Hoare Logic, Part I

CS560: Reasoning About Programs

Roopsha Samanta

PURDUE UNIVERSITY

Partly based on slides by Isil Dillig

Announcements

- There be no midterm this time
- Keep an eye out for updated schedule
- HW 3 will be released today

Grading

Component	Weight
Class Project	~~40%~~ 50%
~~Midterm~~	~~20%~~
Homeworks	~~35%~~ 45%
Participation	5%

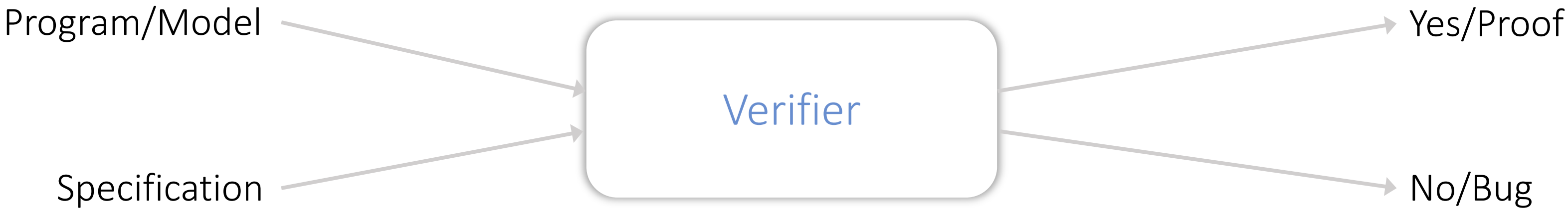
Roadmap

Previously

- Unit 1: Logics and proof engines

Today

- Unit 2: Program verification and analysis
- (Floyd-)Hoare logic: axiomatic approach to program verification
- Partial correctness, total correctness, Hoare triples
- Hoare logic inference rules for partial correctness

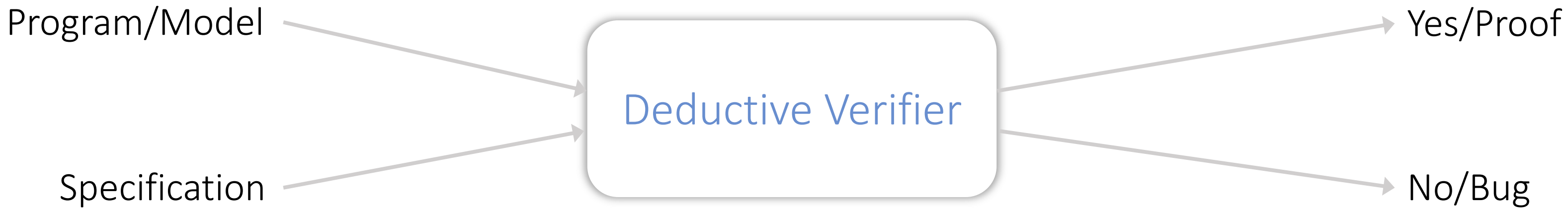


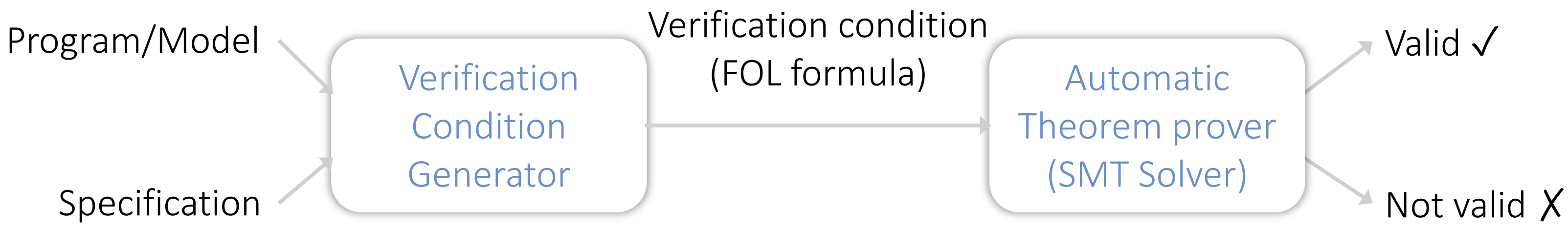
Type Systems

Deductive Verification

Model Checking

Abstract Interpretation


Program/Model
Specification
Deductive Verifier
Yes/Proof
No/Bug



Verification condition is a formula that is valid iff program is correct

Today

- Use Hoare logic to deductively prove programs correct

Next

- Use verification conditions to automate Hoare logic

A bit of history

Dijkstra

Floyd

Hoare

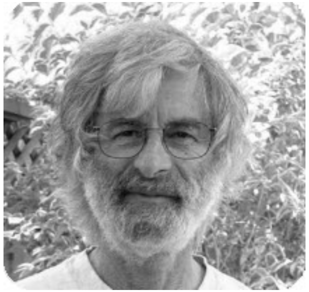
Milner

Pnueli

Clarke

Emerson

Sifakis



Lamport

A bit of history

Dijkstra

Floyd

Hoare

Floyd, *Assigning Meanings to Programs*, 1967

Hoare, *An Axiomatic Basis for Computer Programming*, 1969

Dijkstra, *Guarded Commands, Nondeterminacy and Formal Derivation of Programs*, 1975

