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

$c : P \Rightarrow Q$

Precondition (a logical formula)
Program
Postcondition (a logical formula)
Rules of Hoare Logic
Composition

\[ \vdash c; c' : P \Rightarrow Q \]
Rules of Hoare Logic
Composition

\[ \vdash c : P \Rightarrow R \]

\[ \vdash c ; c' : P \Rightarrow Q \]
Rules of Hoare Logic Composition

\[
\frac{\vdash c : P \Rightarrow R \quad \vdash c' : R \Rightarrow Q}{\vdash c ; c' : P \Rightarrow Q}
\]
Is this correct?
Some Instances

\[ \vdash x := z \cdot 2; z := x \cdot 2 \]

\[ \therefore \{ (z \cdot 2) \cdot 2 = 8 \} \Rightarrow \{ z = 8 \} \]

Is this a valid triple?
Some Instances

\[ \vdash x := z \times 2; \ z := x \times 2 \]

\[ \{ \left( z \times 2 \right) \times 2 = 8 \} \Rightarrow \{ z = 8 \} \]

Is this a valid triple? ✓
Some Instances

How can we prove it?

\[ \vdash x := z \ast 2; z := x \ast 2 : \{(z \ast 2) \ast 2 = 8\} \Rightarrow \{z = 8\} \]
Some Instances

How can we prove it?

\[ \vdash x := z \cdot 2 : \{(z \cdot 2) \cdot 2 = 8\} \Rightarrow \{x \cdot 2 = 8\} \]

\[ \vdash z := x \cdot 2 : \{x \cdot 2 = 8\} \Rightarrow \{z = 8\} \]

\[ \vdash x := z \cdot 2 ; z := x \cdot 2 : \{(z \cdot 2) \cdot 2 = 8\} \Rightarrow \{z = 8\} \]
Correctness Composition Rule

\[
\begin{array}{c}
\vdash c : P \Rightarrow R \\
\vdash c' : R \Rightarrow Q \\
\hline
\vdash c ; c' : P \Rightarrow Q 
\end{array}
\]

To show this rule correct we need to show the validity \( c ; c' : P \Rightarrow Q \) for every \( c, c', P, Q \).
Correctness Composition Rule

\[
\frac{\Gamma \vdash c : P \Rightarrow R \quad \Gamma \vdash c' : R \Rightarrow Q}{\Gamma \vdash c; c' : P \Rightarrow Q}
\]

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

\[ \vdash c : P \Rightarrow R \quad \vdash c' : R \Rightarrow Q \]

\[ \vdash c ; c' : P \Rightarrow Q \]
Correctness Composition Rule

\[ \frac{\vdash c : P \Rightarrow R \quad \vdash c' : R \Rightarrow Q}{\vdash c ; c' : P \Rightarrow Q} \]

By our semantics: \( \{ c ; c' \} _m = m' \) if and only if there is \( m'' \) such that \( \{ c \} _m = m'' \) and \( \{ c' \} _{m''} = m' \).
Correctness Composition Rule

\[ \frac{\vdash c : P \Rightarrow R \quad \vdash c' : R \Rightarrow Q}{\vdash c ; c' : P \Rightarrow Q} \]

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

\[ \frac{\vdash c : P \Rightarrow R \quad \vdash c' : R \Rightarrow Q}{\vdash c ; c' : P \Rightarrow Q} \]

By our semantics: \( \{c ; c'\} \equiv m = m' \) if and only if there is \( m'' \) such that \( \{c\} = m'' \) 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 \( Q(m') \).
Some examples

⊢ \( x := z \times 2; z := x \times 2 \)

: \( \{ z \times 4 = 8 \} \Rightarrow \{ z = 8 \} \)

Is this a valid triple?
Some examples

\[ \vdash x := z * 2 ; z := x * 2 \]
\[ : \quad \{ z * 4 = 8 \} \Rightarrow \{ z = 8 \} \]

Is this a valid triple? ✓
Some examples

\[\vdash x := z \times 2; z := x \times 2\]

\[\vdash z \times 4 = 8 \Rightarrow \{z = 8\}\]

Is this a valid triple?  

Can we prove it with the rules that we have?

