

Automated Reasoning

Lecture 11: Program verification using Hoare Logic (II)

Jacques Fleuriot
jdf@inf.ed.ac.uk

Previously on Hoare Logic

A simple “while” language

- ▶ Sequence: `a ; b`
- ▶ Skip (do nothing): `SKIP`
- ▶ Variable assignment: `X := 0`
- ▶ Conditional:
`IF cond THEN a ELSE b FI`
- ▶ Loop: `WHILE cond DO c OD`

Hoare Logic

- ▶ $\{P\} C \{Q\}$
- ▶ Formal specification
- ▶ Axiomatic semantics
- ▶ Hoare Logic Rules and examples

Conditional Rule

$$\frac{\{P \wedge S\} C_1 \{Q\} \quad \{P \wedge \neg S\} C_2 \{Q\}}{\{P\} \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \text{ FI } \{Q\}}$$

► Example (Max X Y):

$$\frac{\{X \geq X \wedge X \geq Y\} \text{ MAX} := X \{MAX \geq X \wedge MAX \geq Y\}}{\{T \wedge X \geq Y\} \text{ MAX} := X \{MAX \geq X \wedge MAX \geq Y\}} \quad (1)$$

$$\frac{\{Y \geq X \wedge Y \geq Y\} \text{ MAX} := Y \{MAX \geq X \wedge MAX \geq Y\}}{\{T \wedge \neg(X \geq Y)\} \text{ MAX} := Y \{MAX \geq X \wedge MAX \geq Y\}} \quad (2)$$

$$\frac{\begin{array}{c} (1) \qquad (2) \\ \hline \end{array}}{\{T\} \text{ IF } X \geq Y \text{ THEN } \text{ MAX} := X \text{ ELSE } \text{ MAX} := Y \text{ FI } \{MAX \geq X \wedge MAX \geq Y\}} \quad (3)$$

What if?

$$\frac{\{P \wedge S\} C_1 \{Q\} \quad \{P \wedge \neg S\} C_2 \{Q\}}{\{P\} \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \text{ FI } \{Q\}}$$

- Example (Max X Y):

$$\frac{\frac{\{X = \max(X, Y)\} \text{ MAX} := X \{MAX = \max(X, Y)\}}{???}}{\{T \wedge X \geq Y\} \text{ MAX} := X \{MAX = \max(X, Y)\}} \quad (4)$$

$$\frac{\frac{\{Y = \max(X, Y)\} \text{ MAX} := Y \{MAX = \max(X, Y)\}}{???}}{\{T \wedge \neg(X \geq Y)\} \text{ MAX} := Y \{MAX = \max(X, Y)\}} \quad (5)$$

$$\frac{(4) \quad (5)}{\{T\} \text{ IF } X \geq Y \text{ THEN } \text{ MAX} := X \text{ ELSE } \text{ MAX} := Y \text{ FI } \{MAX = \max(X, Y)\}} \quad (6)$$

Precondition Strengthening

$$\frac{P \longrightarrow P' \quad \{P'\} C \{Q\}}{\{P\} C \{Q\}}$$

- ▶ Replace a *precondition* with a stronger condition
- ▶ Example:

$$\frac{X = n \longrightarrow X + 1 = n + 1 \quad \overline{\{X + 1 = n + 1\} X := X + 1 \{X = n + 1\}}}{\{X = n\} X := X + 1 \{X = n + 1\}}$$

Postcondition Weakening

$$\frac{\{P\} C \{Q'\} \quad Q' \longrightarrow Q}{\{P\} C \{Q\}}$$

- ▶ Replace a *postcondition* with a weaker condition
- ▶ Example:

$$\frac{\{X = n\} X := X + 1 \{X = n + 1\} \quad X = n + 1 \longrightarrow X > n}{\{X = n\} X := X + 1 \{X > n\}}$$

Aha!

