COMP4161: Advanced Topics in Software Verification

$\{\mathbf{P}\} \ldots \{\mathbf{Q}\}$

Gerwin Klein, June Andronick, Christine Rizkallah, Miki Tanaka

S2/2018

Last Time

- ➜ Syntax of a simple imperative language
- ➜ Operational semantics
- ➜ Program proof on operational semantics
- ➜ Hoare logic rules
- ➜ Soundness of Hoare logic

Content

→ Intro & motivation, getting started [1]

→ Foundations & Principles

- Lambda Calculus, natural deduction [1,2]
- Higher Order Logic [3[a]]
- Term rewriting [4]

→ Proof & Specification Techniques

- Inductively defined sets, rule induction [5]
- Datatypes, recursion, induction [6, 7]
- Hoare logic, proofs about programs, invariants [8[b],9]
- (mid-semester break)
- C verification [10]
- CakeML, Isar [11[c]]
- Concurrency [12]

---

[a] a1 due; [b] a2 due; [c] a3 due

Automation?

Last time: Hoare rule application is nicer than using operational semantic.

BUT:

- ➜ it's still kind of tedious
- ➜ it seems boring & mechanical

Automation?

Invariant

Invariant

Problem: While – need creativity to find right (invariant) P

Invariant

Problem: While – need creativity to find right (invariant) P

Solution:

➜ annotate program with invariants

Invariant

Problem: While – need creativity to find right (invariant) P

Solution:

- ➜ annotate program with invariants
- ➜ then, Hoare rules can be applied automatically

Invariant

Problem: While – need creativity to find right (invariant) P

Solution:

- ➜ annotate program with invariants
- ➜ then, Hoare rules can be applied automatically

Example:

$$\{M = 0 \wedge N = 0\}$$
$$\text{WHILE } M \neq a \text{ INV } \{N = M * b\} \text{ DO } N := N + b; M := M + 1 \text{ OD}$$
$$\{N = a * b\}$$

Weakest Preconditions

$$\textbf{pre}\ c\ Q = \textbf{weakest}\ P\ \textbf{such that}\ \{P\}\ c\ \{Q\}$$

With annotated invariants, easy to get:

$\text{pre SKIP}\ Q \qquad\qquad\qquad\qquad\qquad =$

Weakest Preconditions

$$\textbf{pre } c\ Q = \textbf{weakest } P \textbf{ such that } \{P\}\ c\ \{Q\}$$

With annotated invariants, easy to get:

$$\begin{array}{lcl}
\text{pre SKIP } Q & = & Q \\
\text{pre } (x := a)\ Q & = &
\end{array}$$

Weakest Preconditions

$$\textbf{pre } c\ Q = \textbf{weakest } P \textbf{ such that } \{P\}\ c\ \{Q\}$$

With annotated invariants, easy to get:

$$\begin{array}{lcl}
\text{pre SKIP } Q & = & Q \\
\text{pre } (x := a)\ Q & = & \lambda\sigma.\ Q(\sigma(x := a\sigma)) \\
\text{pre } (c_1; c_2)\ Q & = &
\end{array}$$

Weakest Preconditions

pre c Q **= weakest** P **such that** $\{P\}$ c $\{Q\}$

With annotated invariants, easy to get:

$$
\begin{array}{lcl}
\text{pre SKIP } Q & = & Q \\
\text{pre } (x := a)\ Q & = & \lambda\sigma.\ Q(\sigma(x := a\sigma)) \\
\text{pre } (c_1; c_2)\ Q & = & \text{pre } c_1\ (\text{pre } c_2\ Q) \\
\text{pre } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2)\ Q & = &
\end{array}
$$

Weakest Preconditions

$$\textbf{pre}\ c\ Q = \textbf{weakest}\ P\ \textbf{such that}\ \{P\}\ c\ \{Q\}$$

With annotated invariants, easy to get:

$$
\begin{array}{lcl}
\text{pre SKIP } Q & = & Q \\
\text{pre } (x := a)\ Q & = & \lambda\sigma.\ Q(\sigma(x := a\sigma)) \\
\text{pre } (c_1; c_2)\ Q & = & \text{pre } c_1\ (\text{pre } c_2\ Q) \\
\text{pre } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2)\ Q & = & \lambda\sigma.\ (b \longrightarrow \text{pre } c_1\ Q\ \sigma) \wedge \\
 & & \quad (\neg b \longrightarrow \text{pre } c_2\ Q\ \sigma) \\
\text{pre } (\text{WHILE } b \text{ INV } I \text{ DO } c \text{ OD})\ Q & = &
\end{array}
$$

Weakest Preconditions

$$\textbf{pre}\ c\ Q = \textbf{weakest}\ P\ \textbf{such that}\ \{P\}\ c\ \{Q\}$$

