CS 591: Formal Methods in Security and Privacy

More Hoare Logic

Marco Gaboardi
gaboardi@bu.edu

Alley Stoughton
stough@bu.edu

From the previous classes

Specifications - Hoare triple

Precondition
(a logical formula)

Precondition
Program
Postcondition

$$c : P \Rightarrow Q$$

Program

Postcondition
(a logical formula)

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 $Q(m')$.

Is this condition easy to check?

Rules of Hoare Logic: Skip

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

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.

Rules of Hoare Logic: Assignment

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

Today: more rules

Rules of Hoare Logic
Composition

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

Rules of Hoare Logic
Composition

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

Is this correct?

An Instance

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

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

Is this a valid triple?

An Instance

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

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

Is this a valid triple? ✓

An Instance

How can we prove it?

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

An Instance

How can we prove it?

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

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

Correctness of a rule

$$\frac{\vdash c_1 : P_1 \Rightarrow Q_1 \qquad \ldots \qquad \vdash c_n : P_n \Rightarrow Q_n}{\vdash c \; : \; P \; \Rightarrow \; Q}$$

We say that a rule is correct if given valid triples as described by the assumption(s), we can prove the validity of the triple in the conclusion.

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

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

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

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

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

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

By our semantics: $\{\texttt{c};\texttt{c}'\}_{\texttt{m}}=\texttt{m}'$ 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 $\texttt{P}(\texttt{m})$ we can show $\texttt{R}(\texttt{m}'')$ and if $\texttt{R}(\texttt{m}'')$ we can show $\texttt{Q}(\texttt{m}')$, hence since we have $\texttt{P}(\texttt{m})$ we can conclude $\texttt{Q}(\texttt{m}')$.

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: $\{\texttt{c;c'}\}_{\texttt{m}}=\texttt{m'}$ 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 $\texttt{Q(m')}$. ✓

An example

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

Is this a valid triple?

An example

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

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

Is this a valid triple? ✓

An example

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

Is this a valid triple? ✓

Can we prove it with the rules that we have?

An example

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

Is this a valid triple? ✓

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

An Instance

What is the issue?

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

An Instance

What is the issue?

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

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

An Instance

What is the issue?

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

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

Rules of Hoare Logic
Consequence

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

We can weaken P, i.e. replace it by something that is implied by P. In this case S.

We can strengthen Q, i.e. replace it by something that implies Q. In this case R.

An example

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

Is this a valid triple?

An example

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

Is this a valid triple? ✓

An example

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

Is this a valid triple? ✓

Can we prove it with the rules that we have?

An example

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

Is this a valid triple? ✓

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

An Instance

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

$$\{z * 4 = 8\} \Rightarrow \{(z * 2) * 2 = 8\}$$

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

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

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

Is this correct?

An example

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

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

Is this a valid triple?

An example

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

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

Is this a valid triple?

✓

An example

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

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

Is this a valid triple? ✓

Can we prove it with the rules that we have?

An example

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

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

Is this a valid triple? ✓

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

An Instance

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

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

Is this strong enough?

An example

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

Is this a valid triple?

An example

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

Is this a valid triple? ✓

An example

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

Is this a valid triple? ✓

Can we prove it with the rules that we have?

An example

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

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

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

Rules of Hoare Logic
If then else

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

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

An Instance

$$\dfrac{\dfrac{\vdots}{\vdash \texttt{skip}: \{x = 0 \wedge \mathit{false}\} \Rightarrow \{x = 1\}} \qquad \dfrac{\vdots}{\vdash x := x + 1 : \{x = 0 \wedge \neg \mathit{false}\} \Rightarrow \{x = 1\}}}{\vdash \texttt{if false then skip else } x := x + 1 : \{x = 0\} \Rightarrow \{x = 1\}}$$

An Instance

$$\dfrac{\dfrac{\vdots}{\vdash \texttt{skip}: \{x = 0 \wedge false\} \Rightarrow \{x = 1\}} \qquad \dfrac{\vdots}{\vdash x := x + 1 : \{x = 0 \wedge \neg false\} \Rightarrow \{x = 1\}}}{\vdash \texttt{if false then skip else } x := x + 1 : \{x = 0\} \Rightarrow \{x = 1\}}$$

Homework

Rules of Hoare Logic: Abort

$\vdash$ `Abort: ?⇒?`

Rules of Hoare Logic: Abort

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

What can be a good specification?

