CS 511: Formal Methods in Security and Privacy

Hoare Triples and Hoare Logic

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu

Programming Language

```
c::= abort
   | skip
   | x:=e
   | c;c
   | if e then c else c
   | while e do c
```

$x, y, z, \ldots$ program variables

$e_1, e_2, \ldots$ expressions

$c_1, c_2, \ldots$ commands

Specifications - Hoare triple

Precondition
(a logical formula)

```
Precondition
Program
Postcondition
```

$$c : P \Rrightarrow Q$$

Program

Postcondition
(a logical formula)

Some examples

```
i:=0;
r:=1;
while(i≤k)do
 r:=r * n;
 i:=i + 1
```

Precondition

$$: \{0 \leq k\} \Rightarrow \{r = n^k\}$$

Postcondition

Is it a good specification?

Some examples

```
i:=0;
r:=1;
while(i≤k)do
  r:=r * n;
  i:=i + 1
```

Precondition

$$: \{0 \leq k\} \Rightarrow \{r = n^k\}$$

Postcondition

Is it a good specification?

✗

Some examples

```
i:=0;
r:=1;
while(i≤k)do
  r:=r * n;
  i:=i + 1
```

Precondition

$$: \{0 \le k\} \Rightarrow \{r = n^k\}$$

Postcondition

Is it a good specification?

$$m_{in} = [k = 0, n = 2, i = 0, r = 0]$$

$$m_{out} = [k = 0, n = 2, i = 1, r = 2]$$

Some examples

Precondition

$$x := z + 1 : \{z + 1 > 0\} \Rightarrow \{x > 0\}$$

Postcondition

Is it a good specification?

Some examples

Precondition

$$x := z + 1 : \{z + 1 > 0\} \Rightarrow \{x > 0\}$$

Postcondition

Is it a good specification?

✓

How do we determine the validity of an Hoare triple?

Validity of Hoare triple

Precondition
(a logical formula)

$$c : P \Rightarrow Q$$

Program

Postcondition
(a logical formula)

Validity of Hoare triple

Precondition
(a logical formula)

$$c : P \Rightarrow Q$$

Program

Postcondition
(a logical formula)

We are interested only in inputs that meets P and we want to have outputs satisfying Q.

Validity of Hoare triple

Precondition
(a logical formula)

$$c : P \Rightarrow Q$$

Program

Postcondition
(a logical formula)

We are interested only in inputs that meets P and we want to have outputs satisfying Q.

How shall we formalize this intuition?

Validity of Hoare triple

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

if and only if

for every memory $\mathtt{m}$ such that $\mathtt{P(m)}$

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

we have $\mathtt{Q(m')}$.

Validity of Hoare triple

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

if and only if

for every memory $\mathtt{m}$ such that $\mathtt{P(m)}$

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

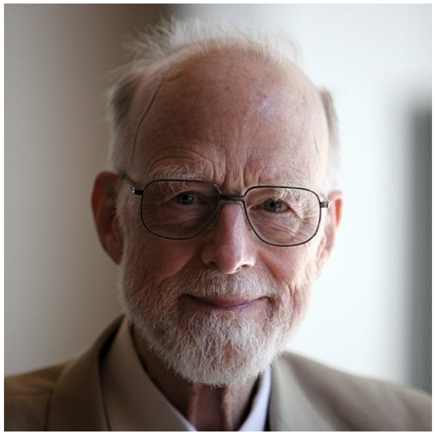
we have $\mathtt{Q(m')}$.

Is this condition easy to check?

Hoare Logic

Floyd-Hoare reasoning

Robert W Floyd



Tony Hoare

A *verification* of an interpretation of a flowchart is a proof that for every command c of the flowchart, if control should enter the command by an entrance a_i with P_i true, then control must leave the command, if at all, by an exit b_j with Q_j true. *A semantic definition* of a particular set of command types, then, is a rule for constructing, for any command c of one of these types, a *verification condition* $V_c(\mathbf{P}; \mathbf{Q})$ on the antecedents and consequents of c. This verification condition must be so constructed that a proof that the verification condition is satisfied for the antecedents and consequents of each command in a flowchart is a verification of the interpreted flowchart.

Rules of Hoare Logic: Skip

$$\frac{}{\vdash \texttt{skip}:\ P \Rightarrow P}$$

Rules of Hoare Logic: Skip

$$\frac{}{\vdash \texttt{skip}: \; P \Rightarrow P}$$

Is this correct?

Correctness of an axiom

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

We say that an axiom is correct if we can prove the validity of each triple which is an instance of the conclusion.

Correctness of Skip Rule

$$\frac{}{\vdash \texttt{skip: } P \Rightarrow P}$$

To show this rule correct we need to show the validity of the triple `skip: P⇒P`.

Correctness of Skip Rule

$$\overline{\vdash \texttt{skip: } P \Rightarrow P}$$

To show this rule correct we need to show the validity of the triple `skip: P⇒P`.

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

Correctness of Skip Rule

$$\overline{\vdash \texttt{skip: } P \Rightarrow P}$$

To show this rule correct we need to show the validity of the triple `skip: P⇒P`.

For every `m` such that `P(m)` and m' such that $\{\texttt{skip}\}_m = m'$ we need `P(m')`.