$$\frac{P \longrightarrow P' \quad \{P'\} C \{Q\}}{\{P\} C \{Q\}}$$

► Example (Max X Y):

$$\frac{\mathbf{T} \wedge X \geq Y \longrightarrow X = \max(X, Y) \quad \overline{\{X = \max(X, Y)\} \text{MAX} := X \{MAX = \max(X, Y)\}}}{\{\mathbf{T} \wedge X \geq Y\} \text{MAX} := X \{MAX = \max(X, Y)\}} \quad (7)$$

$$\frac{\mathbf{T} \wedge \neg(X \geq Y) \longrightarrow Y = \max(X, Y) \quad \overline{\{Y = \max(X, Y)\} \text{MAX} := Y \{MAX = \max(X, Y)\}}}{\{\mathbf{T} \wedge \neg(X \geq Y)\} \text{MAX} := Y \{MAX = \max(X, Y)\}} \quad (8)$$

$$\frac{\overline{\{ \text{(7)} \quad \text{(8)} \}}}{\{\mathbf{T}\} \text{ IF } X \geq Y \text{ THEN MAX} := X \text{ ELSE MAX} := Y \text{ FI } \{MAX = \max(X, Y)\}} \quad (9)$$

Verification Conditions (VCs)

$\{T\}$ IF $X \geq Y$ THEN $MAX := X$ ELSE $MAX := Y$ FI $\{MAX = \max(X, Y)\}$

- ▶ FOL VCs:

$$T \wedge X \geq Y \longrightarrow X = \max(X, Y)$$

$$T \wedge \neg(X \geq Y) \longrightarrow Y = \max(X, Y)$$

- ▶ Hoare Logic rules can be applied *automatically* to generate VCs
 - ▶ e.g. Isabelle's `vcc` tactic
- ▶ We need to provide proofs for the VCs / *proof obligations*
 - ▶ Reduced to FOL statements
 - ▶ From simple algebraic proofs to reasoning about inductive data types

WHILE Rule

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{ WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}}$$

- ▶ P is an *invariant* for C whenever S holds
- ▶ *WHILE rule*: If executing C *once* preserves the truth of P , then executing C *any number of times* also preserves the truth of P
- ▶ If P is an invariant for C when S holds then P is an invariant of the *whole* WHILE loop, i.e. a *loop invariant*

WHILE Rule

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{ WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}}$$

```
{Y = 1 ∧ Z = 0}
WHILE Z ≠ X DO
  Z := Z + 1 ;
  Y := Y × Z
OD
{Y = X!}
```

WHILE Rule

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{ WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}}$$

$\{Y = 1 \wedge Z = 0\}$
WHILE $Z \neq X$ DO
 $Z := Z + 1$;
 $Y := Y \times Z$
OD
 $\{Y = X!\}$

vs.

$\{P\}$
WHILE $Z \neq X$ DO
 $Z := Z + 1$;
 $Y := Y \times Z$
OD
 $\{P \wedge \neg Z \neq X\}$

► What is P ?

WHILE Rule - How to find an invariant

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{ WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}}$$

- ▶ The invariant P should:
 - ▶ Say what *has been done so far* together with what *remains to be done*
 - ▶ Hold *at each iteration* of the loop.
 - ▶ Give the *desired result* when the loop terminates

WHILE Rule - Invariant VCs

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{ WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}}$$

$\{Y = 1 \wedge Z = 0\} \text{ WHILE } Z \neq X \text{ DO } Z := Z + 1 ; Y := Y \times Z \text{ OD } \{Y = X!\}$

$\{P\} \text{ WHILE } Z \neq X \text{ DO } Z := Z + 1 ; Y := Y \times Z \text{ OD } \{P \wedge \neg Z \neq X\}$

► We need to find an invariant P such that:

- $\{P \wedge Z \neq X\} Z := Z + 1 ; Y := Y \times Z \{P\}$ (WHILE rule)
- $Y = 1 \wedge Z = 0 \longrightarrow P$ (precondition strengthening)
- $P \wedge \neg(Z \neq X) \longrightarrow Y = X!$ (postcondition weakening)

WHILE Rule - Loop invariant for factorial

$$\{P \wedge Z \neq X\} Z := Z + 1 ; Y := Y \times Z \{P\}$$

$$Y = 1 \wedge Z = 0 \longrightarrow P$$

$$P \wedge \neg(Z \neq X) \longrightarrow Y = X!$$

► ???