Simple imperative programming language (IMP)

Expression $E \coloneqq Z \mid V \mid e_1 + e_2 \mid e_1 \times e_2$

Condition $C \coloneqq \texttt{true} \mid \texttt{false} \mid e_1 = e_2 \mid e_1 \leq e_2$

Statement $S \coloneqq V \coloneqq E$

$S_1; S_2$

$\texttt{if } C \texttt{ then } S_1 \texttt{ else } S_2$

$\texttt{while } C \texttt{ do } S_1$

We will use this to illustrate Hoare logic

Hoare triple: partial correctness

$$\{P\}\ S\ \{Q\}$$

S is a program statement in IMP

P, the precondition, is a FOL formula

Q, the postcondition, is a FOL formula

Hoare triple: partial correctness

$$\{P\}\ S\ \{Q\}$$

S is a program statement in IMP

P, the precondition, is a FOL formula

Q, the postcondition, is a FOL formula

Partial correctness / Validity of $\{P\}\ S\ \{Q\}$:

If S is executed in a **program state** satisfying P,

and if execution of S terminates,

then the resulting program state satisfies Q

Program state:
Assignment of values from proper domain to all program variables

Sets of program states can be represented using FOL formulas over program variables

Hoare triple: total correctness

$$[P]\ S\ [Q]$$

S is a program statement in IMP

P, the precondition, is a FOL formula

Q, the postcondition, is a FOL formula

Hoare triple: total correctness

$[P]\ S\ [Q]$

Total correctness / Validity of $[P]\ S\ [Q]$:

If S is executed in a **program state** satisfying P,

then execution of S terminates,

and the resulting program state satisfies Q

S is a program statement in IMP

P, the precondition, is a FOL formula

Q, the postcondition, is a FOL formula

Total correctness = Partial correctness + termination

Safety

Liveness

Proving partial correctness

$\vDash \{P\}\ C\ \{Q\}$ Hoare triple is valid
$\vdash \{P\}\ C\ \{Q\}$ Hoare triple is provable

Soundness: If $\vdash \{P\}\ C\ \{Q\}$, then $\vDash \{P\}\ C\ \{Q\}$
Completeness: If $\vDash \{P\}\ C\ \{Q\}$, then $\vdash \{P\}\ C\ \{Q\}$

Hoare gave a sound and *relatively* complete proof system that allows semi-automation of correctness proofs

$\models \{false\}\ S\ \{Q\}$? ✓

$\{true\}\ S\ \{Q\}$ ✗

$\{P\}\ S\ \{true\}$ ✓

$[P]\ S\ [true]$ ✗

$\{true\}\ S\ \{false\}$ ✗

$\{x=0\}\ x := x+1\ \{x>0\}$ ✓

→ $\{x=1 \vee y>0\}$ ✓

→ $\{y>0\}$ ✗

$\{x=0\}$ while true do $x:=0$ $\{x>0\}$ ✓

Inference rules

$$\frac{\vdash \{P_1\}\ C\ \{Q_1\}\ \ldots\ \vdash \{P_n\}\ C\ \{Q_n\}}{\vdash \{P\}\ C\ \{Q\}}$$

If $\{P_1\}\ C\ \{Q_1\}, \ldots, \{P_n\}\ C\ \{Q_n\}$ are provable in proof system, then $\{P\}\ C\ \{Q\}$ is also provable

$$\begin{aligned} S \ ::= \ & V := E \\ & S_1; S_2 \\ & \texttt{if}\ C\ \texttt{then}\ S_1\ \texttt{else}\ S_2 \\ & \texttt{while}\ C\ \texttt{do}\ S_1 \end{aligned}$$

One inference rule for every statement

Inference rules without hypotheses correspond to base cases in proof

Inference rules with hypotheses correspond to inductive cases in proof

Hoare inference rules

Assignment

Q with x substituted by E

$$\overline{\vdash \{Q[E/x]\}\ x := E\ \{Q\}}$$

$\{?\}\ x := E\ \{Q\}$

$\{i > 9\}\ i := i+1\ \{i > 10\}$

$Q[i+1/i]$

$\downarrow$

$i+1 > 10$

$i > 9$

$\{x = y\}\ x := 4\ \{x = y\}$

$x = y\,[4/x]$

$4 = y$

$\{y = y\}\ x := y\ \{y = x\}$

$y = x\,[y/x]$

$y = y$

Hoare inference rules

Assignment

Q with x substituted by E

$$\overline{\vdash \{Q[E/x]\}\ x := E\ \{Q\}}$$

Precondition strengthening/
Postcondition weakening

$$\frac{P' \Rightarrow P \quad \vdash \{P\}\ S\ \{Q\} \quad Q \Rightarrow Q'}{\vdash \{P'\}\ S\ \{Q'\}}$$

$\{z=2\}\ y := x\ \{y=x\}$

Valid? Yes!

