CS 599: Formal Methods in Security and Privacy

Hoare Triples and Hoare Logic

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu

Specifications - Hoare triple

Precondition
Program
Postcondition

Precondition
(a logical formula)

$$c : P \Rightarrow Q$$

Program

Postcondition
(a logical formula)

Rules of Hoare Logic
Composition

$$\dfrac{}{\vdash \texttt{c;c'}:\ P \Rightarrow Q}$$

Rules of Hoare Logic
Composition

$$\frac{\vdash \texttt{c} : P \Rightarrow R}{\vdash \texttt{c;c'} : \ P \Rightarrow Q}$$

Rules of Hoare Logic
Composition

$$\frac{\vdash c : P \Rightarrow R \qquad \vdash c' : R \Rightarrow Q}{\vdash c;c' : \ P \Rightarrow Q}$$

Rules of Hoare Logic
Composition

$$\frac{\vdash \texttt{c} : P \Rightarrow R \qquad \vdash \texttt{c}' : R \Rightarrow Q}{\vdash \texttt{c;c}' : P \Rightarrow Q}$$

Is this correct?

Some Instances

$$\vdash x := z * 2; z := x * 2$$

$$: \{(z * 2) * 2 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

Some Instances

$$\vdash x := z * 2; z := x * 2$$

$$: \{(z * 2) * 2 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

✓

Some Instances

How can we prove it?

$$\frac{}{\vdash x := z * 2; z := x * 2 : \{(z * 2) * 2 = 8\} \Rightarrow \{z = 8\}}$$

Some Instances

How can we prove it?

$$\dfrac{\dfrac{}{\vdash x := z * 2 : \{(z * 2) * 2 = 8\} \Rightarrow \{x * 2 = 8\}} \qquad \dfrac{}{\vdash z := x * 2 : \{x * 2 = 8\} \Rightarrow \{z = 8\}}}{\vdash x := z * 2; z := x * 2 : \{(z * 2) * 2 = 8\} \Rightarrow \{z = 8\}}$$

Correctness Composition Rule

$$\frac{\vdash \mathtt{c} : \mathtt{P} \Rightarrow \mathtt{R} \qquad \vdash \mathtt{c'} : \mathtt{R} \Rightarrow \mathtt{Q}}{\vdash \mathtt{c;c'} : \mathtt{P} \Rightarrow \mathtt{Q}}$$

To show this rule correct we need to show the validity $\mathtt{c;c'} : \mathtt{P} \Rightarrow \mathtt{Q}$ for every $\mathtt{c}, \mathtt{c'}, \mathtt{P}, \mathtt{Q}$.

Correctness Composition Rule

$$\frac{\vdash c : P \Rightarrow R \qquad \vdash c' : R \Rightarrow Q}{\vdash c;c' : P \Rightarrow Q}$$

To show this rule correct we need to show the validity $c;c' : P \Rightarrow Q$ for every c, c', P, Q.

For every m such that $P(m)$ and m' such that $\{c,c'\}_m = m'$ we need $Q(m')$.

Correctness Composition Rule

$$\frac{\vdash \mathtt{c} : P \Rightarrow R \qquad \vdash \mathtt{c'} : R \Rightarrow Q}{\vdash \mathtt{c;c'} : P \Rightarrow Q}$$

Correctness Composition Rule

$$\frac{\vdash \texttt{c}:P\Rightarrow R \qquad \vdash \texttt{c'}:R\Rightarrow Q}{\vdash \texttt{c;c'}:\ P\Rightarrow Q}$$

By our semantics: $\{\texttt{c;c'}\}_{\texttt{m}}=\texttt{m'}$ if and only if there is $\texttt{m''}$ such that $\{\texttt{c}\}_{\texttt{m}}=\texttt{m''}$ and $\{\texttt{c'}\}_{\texttt{m''}}=\texttt{m'}$.