With annotated invariants, easy to get:

$$
\begin{array}{lcl}
\text{pre SKIP } Q & = & Q \\
\text{pre } (x := a)\ Q & = & \lambda\sigma.\ Q(\sigma(x := a\sigma)) \\
\text{pre } (c_1; c_2)\ Q & = & \text{pre } c_1\ (\text{pre } c_2\ Q) \\
\text{pre } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2)\ Q & = & \lambda\sigma.\ (b \longrightarrow \text{pre } c_1\ Q\ \sigma) \wedge \\
 & & \quad (\neg b \longrightarrow \text{pre } c_2\ Q\ \sigma) \\
\text{pre } (\text{WHILE } b \text{ INV } I \text{ DO } c \text{ OD})\ Q & = & I
\end{array}
$$

Verification Conditions

$\{\text{pre } c \ Q\} \ c \ \{Q\}$ **only true under certain conditions**

Verification Conditions

$\{\text{pre } c \; Q\} \; c \; \{Q\}$ **only true under certain conditions**

These are called **verification conditions** vc c Q:

$$\text{vc SKIP } Q \quad = \quad \text{True}$$

Verification Conditions

$\{\text{pre } c\ Q\}\ c\ \{Q\}$ **only true under certain conditions**

These are called **verification conditions** vc c Q:

$$
\begin{array}{lcl}
\text{vc SKIP } Q & = & \text{True} \\
\text{vc } (x := a)\ Q & = & \text{True}
\end{array}
$$

Verification Conditions

$\{\text{pre } c\ Q\}\ c\ \{Q\}$ **only true under certain conditions**

These are called **verification conditions** vc c Q:

$$
\begin{array}{lcl}
\text{vc SKIP } Q & = & \text{True} \\
\text{vc } (x := a)\ Q & = & \text{True} \\
\text{vc } (c_1; c_2)\ Q & = & \text{vc } c_2\ Q \wedge (\text{vc } c_1\ (\text{pre } c_2\ Q))
\end{array}
$$

Verification Conditions

$\{\text{pre } c\ Q\}\ c\ \{Q\}$ **only true under certain conditions**

These are called **verification conditions** $\text{vc}\ c\ Q$:

$$
\begin{array}{lcl}
\text{vc SKIP } Q & = & \text{True} \\
\text{vc } (x := a)\ Q & = & \text{True} \\
\text{vc } (c_1; c_2)\ Q & = & \text{vc } c_2\ Q \wedge (\text{vc } c_1\ (\text{pre } c_2\ Q)) \\
\text{vc } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2)\ Q & = & \text{vc } c_1\ Q \wedge \text{vc } c_2\ Q
\end{array}
$$

Verification Conditions

$\{\text{pre } c\ Q\}\ c\ \{Q\}$ **only true under certain conditions**

These are called **verification conditions** vc c Q:

$$
\begin{array}{lcl}
\text{vc SKIP } Q & = & \text{True} \\
\text{vc } (x := a)\ Q & = & \text{True} \\
\text{vc } (c_1; c_2)\ Q & = & \text{vc } c_2\ Q \wedge (\text{vc } c_1\ (\text{pre } c_2\ Q)) \\
\text{vc } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2)\ Q & = & \text{vc } c_1\ Q \wedge \text{vc } c_2\ Q \\
\text{vc } (\text{WHILE } b \text{ INV } I \text{ DO } c \text{ OD})\ Q & = & (\forall \sigma.\ I \sigma \wedge b \sigma \longrightarrow \text{pre } c\ I\ \sigma) \wedge \\
 & & (\forall \sigma.\ I \sigma \wedge \neg b \sigma \longrightarrow Q\ \sigma) \wedge \\
 & & \text{vc } c\ I
\end{array}
$$

Verification Conditions

$\{\text{pre } c\ Q\}\ c\ \{Q\}$ **only true under certain conditions**

These are called **verification conditions** vc c Q:

$$
\begin{array}{lcl}
\text{vc SKIP } Q & = & \text{True} \\
\text{vc } (x := a)\ Q & = & \text{True} \\
\text{vc } (c_1; c_2)\ Q & = & \text{vc } c_2\ Q \wedge (\text{vc } c_1\ (\text{pre } c_2\ Q)) \\
\text{vc } (\text{IF } b \text{ THEN } c_1 \text{ ELSE } c_2)\ Q & = & \text{vc } c_1\ Q \wedge \text{vc } c_2\ Q \\
\text{vc } (\text{WHILE } b \text{ INV } I \text{ DO } c \text{ OD})\ Q & = & (\forall \sigma.\ I\sigma \wedge b\sigma \longrightarrow \text{pre } c\ I\ \sigma) \wedge \\
 & & (\forall \sigma.\ I\sigma \wedge \neg b\sigma \longrightarrow Q\ \sigma) \wedge \\
 & & \text{vc } c\ I
\end{array}
$$

$$\text{vc } c\ Q \wedge (P \Longrightarrow \text{pre } c\ Q) \Longrightarrow \{P\}\ c\ \{Q\}$$

Syntax Tricks

- $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Syntax Tricks

- $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Problem: program variables are functions, not values

Syntax Tricks

- $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Problem: program variables are functions, not values

Solution: distinguish program variables syntactically

Syntax Tricks

- ➜ $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- ➜ $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Problem: program variables are functions, not values

Solution: distinguish program variables syntactically

Choices:

- ➜ declare program variables with each Hoare triple

Syntax Tricks

- $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Problem: program variables are functions, not values