Provable using ass. rule?

$y=x[x/y]$

$\leadsto x=x$

$\leadsto \text{true}$

$$\frac{\vdash \{\text{true}\}\ y := x\ \{y=x\} \qquad z=2 \Rightarrow \text{true}}{\vdash \{z=2\}\ y := x\ \{y=x\}}$$

$\{z=2\}\ y:=x\ \{y=x \land z=2\}$ Valid? ✓

$\vdash \{z=2\}\ y:=x\ \{y=x\}$ Provable? ✓ using ass. rule

What else is provable?

$\{z=2\}\ y:=x$

- $\{y=x \lor z=2\}$ ✓
- $\{z=2\}$ ✓
- $\{\exists x.\ x=y\}$ ✓
- $\{\forall x.\ x=y\}$ ✗

$y=x \land z=2[x/y]$

$x=x \land z=2$

$\equiv \text{true} \land z=2$

$\equiv z=2$ ✓

Hoare inference rules

Assignment

Q with x substituted by E

$$\frac{}{\vdash \{Q[E/x]\}\ x \coloneqq E\ \{Q\}}$$

Precondition strengthening/
Postcondition weakening

$$\frac{P' \Rightarrow P \quad \vdash \{P\}\ S\ \{Q\} \quad Q \Rightarrow Q'}{\vdash \{P'\}\ S\ \{Q'\}}$$

Composition

$$\frac{\vdash \{P\}\ S_1\ \{Q\} \quad \vdash \{Q\}\ S_2\ \{R\}}{\vdash \{P\}\ S_1; S_2\ \{\mathrm{R}\}}$$

$\{P\}$ S_1 $\{Q\}$ S_2 $\{R\}$

$\{P\}$ $S_1;$ S_2 $\{R\}$

$$\dfrac{}{\vdash \{x=2[2/x]\}\ x:=2\ \{x=2\}}\ \text{Ass}$$

$$\vdash \{\text{true}\}\ x:=2\ \{x=2\}$$

$$\dfrac{}{\{x=2 \wedge y=2[x/y]\}\ y:=x\ \{y=2 \wedge x=2\}}\ \text{Ass}$$

$$\{x=2\}\ y:=x\ \{y=2 \wedge x=2\}$$

$$\dfrac{\vdash \{\text{true}\}\ x:=2\ \{x=2\} \qquad \{x=2\}\ y:=x\ \{y=2 \wedge x=2\}}{\vdash \{\text{true}\}\ x:=2;\ y:=x\ \{y=2 \wedge x=2\}}\ \text{Comp}$$

Hoare inference rules

Assignment

Q with x substituted by E

$$\frac{}{\vdash \{Q[E/x]\}\ x := E\ \{Q\}}$$

Precondition strengthening/
Postcondition weakening

$$\frac{P' \Rightarrow P \quad \vdash \{P\}\ S\ \{Q\} \quad Q \Rightarrow Q'}{\vdash \{P'\}\ S\ \{Q'\}}$$

Composition

$$\frac{\vdash \{P\}\ S_1\ \{Q\} \quad \vdash \{Q\}\ S_2\ \{R\}}{\vdash \{P\}\ S_1; S_2\ \{\mathrm{R}\}}$$

If

$$\frac{\vdash \{C \wedge P\}\ S_1\ \{Q\} \quad \vdash \{\neg C \wedge P\}\ S_2\ \{Q\}}{\vdash \{P\}\ \text{if}\ C\ \text{then}\ S_1\ \text{else}\ S_2\ \{Q\}}$$

{true} if x>0 then y:=x {y≥0}
else y:=-x

Try this at

Hoare inference rules

Assignment

Q with x substituted by E

$$\frac{}{\vdash \{Q[E/x]\}\ x := E\ \{Q\}}$$

Precondition strengthening/
Postcondition weakening

$$\frac{P' \Rightarrow P \quad \vdash \{P\}\ S\ \{Q\} \quad Q \Rightarrow Q'}{\vdash \{P'\}\ S\ \{Q'\}}$$

Composition

$$\frac{\vdash \{P\}\ S_1\ \{Q\} \quad \vdash \{Q\}\ S_2\ \{R\}}{\vdash \{P\}\ S_1; S_2\ \{\mathrm{R}\}}$$