✓
Some examples

\[
\Gamma \vdash x := z \times 2; \; z := x \times 2
\]

\[
: \{z \times 4 = 8\} \Rightarrow \{z = 8\}
\]

Is this a valid triple?  

✓

Can we prove it with the rules that we have?  

✗
Some Instances

⊢ $x := z \cdot 2; z := x \cdot 2 : \{z \cdot 4 = 8\} \Rightarrow \{z = 8\}$

What is the issue?
Some Instances

What is the issue?

\[\vdash x := z * 2 : \{z * 4 = 8\} \Rightarrow \{x * 2 = 8\}\]

\[\vdash z := x * 2 : \{x * 2 = 8\} \Rightarrow \{z = 8\}\]

\[\vdash x := z * 2; z := x * 2 : \{z * 4 = 8\} \Rightarrow \{z = 8\}\]
Some Instances

What is the issue?

\[ \vdash x := z \ast 2 : \{ z \ast 4 = 8 \} \Rightarrow \{ x \ast 2 = 8 \} \]
\[ \vdash z := x \ast 2 : \{ x \ast 2 = 8 \} \Rightarrow \{ z = 8 \} \]
\[ \vdash x := z \ast 2; z := x \ast 2 : \{ z \ast 4 = 8 \} \Rightarrow \{ z = 8 \} \]
Rules of Hoare Logic

Consequence

\[ \frac{P \Rightarrow S \quad \Gamma \vdash c : S \Rightarrow R \quad R \Rightarrow Q}{\Gamma \vdash c : P \Rightarrow Q} \]
Some examples

\[ \vdash x := z \times 2; z := x \times 2 \]

\[ : \{ z \times 4 = 8 \} \implies \{ z = 8 \} \]

Is this a valid triple?
Some examples

\[ \vdash x \leftarrow z \cdot 2 ; z \leftarrow x \cdot 2 \]

\[ : \{ z \cdot 4 = 8 \} \Rightarrow \{ z = 8 \} \]

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

⊢ $x := z * 2; z := x * 2$

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

Is this a valid triple? ✓

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

\[ \vdash x := z \cdot 2 \{ (z \cdot 2)^2 = 8 \} \Rightarrow \{ x \cdot 2 = 8 \} \]

\[ \{ z \cdot 4 = 8 \} \Rightarrow \{ (z \cdot 2)^2 = 8 \} \]

\[ \vdash x := z \cdot 2 : \{ z \cdot 4 = 8 \} \Rightarrow \{ x \cdot 2 = 8 \} \quad \vdash z := x \cdot 2 : \{ x \cdot 2 = 8 \} \Rightarrow \{ z = 8 \} \]

\[ \vdash x := z \cdot 2 ; z := x \cdot 2 : \{ z \cdot 4 = 8 \} \Rightarrow \{ z = 8 \} \]
Rules of Hoare Logic

If then else

\[ \vdash \text{if } e \text{ then } c_1 \text{ else } c_2 : P \Rightarrow Q \]
Rules of Hoare Logic
If then else

\[
\begin{align*}
\vdash c_1 : P \Rightarrow Q & \quad \vdash c_2 : P \Rightarrow Q \\
\hline
\vdash \text{if } e \text{ then } c_1 \text{ else } c_2 : P \Rightarrow Q
\end{align*}
\]
Rules of Hoare Logic
If then else

\[
\begin{align*}
\vdash c_1 : P \Rightarrow Q \\
\vdash c_2 : P \Rightarrow Q
\end{align*}
\]

\[
\vdash \text{if } e \text{ then } c_1 \text{ else } c_2 : P \Rightarrow Q
\]

Is this correct?
Some examples

\[
\begin{align*}
\text{⊢ if } y = 0 \text{ then skip else } & x := x + 1; x := x - 1 \\
& : \{x = 1\} \Rightarrow \{x = 1\}
\end{align*}
\]

Is this a valid triple?
Some examples

⊢ if y = 0 then skip else x := x + 1; x := x - 1

: {x = 1} ⇒ {x = 1}

Is this a valid triple? ✓
Some examples

⊢ if y = 0 then skip else x := x + 1; x := x − 1
     : {x = 1} ⇒ {x = 1}

Is this a valid triple?