Correctness Composition Rule

$$\frac{\vdash c : P \Rightarrow R \qquad \vdash c' : R \Rightarrow Q}{\vdash c;c' : \; P \Rightarrow Q}$$

By our semantics: $\{c;c'\}_m = m'$ if and only if there is m'' such that $\{c\}_m = m''$ and $\{c'\}_{m''} = m'$.

Assuming $c : P \Rightarrow R$ and $c' : R \Rightarrow Q$ valid, if $P(m)$ we can show $R(m'')$ and if $R(m'')$ we can show $Q(m')$, hence since we have $P(m)$ we can conclude $Q(m')$.

Correctness Composition Rule

$$\frac{\vdash \texttt{c}:\texttt{P}\Rightarrow\texttt{R} \qquad \vdash \texttt{c'}:\texttt{R}\Rightarrow\texttt{Q}}{\vdash \texttt{c;c'}:\ \texttt{P}\Rightarrow\texttt{Q}}$$

By our semantics: $\{\texttt{c;c'}\}_{\texttt{m}}=\texttt{m'}$ if and only if there is $\texttt{m''}$ such that $\{\texttt{c}\}_{\texttt{m}}=\texttt{m''}$ and $\{\texttt{c'}\}_{\texttt{m''}}=\texttt{m'}$.

Assuming $\texttt{c}:\texttt{P}\Rightarrow\texttt{R}$ and $\texttt{c'}:\texttt{R}\Rightarrow\texttt{Q}$ valid, if $\texttt{P(m)}$ we can show $\texttt{R(m'')}$ and if $\texttt{R(m'')}$ we can show $\texttt{Q(m')}$, hence since we have $\texttt{P(m)}$ we can conclude $\texttt{Q(m')}$. ✓

Some examples

$$\vdash x := z * 2; z := x * 2$$

$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

Some examples

$$\vdash x := z * 2; z := x * 2$$

$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

✓

Some examples

$$\vdash x := z * 2; z := x * 2$$
$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple? ✓

Can we prove it with the rules that we have?

Some examples

$$\vdash x := z * 2; z := x * 2$$

$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?	✓
Can we prove it with the rules that we have?	✗

Some Instances

What is the issue?

$$\vdash x := z * 2; z := x * 2 : \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Some Instances

What is the issue?

$$\frac{}{\vdash x := z * 2 : \{z * 4 = 8\} \Rightarrow \{x * 2 = 8\}} \qquad \frac{}{\vdash z := x * 2 : \{x * 2 = 8\} \Rightarrow \{z = 8\}}$$

$$\vdash x := z * 2; z := x * 2 : \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Some Instances

What is the issue?

$$\dfrac{\dfrac{}{\vdash x := z * 2 : \{z * 4 = 8\} \Rightarrow \{x * 2 = 8\}} \qquad \dfrac{}{\vdash z := x * 2 : \{x * 2 = 8\} \Rightarrow \{z = 8\}}}{\vdash x := z * 2; z := x * 2 : \{z * 4 = 8\} \Rightarrow \{z = 8\}}$$

Rules of Hoare Logic
Consequence

$$\frac{P \Rightarrow S \qquad \vdash c : S \Rightarrow R \qquad R \Rightarrow Q}{\vdash c : \; P \Rightarrow Q}$$

Some examples

$$\vdash x := z * 2; z := x * 2$$

$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

Some examples

$$\vdash x := z * 2; z := x * 2$$

$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

Some examples

$$\vdash x := z * 2; z := x * 2$$

$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple?

✓

Can we prove it with the rules that we have?