If

$$\frac{\vdash \{C \wedge P\}\ S_1\ \{Q\} \qquad \vdash \{\neg C \wedge P\}\ S_2\ \{Q\}}{\vdash \{P\}\ \text{if } C \text{ then } S_1 \text{ else } S_2\ \{Q\}}$$

While

$$\frac{\vdash \{C \wedge I\}\ S\ \{I\}}{\vdash \{I\}\ \text{while } C \text{ do } S\ \{I \wedge \neg C\}}$$

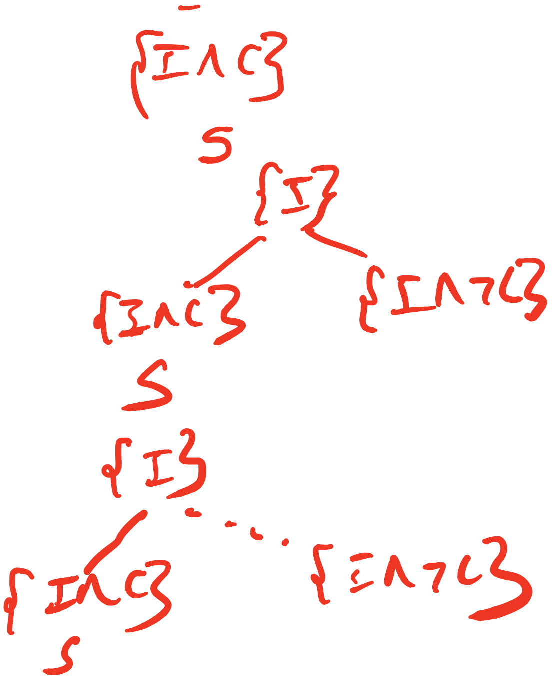
Loop Invariant

1. I holds initially before loop
2. I holds after each loop iter.

$\{P\}$ while C do S $\{P \lor \bigvee_{i=1}^{??} (Q_i \land \neg C)\}$

Loop iteration

0	$\{P\}$
1	$\{P \land C\}\ S\ \{Q_1 \land \neg C\}$
2	$\{P \land C\}\ S; S\ \{Q_2 \land \neg C\}$
3	$\{P \land C\}\ S; S; S\ \{Q_3 \land \neg C\}$
⋮	
n	$\{P \land C\}\ \underbrace{S; \dots; S}_{n \text{ times}}\ \{Q_n \land \neg C\}$



$$\{x < n\} \; \text{while } x < n \text{ do } x := x+1 \; \{x \geq n\}$$

$$\{x \leq n[x+1/x]\} \; x := x+1 \; \{x \leq n\} \quad \text{Ass}$$

$x \leq n[x+1/x]$

$x+1 \leq n$

$x < n$

$$\vdash \{x \leq n \wedge x < n\} \; x := x+1 \; \{x \leq n\} \quad \text{Loop}$$

$$\vdash \{x \leq n\} \; \text{while } x < n \text{ do } x := x+1 \; \{x \leq n \wedge x \geq n\}$$

$$x \leq n \wedge x \geq n \rightarrow x \geq n \quad \text{Post weaken}$$

$$\vdash \{x \leq n\} \; \text{while } \{x < n\} \text{ do } x := x+1 \; \{x \geq n\}$$

Loop invariant ($x \leq n$)

Invariant vs. Inductive Invariant

- Loop invariant I may not always satisfy $\{I \land C\}\ S\ \{I\}$
- Inductive invariant always satisfies $\{I \land C\}\ S\ \{I\}$
- Inductive invariants are the only invariants we can prove

- Key challenge in verification: finding inductive invariants

Consider:

```
i := 1 ;
j := 1 ;
while i<n do
    j := j + i
    i := i + 1
```

The loop invariant $j \geq 1$ is not inductive. Why?

We can strengthen $j \geq 1$ to $j \geq 1 \wedge i \geq 1$ to get an inductive invariant!

Hoare Logic: Soundness and Completeness

If $\vdash \{P\}\, S\, \{Q\}$, then $\vDash\ \{P\}\, S\, \{Q\}$
Proof rules for Hoare logic are sound

If $\vDash\ \{P\}\, S\, \{Q\}$ and we have an oracle for deciding implications, then $\vdash \{P\}\, S\, \{Q\}$
Proof rules for Hoare logic are *relatively* complete

Precondition strengthening/Postcondition weakening may need reasoning about implications in Peano arithmetic, which is incomplete.

Summary

Today

- (Floyd-)Hoare logic: axiomatic approach to program verification
- Partial correctness, total correctness, Hoare triples
- Hoare logic inference rules for partial correctness

Next

- Automating Hoare logic inference rules using verification conditions