WHILE Rule - Loop invariant for factorial

$$\{P \wedge Z \neq X\} Z := Z + 1 ; Y := Y \times Z \{P\}$$

$$Y = 1 \wedge Z = 0 \longrightarrow P$$

$$P \wedge \neg(Z \neq X) \longrightarrow Y = X!$$

▶ $Y = Z!$

▶ VCs:

▶ $\{Y = Z! \wedge Z \neq X\} Z := Z + 1 ; Y := Y \times Z \{Y = Z!\}$

because: $Y = Z! \wedge Z \neq X \longrightarrow Y \times (Z + 1) = (Z + 1)!$ and (10)

▶ $Y = 1 \wedge Z = 0 \longrightarrow Y = Z!$

because: $0! = 1$

▶ $Y = Z! \wedge \neg(Z \neq X) \longrightarrow Y = X!$

because: $\neg(Z \neq X) \leftrightarrow Z = X$

$$\frac{\{Y \times (Z + 1) = (Z + 1)!\} Z := Z + 1 \{Y \times Z = Z!\} \quad \{Y \times Z = Z!\} Y := Y \times Z \{Y = Z!\}}{\{Y \times (Z + 1) = (Z + 1)!\} Z := Z + 1 ; Y := Y \times Z \{Y = Z!\}}$$

WHILE Rule - Complete factorial example

	$\{Y = 1 \wedge Z = 0\}$
	$\{Y = Z!\}$
WHILE $Z \neq X$ DO	
	$\{Y = Z! \wedge Z \neq X\}$
	$\{Y \times (Z + 1) = (Z + 1)!\}$
$Z := Z + 1 ;$	
	$\{Y \times Z = Z!\}$
$Y := Y \times Z$	
	$\{Y = Z!\}$
OD	
	$\{Y = Z! \wedge \neg Z \neq X\}$
	$\{Y = X!\}$

Another example - Multiplication!

```
I := Y;
Z := 0;
WHILE I  $\neq$  0 DO
  Z := Z + X ;
  I := I - 1
OD
```

$\{Y \geq 0\}$

$\{Z = X \times Y\}$

Another example - Multiplication!

	$\{Y \geq 0\}$
I := Y;	
Z := 0;	
	$\{\text{Invariant?}\}$
WHILE I \neq 0 DO	
	$\{\text{Invariant?} \wedge I \neq 0\}$
Z := Z + X ;	
I := I - 1	
	$\{\text{Invariant?}\}$
OD	
	$\{\text{Invariant?} \wedge \neg I \neq 0\}$
	$\{Z = X \times Y\}$

Another example - Multiplication!

```

                                                    {Y ≥ 0}
I := Y;
Z := 0;
                                                    {Z = (Y - I) × X}
WHILE I ≠ 0 DO
    Z := Z + X ;
    I := I - 1
    {Z = (Y - I) × X}
OD
    {Z = (Y - I) × X ∧ ¬I ≠ 0}
    {Z = X × Y}
```

Another example - Multiplication!

```

                                                    {Y ≥ 0}
I := Y;
Z := 0;
                                                    {Z = (Y - I) × X}
WHILE I ≠ 0 DO
    {Z = (Y - I) × X ∧ I ≠ 0}
    {Z + X = (Y - (I - 1)) × X}
    Z := Z + X ;
    {Z = (Y - (I - 1)) × X}
    I := I - 1
    {Z = (Y - I) × X}
OD
    {Z = (Y - I) × X ∧ ¬I ≠ 0}
    {Z = X × Y}
```

Another example - Multiplication!

	$\{Y \geq 0\}$
	$\{0 = (I - 1) \times X\}$
I := Y;	
	$\{0 = (Y - I) \times X\}$
Z := 0;	
	$\{Z = (Y - I) \times X\}$
WHILE I \neq 0 DO	
	$\{Z = (Y - I) \times X \wedge I \neq 0\}$
	$\{Z + X = (Y - (I - 1)) \times X\}$
Z := Z + X ;	
	$\{Z = (Y - (I - 1)) \times X\}$
I := I - 1	
	$\{Z = (Y - I) \times X\}$
OD	
	$\{Z = (Y - I) \times X \wedge \neg I \neq 0\}$
	$\{Z = X \times Y\}$

Isabelle

```
Lemma Multipl: "VARS (z :: int) i
{0 ≤ y}
i := y;
z := 0;
WHILE i ≠ 0
INV { z = (y - i) * x }
DO
  z := z + x;
  i := i - 1
OD
{z = x * y}"
apply vcg
apply (auto simp add: algebra_simps)
```

Proof state Auto update Search: 100%

proof (prove)

goal (3 subgoals):