Rules of Hoare Logic: Abort

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

Rules of Hoare Logic: Abort

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

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

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

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

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

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 $Q\texttt{(m')}$.

Vacuously True

Rules of Hoare Logic
While

$\vdash$ `while e do c : ??`

Rules of Hoare Logic
While

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

Rules of Hoare Logic
While

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

Rules of Hoare Logic
While

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

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

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

An example

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

An example

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

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?

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

Another example

$$\frac{}{\vdash x := 3; y := 1 : \{true\} \Rightarrow \{x = 3 \wedge 1 = 1 \wedge y = 4 - x\}}$$

Another example

$$\dfrac{\dfrac{\vdash x := 3 : \{true\} \Rightarrow \{x = 3\} \qquad \vdash y := 1 : \{x = 3\} \Rightarrow \{x = 3 \wedge y = 1\}}{\vdash x := 3; y := 1 : \{true\} \Rightarrow \{x = 3 \wedge y = 1\}} \qquad x = 3 \wedge y = 1 \Rightarrow x = 3 \wedge 1 = 1 \wedge y = 4 - x}{\vdash x := 3; y := 1 : \{true\} \Rightarrow \{x = 3 \wedge 1 = 1 \wedge y = 4 - x\}}$$

Another example

$$\dfrac{\dfrac{true \Rightarrow 3 = 3 \quad \vdash x := 3 : \{3 = 3\} \Rightarrow \{x = 3\}}{\vdash x := 3 : \{true\} \Rightarrow \{x = 3\}} \quad \dfrac{x = 3 \Rightarrow x = 3 \wedge 1 = 1 \quad \vdash y := 1 : \{x = 3 \wedge 1 = 1\} \Rightarrow \{x = 3 \wedge y = 1\}}{\vdash y := 1 : \{x = 3\} \Rightarrow \{x = 3 \wedge y = 1\}}}{\dfrac{\vdash x := 3; y := 1 : \{true\} \Rightarrow \{x = 3 \wedge y = 1\} \quad x = 3 \wedge y = 1 \Rightarrow x = 3 \wedge 1 = 1 \wedge y = 4 - x}{\vdash x := 3; y := 1 : \{true\} \Rightarrow \{x = 3 \wedge 1 = 1 \wedge y = 4 - x\}}}$$

Another example

$x = 3 \land y = 1 \land y = 4 - x \Rightarrow y = 4 - x \land x \geq 1$

$\vdash$
```
while x > 1 do
  y := y+1;
  x := x-1
```
$: \{y = 4 - x \land x \geq 1\} \Rightarrow \{y = 4 - x \land x = 1\}$

$y = 4 - x \land x = 1 \Rightarrow y = 3$

$\vdash$
```
while x > 1 do
  y := y+1;
  x := x-1
```
$$: \{x = 3 \land y = 1 \land y = 4 - x\} \Rightarrow \{y = 3\}$$

Another example

$\vdash$ `y := y+1; x := x-1` $: \{y = 4 - x \wedge x \geq 1 \wedge x > 1\} \Rightarrow \{y = 4 - x \wedge x \geq 1\}$

$\vdash$ `while x > 1 do: y := y+1; x := x-1` $\{y = 4 - x \wedge x \geq 1\} \Rightarrow \{y = 4 - x \wedge x \geq 1 \wedge \neg(x > 1)\}$

$\{y = 4 - x \wedge x \geq 1 \wedge \neg(x > 1)\} \Rightarrow \{y = 4 - x \wedge x = 1\}$

$x = 3 \wedge y = 1 \wedge y = 4 - x \Rightarrow y = 4 - x \wedge x \geq 1$

$\vdash$ `while x > 1 do y := y+1; x := x-1` $: \{y = 4 - x \wedge x \geq 1\} \Rightarrow \{y = 4 - x \wedge x = 1\}$

$y = 4 - x \wedge x = 1 \Rightarrow y = 3$

$\vdash$ `while x > 1 do y := y+1; x := x-1` $: \{x = 3 \wedge y = 1 \wedge y = 4 - x\} \Rightarrow \{y = 3\}$