Some examples

$$\vdash x := z * 2; z := x * 2$$
$$: \{z * 4 = 8\} \Rightarrow \{z = 8\}$$

Is this a valid triple? ✓

Can we prove it with the rules that we have? ✓

Some Instances

$$\dfrac{\dfrac{\{z*4=8\} \Rightarrow \{(z*2)*2=8\} \qquad \dfrac{}{\vdash x := z*2\ \{(z*2)*2=8\} \Rightarrow \{x*2=8\}}}{\vdash x := z*2\colon \{z*4=8\} \Rightarrow \{x*2=8\}} \qquad \dfrac{}{\vdash z := x*2\colon \{x*2=8\} \Rightarrow \{z=8\}}}{\vdash x := z*2; z := x*2\colon \{z*4=8\} \Rightarrow \{z=8\}}$$

Rules of Hoare Logic
If then else

$$\frac{}{\vdash \texttt{if } e \texttt{ then } c_1 \texttt{ else } c_2 : P \Rightarrow Q}$$

Rules of Hoare Logic
If then else

$$\frac{\vdash c_1 : P \Rightarrow Q \qquad \vdash c_2 : P \Rightarrow Q}{\vdash \texttt{if e then } c_1 \texttt{ else } c_2 \ : \ P \Rightarrow Q}$$

Rules of Hoare Logic
If then else

$$\frac{\vdash c_1 : P \Rightarrow Q \qquad \vdash c_2 : P \Rightarrow Q}{\vdash \texttt{if } e \texttt{ then } c_1 \texttt{ else } c_2 : P \Rightarrow Q}$$

Is this correct?

Some examples

$$\vdash \texttt{if y} = 0 \texttt{ then skip else } x := x + 1; x := x - 1$$

$$: \{x = 1\} \Rightarrow \{x = 1\}$$

Is this a valid triple?

Some examples

$$\vdash \texttt{if y} = 0 \texttt{ then skip else } x := x+1; x := x-1$$
$$: \{x = 1\} \Rightarrow \{x = 1\}$$

Is this a valid triple? ✓

Some examples

$$\vdash \texttt{if } \texttt{y} = 0 \texttt{ then skip else } x := x + 1; x := x - 1$$

$$: \{x = 1\} \Rightarrow \{x = 1\}$$

Is this a valid triple? ✓

Can we prove it with the rules that we have?

Some examples

$$\vdash \texttt{if } \texttt{y} = 0 \texttt{ then skip else } x := x + 1; x := x - 1$$

$$: \{x = 1\} \Rightarrow \{x = 1\}$$

Is this a valid triple? ✓

Can we prove it with the rules that we have? ✓

Some Instances

$$\dfrac{\dfrac{}{\vdash \texttt{skip}: \{x = 1\} \Rightarrow \{x = 1\}} \qquad \dfrac{\vdots}{\vdash x := x + 1; x := x - 1 : \{x = 1\} \Rightarrow \{x = 1\}}}{\vdash \texttt{if } \texttt{y} = \texttt{0} \texttt{ then skip else } x := x + 1; x := x - 1 \quad : \{x = 1\} \Rightarrow \{x = 1\}}$$

Rules of Hoare Logic
If then else

$$\frac{\vdash c_1 : P \Rightarrow Q \qquad\qquad \vdash c_2 : P \Rightarrow Q}{\vdash \texttt{if e then } c_1 \texttt{ else } c_2 \texttt{ : } P \Rightarrow Q}$$

Rules of Hoare Logic
If then else

$$\frac{\vdash c_1 : P \Rightarrow Q \qquad\qquad \vdash c_2 : P \Rightarrow Q}{\vdash \texttt{if e then } c_1 \texttt{ else } c_2 : P \Rightarrow Q}$$

Is this strong enough?

Some examples

$$\vdash \texttt{if false then skip else } x = x + 1$$

$$: \{x = 0\} \Rightarrow \{x = 1\}$$

Is this a valid triple?

Some examples

$$\vdash \texttt{if false then skip else } x = x + 1$$
$$: \{x = 0\} \Rightarrow \{x = 1\}$$

Is this a valid triple?

✓

Some examples

$$\vdash \texttt{if false then skip else } x = x + 1$$
$$: \{x = 0\} \Rightarrow \{x = 1\}$$

Is this a valid triple? ✓

Can we prove it with the rules that we have?