Solution: distinguish program variables syntactically

Choices:

- declare program variables with each Hoare triple
  - nice, usual syntax
  - works well if you state full program and only use vcg

Syntax Tricks

- $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Problem: program variables are functions, not values

Solution: distinguish program variables syntactically

Choices:

- declare program variables with each Hoare triple
  - nice, usual syntax
  - works well if you state full program and only use vcg
- separate program variables from Hoare triple (use extensible records), indicate usage as function syntactically

Syntax Tricks

- $x := \lambda\sigma.\ 1$ instead of $x := 1$ sucks
- $\{\lambda\sigma.\ \sigma\ x = n\}$ instead of $\{x = n\}$ sucks as well

Problem: program variables are functions, not values

Solution: distinguish program variables syntactically

Choices:

- declare program variables with each Hoare triple
  - nice, usual syntax
  - works well if you state full program and only use vcg
- separate program variables from Hoare triple (use extensible records), indicate usage as function syntactically
  - more syntactic overhead
  - program pieces compose nicely

Demo

Arrays

Depending on language, model arrays as functions:

➜ Array access = function application:

a[i] = a i

➜ Array update = function update:

a[i] :== v = a :== a(i:= v)

Arrays

Depending on language, model arrays as functions:

- ➜ Array access = function application:

  a[i] = a i

- ➜ Array update = function update:

  a[i] :== v = a :== a(i:= v)

Use lists to express length:

- ➜ Array access = nth:

  a[i] = a ! i

- ➜ Array update = list update:

  a[i] :== v = a :== a[i:= v]

- ➜ Array length = list length:

  a.length = length a

Pointers

Choice 1

$$
\begin{array}{lll}
\textbf{datatype} & \mathsf{ref} & = \mathsf{Ref\ int} \mid \mathsf{Null} \\
\textbf{types} & \mathsf{heap} & = \mathsf{int} \Rightarrow \mathsf{val} \\
\textbf{datatype} & \mathsf{val} & = \mathsf{Int\ int} \mid \mathsf{Bool\ bool} \mid \mathsf{Struct\_x\ int\ int\ bool} \mid \ldots
\end{array}
$$

Pointers

Choice 1

$$
\begin{array}{lll}
\textbf{datatype} & \mathsf{ref} & = \mathsf{Ref\ int} \mid \mathsf{Null} \\
\textbf{types} & \mathsf{heap} & = \mathsf{int} \Rightarrow \mathsf{val} \\
\textbf{datatype} & \mathsf{val} & = \mathsf{Int\ int} \mid \mathsf{Bool\ bool} \mid \mathsf{Struct\_x\ int\ int\ bool} \mid \ldots
\end{array}
$$

- ➜ hp :: heap, p :: ref
- ➜ Pointer access: *p = the_Int (hp (the_addr p))
- ➜ Pointer update: *p :== v = hp :== hp ((the_addr p) := v)

Pointers

Choice 1

datatype ref = Ref int | Null
types heap = int ⇒ val
datatype val = Int int | Bool bool | Struct_x int int bool | ...

- hp :: heap, p :: ref
- Pointer access: *p = the_Int (hp (the_addr p))
- Pointer update: *p :== v = hp :== hp ((the_addr p) := v)

- a bit klunky
- gets even worse with structs
- lots of value extraction (the_Int) in spec and program

Pointers

Choice 2 (Burstall '72, Bornat '00)

Example: struct with next pointer and element

$$\begin{array}{lll} \textbf{datatype} & \text{ref} & = \text{Ref int} \mid \text{Null} \\ \textbf{types} & \text{next\_hp} & = \text{int} \Rightarrow \text{ref} \\ \textbf{types} & \text{elem\_hp} & = \text{int} \Rightarrow \text{int} \end{array}$$

Pointers

Choice 2 (Burstall '72, Bornat '00)

Example: struct with next pointer and element

datatype	ref	= Ref int | Null
types	next_hp	= int ⇒ ref
types	elem_hp	= int ⇒ int

- ➜ next :: next_hp, elem :: elem_hp, p :: ref
- ➜ Pointer access: p→next = next (the_addr p)
- ➜ Pointer update: p→next :== v = next :== next ((the_addr p) := v)

 COMP4161 |

Pointers

Choice 2 (Burstall '72, Bornat '00)

Example: struct with next pointer and element

datatype	ref	$=$ Ref int $\mid$ Null
types	next_hp	$=$ int $\Rightarrow$ ref
types	elem_hp	$=$ int $\Rightarrow$ int

- ➜ next :: next_hp, elem :: elem_hp, p :: ref
- ➜ Pointer access: p$\rightarrow$next $\quad = \quad$ next (the_addr p)
- ➜ Pointer update: p$\rightarrow$next :== v $\quad = \quad$ next :== next ((the_addr p) := v)

In general:

- ➜ a separate heap for each struct field
- ➜ buys you p$\rightarrow$next $\neq$ p$\rightarrow$elem automatically (aliasing)
- ➜ still assumes type safe language

Demo

We have seen today ...

- ➜ Weakest precondition
- ➜ Verification conditions
- ➜ Example program proofs
- ➜ Arrays, pointers