Another example

$y = 4 - x \wedge x \geq 1 \wedge x > 1 \Rightarrow y + 1 = 4 - (x - 1) \wedge x - 1 \geq 1$

$\vdash$ `y := y+1; x := x-1` $: \{y + 1 = 4 - (x - 1) \wedge x - 1 \geq 1\} \Rightarrow \{y = 4 - x \wedge x \geq 1\}$

$\vdash$ `y := y+1; x := x-1` $: \{y = 4 - x \wedge x \geq 1 \wedge x > 1\} \Rightarrow \{y = 4 - x \wedge x \geq 1\}$

$\vdash$

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

$\{y = 4 - x \wedge x \geq 1\} \Rightarrow \{y = 4 - x \wedge x \geq 1 \wedge \neg(x > 1)\}$

$\{y = 4 - x \wedge x \geq 1 \wedge \neg(x > 1)\} \Rightarrow \{y = 4 - x \wedge x = 1\}$

$x = 3 \wedge y = 1 \wedge y = 4 - x \Rightarrow y = 4 - x \wedge x \geq 1$

$\vdash$

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

$: \{y = 4 - x \wedge x \geq 1\} \Rightarrow \{y = 4 - x \wedge x = 1\}$

$y = 4 - x \wedge x = 1 \Rightarrow y = 3$

$\vdash$

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

$: \{x = 3 \wedge y = 1 \wedge y = 4 - x\} \Rightarrow \{y = 3\}$

Another example

$\vdash$ `y := y+1` $: \{y+1 = 4-(x-1) \wedge x-1 \geq 1\} \Rightarrow \{y = 4-(x-1) \wedge x-1 \geq 1\}$

$\vdash$ `x := x-1` $: \{y = 4-(x-1) \wedge x-1 \geq 1\} \Rightarrow \{y = 4-x \wedge x \geq 1\}$

$y = 4-x \wedge x \geq 1 \wedge x > 1 \Rightarrow y+1 = 4-(x-1) \wedge x-1 \geq 1$

$\vdash$ `y := y+1; x := x-1` $: \{y+1 = 4-(x-1) \wedge x-1 \geq 1\} \Rightarrow \{y = 4-x \wedge x \geq 1\}$

$\vdash$ `y := y+1; x := x-1` $: \{y = 4-x \wedge x \geq 1 \wedge x > 1\} \Rightarrow \{y = 4-x \wedge x \geq 1\}$

$\vdash$ `while x > 1 do: y := y+1; x := x-1` $\{y = 4-x \wedge x \geq 1\} \Rightarrow \{y = 4-x \wedge x \geq 1 \wedge \neg(x > 1)\}$

$\{y = 4-x \wedge x \geq 1 \wedge \neg(x > 1)\} \Rightarrow \{y = 4-x \wedge x = 1\}$

$x = 3 \wedge y = 1 \wedge y = 4-x \Rightarrow y = 4-x \wedge x \geq 1$

$\vdash$ `while x > 1 do y := y+1; x := x-1` $: \{y = 4-x \wedge x \geq 1\} \Rightarrow \{y = 4-x \wedge x = 1\}$

$y = 4-x \wedge x = 1 \Rightarrow y = 3$

$\vdash$ `while x > 1 do y := y+1; x := x-1` $: \{x = 3 \wedge y = 1 \wedge y = 4-x\} \Rightarrow \{y = 3\}$

Another example

$$\dfrac{\vdash \begin{array}{l}\texttt{x :=3;}\\ \texttt{y :=1;}\end{array} : \{true\} \Rightarrow \{x = 3 \wedge 1 = 1 \wedge y = 4 - x\} \qquad \vdash \begin{array}{l}\texttt{while x > 1 do}\\ \quad\texttt{y := y+1;}\\ \quad\texttt{x := x-1;}\end{array} : \{x = 3 \wedge y = 1 \wedge y = 4 - x\} \Rightarrow \{y = 3\}}{\vdash \begin{array}{l}\texttt{x:=3;}\\ \texttt{y:=1;}\\ \texttt{while x > 1 do}\\ \quad\texttt{y := y+1;}\\ \quad\texttt{x := x-1;}\end{array} : \{true\} \Rightarrow \{y = 3\}}$$

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.