim c_2 : \neg e < 1 > \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{c} \text{if } e \text{ then } c_1 \text{ else } c_1' \\ \sim \\ c_2 \end{array} : P \Rightarrow Q$$

Rules of Relational Hoare Logic

If-then-else — right

$$\vdash c_1 \sim c_2 : e \langle 2 \rangle \wedge P \Rightarrow Q$$

$$\vdash c_1 \sim c_2' : \neg e \langle 2 \rangle \wedge P \Rightarrow Q$$

$$\vdash \begin{array}{c} c_1 \\ \sim \\ \text{if } e \text{ then } c_2 \text{ else } c_2' \end{array} : P \Rightarrow Q$$

Assignment — left

$\vdash x := e \sim \text{skip} :$

$P[e \langle 1 \rangle / x \langle 1 \rangle] \Rightarrow P$

Assignment — right

$$\vdash \text{skip} \sim x := e :$$
$$P[e\langle 2 \rangle / x\langle 2 \rangle] \Rightarrow P$$

Also pair of one-sided rules for while — we'll ignore for now

Rules of Relational Hoare Logic

Program Equivalence Rule

$$\models P : c_1' \equiv c_1$$

$$\models P : c_2' \equiv c_2$$

$$\vdash c_1' \sim c_2' : P \Rightarrow Q$$

$$\vdash c_1 \sim c_2 : P \Rightarrow Q$$

$\models P : c_1 \equiv c_2$ means $\{c_1\}_m = \{c_2\}_m$

for all m such that $P(m)$

Rules of Relational Hoare Logic

Program Equivalences

$$\models P : \text{skip}; c \equiv c$$

$$\models P : c; \text{skip} \equiv c$$

$$\models P : (c1; c2); c3 \equiv c1; (c2; c3)$$

...

Rules of Relational Hoare Logic

Combining Composition and Equivalence

We can combine the Composition and Program Equivalence Rules to split commands where we like:

$$\vdash C_1 ; C_2 \sim C_1' : P \Rightarrow R$$

$$\vdash C_3 \sim C_2' ; C_3' : R \Rightarrow Q$$

$$\vdash C_1 ; C_2 ; C_3 \sim C_1' ; C_2' ; C_3' : P \Rightarrow Q$$

Rules of Relational Hoare Logic

Combining Composition and Equivalence

$$\frac{\begin{array}{l} \vdash c_1 \sim \text{skip} : P \Rightarrow R \\ \vdash c_2 \sim c_1' : R \Rightarrow Q \end{array}}{\vdash c_1 ; c_2 \sim \text{skip} ; c_1' : P \Rightarrow Q}$$

$$\vdash c_1 ; c_2 \sim c_1' : P \Rightarrow Q$$

Rules of Relational Hoare Logic

Combining Composition and Equivalence

$$\frac{\begin{array}{l} \vdash C_1 \sim C_1' : P \Rightarrow R \\ \vdash C_2 \sim \text{skip} : R \Rightarrow Q \end{array}}{\vdash C_1 ; C_2 \sim C_1' ; \text{skip} : P \Rightarrow Q}$$

$$\vdash C_1 ; C_2 \sim C_1' : P \Rightarrow Q$$

Soundness

If we can derive $\vdash C_1 \sim C_2 : P \Rightarrow Q$ through the rules of the logic, then the quadruple $C_1 \sim C_2 : P \Rightarrow Q$ is valid.

Validity of Hoare quadruple

We say that the quadruple $c_1 \sim c_2 : P \Rightarrow Q$ is **valid** if and only if for every pair of memories m_1, m_2 such that $P(m_1, m_2)$ we have:

- 1) $\{c_1\}_{m_1} = \perp$ iff $\{c_2\}_{m_2} = \perp$
- 2) $\{c_1\}_{m_1} = m_1'$ and $\{c_2\}_{m_2} = m_2'$ implies $Q(m_1', m_2')$.

Validity of Hoare quadruple

We say that the quadruple $c_1 \sim c_2 : P \Rightarrow Q$ is **valid** if and only if for every pair of memories m_1, m_2 such that $P(m_1, m_2)$ we have:

- 1) $\{c_1\}_{m_1} = \perp$ iff $\{c_2\}_{m_2} = \perp$
- 2) $\{c_1\}_{m_1} = m_1'$ and $\{c_2\}_{m_2} = m_2'$ implies $Q(m_1', m_2')$.

How do we check this?

Relative Completeness

If a quadruple $C_1 \sim C_2 : P \Rightarrow Q$ is valid, and we have an oracle to derive all the true statements of the form $P \Rightarrow S$ and of the form $R \Rightarrow Q$, then we can derive $\vdash C_1 \sim C_2 : P \Rightarrow Q$ through the rules of the logic.

Soundness and completeness with respect to Hoare Logic

$$\vdash_{\text{RHL}} C_1 \sim C_2 : P \Rightarrow Q$$

iff

$$\vdash_{\text{HL}} C_1; C_2 : P \Rightarrow Q$$

Soundness and completeness with respect to Hoare Logic

$$\vdash_{\text{RHL}} C_1 \sim C_2 : P \Rightarrow Q$$

iff

$$\vdash_{\text{HL}} C_1; C_2 : P \Rightarrow Q$$

Under the assumption that we can partition the memory adequately, and that we have termination.