Some examples

$$\vdash \texttt{if false then skip else } x = x + 1$$
$$: \{x = 0\} \Rightarrow \{x = 1\}$$

Is this a valid triple? ✓

Can we prove it with the rules that we have? ✗

Rules of Hoare Logic
If then else

$$\frac{\vdash c_1 : e \wedge P \Rightarrow Q \qquad \vdash c_2 : \neg e \wedge P \Rightarrow Q}{\vdash \texttt{if } e \texttt{ then } c_1 \texttt{ else } c_2 : P \Rightarrow Q}$$

Is this correct?

Rules of Hoare Logic
If then else

$$\frac{\vdash c_1 : e \wedge P \Rightarrow Q \qquad \vdash c_2 : \neg e \wedge P \Rightarrow Q}{\vdash \texttt{if } e \texttt{ then } c_1 \texttt{ else } c_2 : P \Rightarrow Q}$$

Is this correct?

Homework

Rules of Hoare Logic: Abort

$$\frac{}{\vdash \texttt{Abort: } ? \Rightarrow ?}$$

Rules of Hoare Logic: Abort

$$\frac{}{\vdash \texttt{Abort:}\ ? \Rightarrow ?}$$

What can be a good specification?

Validity of Hoare triple

We say that the triple $c : P \Rightarrow Q$ is valid

if and only if

for every memory m such that $P(m)$

and memory m’ such that $\{c\}_m = m'$

we have $Q(m')$.

Rules of Hoare Logic: Abort

$$\frac{}{\vdash \texttt{Abort} : P \Rightarrow Q}$$

Rules of Hoare Logic: Abort

$$\vdash \texttt{Abort:P} \Rightarrow \texttt{Q}$$

To show this rule correct we need to show the validity $\texttt{Abort:P} \Rightarrow \texttt{Q}$ for every $\texttt{P}$, $\texttt{Q}$.

Rules of Hoare Logic: Abort

$$\vdash \texttt{Abort}:\texttt{P}\Rightarrow\texttt{Q}$$

To show this rule correct we need to show the validity $\texttt{Abort}:\texttt{P}\Rightarrow\texttt{Q}$ for every $\texttt{P},\texttt{Q}$.

For every $\texttt{m}$ such that $\texttt{P(m)}$ and m' such that $\{\texttt{Abort}\}_{\texttt{m}}=\texttt{m}'$ we need Q$\texttt{(m')}$.

Rules of Hoare Logic: Abort

$$\vdash \texttt{Abort:P} \Rightarrow \texttt{Q}$$

To show this rule correct we need to show the validity $\texttt{Abort:P} \Rightarrow \texttt{Q}$ for every $\texttt{P,Q}$.

For every $\texttt{m}$ such that $\texttt{P(m)}$ and m' such that $\{\texttt{Abort}\}_{\texttt{m}} = \texttt{m}'$ we need Q$\texttt{(m')}$.

Vacuously True

Rules of Hoare Logic
While

```
⊢while e do c : ??
```

Rules of Hoare Logic
While

$$\frac{P \Rightarrow \neg e}{\vdash \texttt{while e do c} : P \Rightarrow P}$$

Rules of Hoare Logic
While

$$\frac{P \Rightarrow e \qquad\qquad \vdash c : P \Rightarrow P}{\vdash \texttt{while e do c} : P \Rightarrow P}$$

Rules of Hoare Logic
While

$$\frac{\vdash c : e \wedge P \Rightarrow P}{\vdash \texttt{while } e \texttt{ do } c : P \Rightarrow P \wedge \neg e}$$

Invariant

An example

$$\vdash \texttt{while } x = 0 \texttt{ do } x := x + 1 \; : \{x = 1\} \Rightarrow \{x = 1\}$$

How can we derive this?

An example

$$\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1$$
$$: \{x = 1\} \Rightarrow \{x = 1\}$$

What can be a good Invariant?