Can we prove it with the rules that we have?
Some examples

⊢ if y = 0 then skip else x := x + 1; x := x − 1

: {x = 1} ⇒ {x = 1}

Is this a valid triple? ✓

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

⊢ \text{skip}: \{ x = 1 \} \Rightarrow \{ x = 1 \} \quad \vdash x := x + 1; x := x - 1 : \{ x = 1 \} \Rightarrow \{ x = 1 \}

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

: \{ x = 1 \} \Rightarrow \{ x = 1 \}
Rules of Hoare Logic
If then else

\[ \vdash c_1 : P \Rightarrow Q \quad \vdash c_2 : P \Rightarrow Q \]

\[ \vdash \text{if } e \text{ then } c_1 \text{ else } c_2 : P \Rightarrow Q \]
Rules of Hoare Logic
If then else

\[ \vdash c_1 : P \Rightarrow Q \quad \vdash c_2 : P \Rightarrow Q \]

\[ \vdash \text{if } e \text{ then } c_1 \text{ else } c_2 : P \Rightarrow Q \]

Is this strong enough?
Some examples

⊢ if false then skip else \( x = x + 1 \)

: \( \{ x = 0 \} \Rightarrow \{ x = 1 \} \)

Is this a valid triple?
Some examples

⊢ if false then skip else $x = x + 1$

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

Is this a valid triple? ✓
Some examples

⊢ 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

\[ \vdash \text{if false then skip else } x = x + 1 \]
\[ : \{x = 0\} \Rightarrow \{x = 1\} \]

Is this a valid triple?  

Can we prove it with the rules that we have?

✓  

✗
Rules of Hoare Logic
If then else

\[ \vdash if \; e \; then \; c_1 \; else \; c_2 : \; P \Rightarrow Q \]

Is this correct?
Rules of Hoare Logic
If then else

\[ \begin{align*}
\vdash c_1 &: e \land P \Rightarrow Q \\
\vdash c_2 &: \neg e \land P \Rightarrow Q
\end{align*} \]

\[ \vdash \text{if } e \text{ then } c_1 \text{ else } c_2 : P \Rightarrow Q \]

Is this correct?

Homework
Rules of Hoare Logic: Abort

\[ \vdash Abort: \ ? \Rightarrow \ ? \]
Rules of Hoare Logic: Abort

⊢ Abort: ?⇒? 

What can be a good specification?
Validity of Hoare triple
We say that the triple $c : P \implies Q$ 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:

\[ \text{Abort} \]

\[ \vdash \text{Abort} : P \Rightarrow Q \]
Rules of Hoare Logic:

Abort

\[ \vdash \text{Abort} : P \Rightarrow Q \]

To show this rule correct we need to show the validity \( \text{Abort} : P \Rightarrow Q \) for every \( P, Q \).
Rules of Hoare Logic: Abort

\[ \vdash \text{Abort} : P \Rightarrow Q \]

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

For every \( m \) such that \( P(m) \) and \( m' \) such that \( \{ \text{Abort} \}_{m=m'} \) we need \( Q(m') \).
Rules of Hoare Logic: Abort

\[ \vdash \text{Abort} : P \Rightarrow Q \]

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

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

Vacuously True
Rules of Hoare Logic
While

\[ \vdash \text{while } e \text{ do } c : ?? \]
Rules of Hoare Logic

While

\[ \Gamma \vdash \text{while } e \text{ do } c : P \Rightarrow P \]
Rules of Hoare Logic

While

\[ P \Rightarrow e \quad \vdash \neg c : P \Rightarrow P \]

\[ \vdash \text{while e do c} : P \Rightarrow P \]
Rules of Hoare Logic

While

\[\vdash \text{while } e \text{ do } c : P \Rightarrow P\]

\[\vdash c : e \land P \Rightarrow P\]

\[\vdash \text{while } e \text{ do } c : P \Rightarrow P \land \neg e\]

Invariant
An example

\[ \text{\texttt{while} } x = 0 \text{ do } x := x + 1 \Rightarrow \{x = 1\} \Rightarrow \{x = 1\} \]