Follow easily by our semantics:

$\{\texttt{skip}\}_m = m$

Rules of Hoare Logic: Assignment

$$\frac{}{\vdash \texttt{x:=e: } P \Rightarrow P[e/x]}$$

Rules of Hoare Logic: Assignment

$$\frac{}{\vdash \texttt{x:=e:}\quad \texttt{P} \Rightarrow \texttt{P[e/x]}}$$

Is this correct?

Some instances

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

Is this a valid triple?

Some instances

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

Is this a valid triple? ✗

Some instances

$$x := z + 1 : \{x > 0\} \Rightarrow \{z + 1 > 0\}$$

Is this a valid triple?

Some instances

$$x := z + 1 : \{x > 0\} \Rightarrow \{z + 1 > 0\}$$

Is this a valid triple? ✗

Rules of Hoare Logic: Assignment

$$\frac{}{\vdash \texttt{x:=e} \ : \ \texttt{P[e/x]} \Rightarrow \texttt{P}}$$

Rules of Hoare Logic: Assignment

$$\frac{}{\vdash \texttt{x:=e} \;:\; \texttt{P[e/x]} \Rightarrow \texttt{P}}$$

Is this correct?

Some instances

$$x := z + 1 : \{z + 1 > 0\} \Rightarrow \{x > 0\}$$

Is this a valid triple?

Some instances

$$x := z + 1 : \{z + 1 > 0\} \Rightarrow \{x > 0\}$$

$\boxed{\text{Is this a valid triple?}}$ ✓

Some instances

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

Is this a valid triple?

Some instances

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

Is this a valid triple? ✓

Correctness Assignment Rule

$$\frac{}{\vdash \texttt{x:=e} \ : \ \texttt{P[e/x]} \Rightarrow \texttt{P}}$$

To show this rule correct we need to show the validity $\texttt{x:=e:P[e/x]} \Rightarrow \texttt{P}$ for every $\texttt{x}$, $\texttt{e}$, $\texttt{P}$.

Correctness Assignment Rule

$$\frac{}{\vdash \texttt{x:=e} \ : \ \texttt{P[e/x]} \Rightarrow \texttt{P}}$$

To show this rule correct we need to show the validity $\texttt{x:=e:P[e/x]} \Rightarrow \texttt{P}$ for every $\texttt{x}$, $\texttt{e}$, $\texttt{P}$.

For every $\texttt{m}$ such that $\texttt{P[e/x](m)}$ and m' such that $\texttt{\{x:=e\}}_{\texttt{m}}\texttt{=m'}$ we need $\texttt{P(m')}$.

Correctness Assignment Rule

$$\frac{}{\vdash \mathtt{x:=e} \; : \; \mathtt{P[e/x]} \Rightarrow \mathtt{P}}$$

To show this rule correct we need to show the validity $\mathtt{x:=e:P[e/x]} \Rightarrow \mathtt{P}$ for every $\mathtt{x, e, P}$.

For every $\mathtt{m}$ such that $\mathtt{P[e/x](m)}$ and m' such that $\mathtt{\{x:=e\}_m=m'}$ we need $\mathtt{P(m')}$.

By our semantics: $\mathtt{\{x:=e\}_m=m[x=\{e\}_m]}$ and we can show $\mathtt{P[e/x](m)= P(m[x=\{e\}_m])}$

Rules of Hoare Logic
Composition

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

Rules of Hoare Logic
Composition

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

Rules of Hoare Logic
Composition

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

Rules of Hoare Logic
Composition

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

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

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

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

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

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

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

Correctness Composition Rule

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

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

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

By our semantics: $\{c;c'\}_m = m'$ 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

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

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?

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

Some Instances

What is the issue?

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

Some Instances

What is the issue?

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

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

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

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

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

$$\frac{\vdash \mathtt{c}_1 : \mathtt{P} \Rightarrow \mathtt{Q} \qquad \vdash \mathtt{c}_2 : \mathtt{P} \Rightarrow \mathtt{Q}}{\vdash \mathtt{if\ e\ then\ c}_1\ \mathtt{else\ c}_2 : \mathtt{P} \Rightarrow \mathtt{Q}}$$

Rules of Hoare Logic
If then else

$$\frac{\vdash \mathtt{c}_1 : \mathtt{P} \Rightarrow \mathtt{Q} \qquad\qquad \vdash \mathtt{c}_2 : \mathtt{P} \Rightarrow \mathtt{Q}}{\vdash \mathtt{if\ e\ then\ c_1\ else\ c_2\ :\ P} \Rightarrow \mathtt{Q}}$$

Is this correct?

Some examples

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

$\boxed{\text{Is this a valid triple?}}$

Some examples

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

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

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? ✓

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

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

Rules of Hoare Logic
If then else

$$\frac{\vdash \mathtt{c}_1 : \mathtt{P} \Rightarrow \mathtt{Q} \qquad \vdash \mathtt{c}_2 : \mathtt{P} \Rightarrow \mathtt{Q}}{\vdash \mathtt{if\ e\ then\ c}_1\ \mathtt{else\ c}_2 : \mathtt{P} \Rightarrow \mathtt{Q}}$$

Rules of Hoare Logic
If then else

$$\frac{\vdash \texttt{c}_1 : P \Rightarrow Q \qquad\qquad \vdash \texttt{c}_2 : P \Rightarrow Q}{\vdash \texttt{if e then c}_1 \texttt{ else c}_2 : P \Rightarrow Q}$$

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

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

$\boxed{\text{Is this a valid triple?}}$ ✓

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?