An example

$$\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1$$
$$: \{x = 1\} \Rightarrow \{x = 1\}$$

What can be a good Invariant?

$$Inv = \{x = 1\}$$

An example

$$\frac{}{\vdash \texttt{while } x = 0 \texttt{ do } x := x + 1 : \{x = 1\} \Rightarrow \{x = 1\}}$$

An example

$$\frac{\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1 \colon \{x = 1\} \Rightarrow \{x = 1 \wedge x \neq 0\} \qquad x = 1 \wedge x \neq 0 \Rightarrow x = 1}{\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1 \colon \{x = 1\} \Rightarrow \{x = 1\}}$$

An example

$$\dfrac{\dfrac{x = 1 \wedge x = 0 \Rightarrow x + 1 = 1 \qquad \vdash x := x + 1 : \{x + 1 = 1\} \Rightarrow \{x = 1\}}{\vdash x := x + 1 : \{x = 1 \wedge x = 0\} \Rightarrow \{x = 1\}}}{\dfrac{\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1 : \{x = 1\} \Rightarrow \{x = 1 \wedge x \neq 0\} \qquad x = 1 \wedge x \neq 0 \Rightarrow x = 1}{\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1 : \{x = 1\} \Rightarrow \{x = 1\}}}$$

An example

$$\frac{\dfrac{x = 1 \wedge x = 0 \Rightarrow x + 1 = 1 \qquad \vdash x := x + 1 : \{x + 1 = 1\} \Rightarrow \{x = 1\}}{\vdash x := x + 1 : \{x = 1 \wedge x = 0\} \Rightarrow \{x = 1\}}}{\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1 : \{x = 1\} \Rightarrow \{x = 1 \wedge x \neq 0\}} \qquad x = 1 \wedge x \neq 0 \Rightarrow x = 1$$

$$\vdash \texttt{while}\ x = 0\ \texttt{do}\ x := x + 1 : \{x = 1\} \Rightarrow \{x = 1\}$$

Another example

$\vdash$

```
x:=3;
y:=1;
while x > 1 do
  y := y+1;
  x := x-1;
```

$: \{true\} \Rightarrow \{y = 3\}$

How can we derive this?

Another example

$\vdash$

```
x:=3;
y:=1;
while x > 1 do
  y := y+1;
  x := x-1;
```

$: \{true\} \Rightarrow \{y = 3\}$

What can be a good Invariant?

Another example

$\vdash$

```
x:=3;
y:=1;
while x > 1 do
  y := y+1;
  x := x-1;
```

$: \{true\} \Rightarrow \{y = 3\}$

What can be a good Invariant?

$\mathtt{Inv} = \{y = 4 - x \wedge x \geq 1\}$

How do we know that these are the right rules?

Soundness

If we can derive $\vdash \texttt{c : P} \Rightarrow \texttt{Q}$ through the rules of the logic, then the triple $\texttt{c : P} \Rightarrow \texttt{Q}$ is valid.

Are the rules we presented sound?

Completeness

If a triple $\texttt{c} : \texttt{P} \Rightarrow \texttt{Q}$ is valid, then we can derive $\vdash \texttt{c} : \texttt{P} \Rightarrow \texttt{Q}$ through the rules of the logic.

Are the rules we presented complete?

Relative Completeness

$$\frac{P \Rightarrow S \qquad \vdash c : S \Rightarrow R \qquad R \Rightarrow Q}{\vdash c : \; P \Rightarrow Q}$$

Relative Completeness

$$\frac{P \Rightarrow S \qquad \vdash c : S \Rightarrow R \qquad R \Rightarrow Q}{\vdash c : \ P \Rightarrow Q}$$

If a triple $c : Pre \Rightarrow Post$ is valid, and we have an oracle to derive all the true statements of the form $P \Rightarrow S$ and of the form $R \Rightarrow Q$,which we can use in applications of the conseq rule, then we can derive $\vdash c : Pre \Rightarrow Post$ through the rules of the logic.