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

Formal Semantics

We need to assign a formal meaning to the different components:

```
Precondition
Program
Postcondition
```

formal semantics of specification conditions

formal semantics of programs

formal semantics of specification conditions

We also need to describe the rules which combine program and specifications.

Programming Language

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

x, y, z, …	program variables
e_1, e_2, …	expressions
c_1, c_2, …	commands

Summary of the Semantics of Commands

$\{\texttt{abort}\}_m = \bot$

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

$\{\texttt{x:=e}\}_m = m[x \leftarrow \{e\}_m]$

$\{\texttt{c;c'}\}_m = \{c'\}_{m'}$ If $\{c\}_m = m'$

$\{\texttt{c;c'}\}_m = \bot$ If $\{c\}_m = \bot$

$\{\texttt{if e then } c_t \texttt{ else } c_f\}_m = \{c_t\}_m$ If $\{e\}_m = \texttt{true}$

$\{\texttt{if e then } c_t \texttt{ else } c_f\}_m = \{c_f\}_m$ If $\{e\}_m = \texttt{false}$

$\{\texttt{while e do c}\}_m = \sup_{n \in Nat} \{\texttt{while}_n \texttt{ e do c}\}_m$

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 $\mathtt{c:P \Rightarrow Q}$ 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?

Rules of Hoare Logic
Skip

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

Rules of Hoare Logic
Assignment

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

Rules of Hoare Logic
Composition

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

Rules of Hoare Logic
Consequence

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

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.

Today: More Hoare Logic

Rules of Hoare Logic
If then else

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

Is this correct?

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.

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 correct?

Rules of Hoare Logic
If then else

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

Is this strong enough?

Some examples

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

How can we derive this?

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
While

$$\frac{\vdash \texttt{c : ??}}{\vdash \texttt{while e do c : ??}}$$

Rules of Hoare Logic
While

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

Invariant

Some examples

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

How can we derive this?

Some examples

$$\dfrac{\vdash x := x+1 : \{x+1=1\} \Rightarrow \{x=1\} \qquad {\color{blue} x=1 \wedge x=0 \Rightarrow x+1=1}}{\vdash x := x+1 : \{x=1 \wedge x=0\} \Rightarrow \{x=1\}}$$

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

Some examples

$\vdash$

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

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

How can we derive this?