1. $\bigwedge z i. 0 \leq y \implies 0 = (y - y) * x$
2. $\bigwedge z i. z = (y - i) * x \wedge i \neq 0 \implies z + x = (y - (i - 1)) * x$
3. $\bigwedge z i. z = (y - i) * x \wedge \neg i \neq 0 \implies z = x * y$

Isabelle

```
Lemma Multipl: "VARs (z :: int) i
{0 ≤ y}
i := y;
z := 0;
WHILE i ≠ 0
INV { z = (y - i) * x }
DO
  z := z + x;
  i := i - 1
OD
{z = x * y}"
apply vcg
apply (auto simp add: algebra_simps)
```

Proof state

Auto update

Update

Search:

100%

proof (prove)

goal:

No subgoals!

Specification and correctness

```
{T}  
I := Y;  
Z := 0;  
WHILE I ≠ 0 DO  
  Z := Z + X ;  
  I := I - 1  
OD  
{Z = X × Y}
```

vs.

```
{Y ≥ 0}  
I := Y;  
Z := 0;  
WHILE I ≠ 0 DO  
  Z := Z + X ;  
  I := I - 1  
OD  
{Z = X × Y}
```

- ▶ What is the difference?

Specification and correctness

$\{T\}$		$\{Y \geq 0\}$
$I := Y;$		$I := Y;$
$Z := 0;$	vs.	$Z := 0;$
WHILE $I \neq 0$ DO		WHILE $I \neq 0$ DO
$Z := Z + X ;$		$Z := Z + X ;$
$I := I - 1$		$I := I - 1$
OD		OD
$\{Z = X \times Y\}$		$\{Z = X \times Y\}$

- ▶ What is the difference? - *Termination!*

Hoare Logic Rules (it does!)

$$\frac{P \longrightarrow P' \quad \{P'\} C \{Q\}}{\{P\} C \{Q\}} \text{ PS}$$

$$\frac{\{P\} C \{Q'\} \quad Q' \longrightarrow Q}{\{P\} C \{Q\}} \text{ PW}$$

$$\overline{\{Q[E/V]\} V := E \{Q\}} \text{ ASSIGN}$$

$$\overline{\{P\} \text{ SKIP } \{P\}} \text{ SKIP}$$

$$\frac{\{P\} C_1 \{Q\} \quad \{Q\} C_2 \{R\}}{\{P\} C_1 ; C_2 \{R\}} \text{ SEQ}$$

$$\frac{\{P \wedge S\} C_1 \{Q\} \quad \{P \wedge \neg S\} C_2 \{Q\}}{\{P\} \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \text{ FI } \{Q\}} \text{ IF}$$

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{ WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}} \text{ WHILE}$$

Other topics

$$\{P\} C \{Q\}$$

- ▶ Weakest preconditions, strongest postconditions

Other topics

$$\{P\} C \{Q\}$$

- ▶ Meta-theory: Is Hoare logic...
 - ▶ ... *sound*? - Yes! Based on programming language semantics (but what about more complex languages?)
 - ▶ ... *decidable*? - No! $\{T\} C \{F\}$ is the halting problem!
 - ▶ ... *complete*? - *Relatively* / only for simple languages

Other topics

$$\{P\} C \{Q\}$$

- ▶ Automatic Verification Condition Generation (VCG)
- ▶ Automatic generation/inference of loop invariants!
- ▶ More complex languages - e.g. Pointers = Separation logic
- ▶ Functional programming (recursion = induction)

Summary

- ▶ Precondition strengthening
- ▶ Postcondition weakening
- ▶ Automated generation of *Verification Conditions* (VCs)
- ▶ WHILE rule: *Loop invariants!*
 - ▶ Properties that hold during *while* loops
 - ▶ Loop invariant generation is generally *undecidable*

Recommended reading

Theory:

- ▶ Mike Gordon, *Background Reading on Hoare Logic*, <https://www.cl.cam.ac.uk/archive/mjcg/HL/Notes/Notes.pdf> (pp. 1-27, 37-48)
- ▶ Huth & Ryan, Sections 4.1-4.3 (pp. 256-292)
- ▶ Nipkow & Klein, Section 12.2.1 (pp. 191-199)

Practice:

- ▶ Isabelle's Hoare Logic library:
<http://isabelle.in.tum.de/dist/library/HOL/HOL-Hoare>
- ▶ Tutorial exercise