How can we derive this?
An example

\[ \vdash \text{while } x = 0 \text{ do } x := x + 1 \]
\[ : \{ x = 1 \} \Rightarrow \{ x = 1 \} \]

What can be a good Invariant?
An example

\[ \text{while } x = 0 \text{ do } x := x + 1 \Rightarrow \{ x = 1 \} \]

What can be a good Invariant?

\[ Inv = \{ x = 1 \} \]
An example

⊢ while \( x = 0 \) do \( x := x + 1 \): \{x = 1\} ⇒ \{x = 1\}
An example

\[\text{\textbf{\# Example \#}}\]

\[\vdash \text{while } x = 0 \text{ do } x := x + 1: \{x = 1\} \Rightarrow \{x = 1 \land x \neq 0\} \quad x = 1 \land x \neq 0 \Rightarrow x = 1\]

\[\vdash \text{while } x = 0 \text{ do } x := x + 1: \{x = 1\} \Rightarrow \{x = 1\}\]
An example

\[ x = 1 \land x = 0 \Rightarrow x + 1 = 1 \]

\[ \vdash x := x + 1 : \{x + 1 = 1\} \Rightarrow \{x = 1\} \]

\[ \vdash x := x + 1 : \{x = 1 \land x = 0\} \Rightarrow \{x = 1\} \]

\[ \vdash \text{while } x = 0 \text{ do } x := x + 1 : \{x = 1\} \Rightarrow \{x = 1 \land x \neq 0\} \quad x = 1 \land x \neq 0 \Rightarrow x = 1 \]

\[ \vdash \text{while } x = 0 \text{ do } x := x + 1 : \{x = 1\} \Rightarrow \{x = 1\} \]
An example

\[ x = 1 \land x = 0 \Rightarrow x + 1 = 1 \]

\[ \vdash x := x + 1 : \{ x + 1 = 1 \} \Rightarrow \{ x = 1 \} \]

\[ \vdash x := x + 1 : \{ x = 1 \} \land x = 0 \Rightarrow \{ x = 1 \} \]

\[ \vdash \text{while } x = 0 \text{ do } x := x + 1 : \{ x = 1 \} \Rightarrow \{ x = 1 \land x \neq 0 \} \quad x = 1 \land x \neq 0 \Rightarrow x = 1 \]

\[ \vdash \text{while } x = 0 \text{ do } x := x + 1 : \{ x = 1 \} \Rightarrow \{ x = 1 \} \]
Another example

\[
\begin{align*}
x &:= 3; \\
y &:= 1; \\
\text{while } x > 1 \text{ do} & \\
& \quad y := y + 1; \\
x &:= x - 1;
\end{align*}
\]

\[\vdash \{ true \} \Rightarrow \{ y = 3 \}\]

How can we derive this?
Another example

\[ x := 3; \]
\[ y := 1; \]
\[ \text{while } x > 1 \text{ do} \]
\[ y := y + 1; \]
\[ x := x - 1; \]

\[ : \{\text{true}\} \Rightarrow \{y = 3\} \]

What can be a good Invariant?
Another example

\begin{verbatim}
x:=3;
y:=1;
while x > 1 do
  y := y+1;
  x := x-1;
\end{verbatim}

\[\vdash \{ true \} \Rightarrow \{ y = 3 \}\]

What can be a good Invariant?

\[\text{Inv} = \{ y = 4 - x \land x \geq 1 \}\]
How do we know that these are the right rules?
If we can derive $\vdash c : P \Rightarrow Q$ through the rules of the logic, then the triple $c : P \Rightarrow Q$ is valid.
Are the rules we presented sound?
Completeness

If a triple $c : P \Rightarrow Q$ is valid, then we can derive $\vdash c : P \Rightarrow Q$ through the rules of the logic.
Are the rules we presented complete?
Relative Completeness

P ⇒ S

⊢ c : S ⇒ R

R ⇒ Q

⊢ c : P ⇒ Q
Relative Completeness

\[ \begin{align*}
& P \Rightarrow S && \vdash c : S \Rightarrow R && R \Rightarrow Q \\
\hline
& \vdash c : P \Rightarrow Q
\end{align*} \]

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.