Axiomatic semantics

Semantics and Application to Program Verification

Antoine Miné

École normale supérieure, Paris
year 2015–2016

Course 6
18 March 2016

Introduction

Operational semantics

Models precisely program execution as low-level transitions between internal states

(transition systems, execution traces, big-step semantics)

Denotational semantics

Maps programs into objects in a mathematical domain

(higher level, compositional, domain oriented)

Aximoatic semantics (today)

Prove properties about programs

- programs are annotated with logical assertions
- a rule-system defines the validity of assertions (logical proofs)
- clearly separates programs from specifications
  (specification $\simeq$ user-provided abstraction of the behavior, it is not unique)
- enables the use of logic tools (partial automation, increased confidence)

Overview

- Specifications (informal examples)
- Floyd–Hoare logic
- Dijkstra's predicate calculus
  (weakest precondition, strongest postcondition)
- Verification conditions
  (partially automated program verification)
- Total correctness (termination)
- Non-determinism
- Arrays
- Concurrency

Specifications

Example: function specification

example in C + ACSL

```
int mod(int A, int B) {
  int Q = 0;
  int R = A;
  while (R >= B) {
    R = R - B;
    Q = Q + 1;
  }
  return R;
}
```

Example: function specification

example in C + ACSL

```
//@ ensures \result == A mod B;
int mod(int A, int B) {
  int Q = 0;
  int R = A;
  while (R >= B) {
    R = R - B;
    Q = Q + 1;
  }
  return R;
}
```

- express the intended behavior of the function (returned value)

Example: function specification

example in C + ACSL

```
//@ requires A>=0 && B>=0;
//@ ensures \result == A mod B;
int mod(int A, int B) {
  int Q = 0;
  int R = A;
  while (R >= B) {
    R = R - B;
    Q = Q + 1;
  }
  return R;
}
```

- express the intended behavior of the function (returned value)
- add requirements for the function to actually behave as intended
  (a requires/ensures pair is a function contract)

Example: function specification

example in C + ACSL

```
//@ requires A>=0 && B>0;
//@ ensures \result == A mod B;
int mod(int A, int B) {
  int Q = 0;
  int R = A;
  while (R >= B) {
    R = R - B;
    Q = Q + 1;
  }
  return R;
}
```

- express the intended behavior of the function (returned value)
- add requirements for the function to actually behave as intended
  (a requires/ensures pair is a function contract)
- strengthen the requirements to ensure termination

Example: program annotations

example with full assertions

```
//@ requires A>=0 && B>0;
//@ ensures \result == A mod B;
int mod(int A, int B) {
  int Q = 0;
  int R = A;
  //@ assert A>=0 && B>0 && Q=0 && R==A;
  while (R >= B) {
    //@ assert A>=0 && B>0 && R>=B && A==Q*B+R;
    R = R - B;
    Q = Q + 1;
  }
  //@ assert A>=0 && B>0 && R>=0 && R<B && A==Q*B+R;
  return R;
}
```

Assertions give detail about the internal computations
why and how contracts are fulfilled

(Note: $r = a \mod b$ means $\exists q$: $a = qb + r \land 0 \leq r < b$)

Example: ghost variables

example with ghost variables

```
//@ requires A>=0 && B>0;
//@ ensures \result == A mod B;
int mod(int A, int B) {

  int R = A;

  while (R >= B) {

    R = R - B;

  }
  // ∃Q: A = QB + R and 0 ≤ R < B
  return R;
}
```

The annotations can be more complex than the program itself

Example: ghost variables

example with ghost variables

```
//@ requires A>=0 && B>0;
//@ ensures \result == A mod B;
int mod(int A, int B) {
  //@ ghost int q = 0;
  int R = A;
  //@ assert A>=0 && B>0 && q=0 && R==A;
  while (R >= B) {
    //@ assert A>=0 && B>0 && R>=B && A==q*B+R;
    R = R - B;
    //@ ghost q = q + 1;
  }
  //@ assert A>=0 && B>0 && R>=0 && R<B && A==q*B+R;
  return R;
}
```

The annotations can be more complex than the program itself and require reasoning on enriched states (ghost variables)

Example: class invariants

example in ESC/Java

```
public class OrderedArray {
  int a[];
  int nb;
  //@invariant nb >= 0 && nb <= 20
  //@invariant (\forall int i; (i >= 0 && i < nb-1) ==> a[i] <= a[i+1])

  public OrderedArray() { a = new int[20]; nb = 0; }

  public void add(int v) {
    if (nb >= 20) return;
    int i; for (i=nb; i > 0 && a[i-1] > v; i--) a[i] = a[i-1];
    a[i] = v; nb++;
  }
}
```

class invariant: property of the fields true outside all methods

it can be temporarily broken within a method
but it must be restored before exiting the method

Language support

Contracts (and class invariants):

- built in few languages (Eiffel)
- available as a library / external tool (C, Java, C#, etc.)

Contracts can be:

- checked dynamically
- checked statically (Frama-C, Why, ESC/Java)
- inferred statically (CodeContracts)

In this course:
deductive methods (logic) to check (prove) statically (at compile-time) partially automatically (with user help) that contracts hold

Floyd–Hoare logic

Hoare triples

Hoare triple: $\{P\}$ *prog* $\{Q\}$

- *prog* is a program fragment
- P and Q are logical assertions over program variables
  (e.g. $P \stackrel{\text{def}}{=} (X \geq 0 \wedge Y \geq 0) \vee (X < 0 \wedge Y < 0)$)

A triple means:

- if P holds before *prog* is executed
- then Q holds after the execution of *prog*
- unless *prog* does not terminate or encounters an error

P is the precondition, Q is the postcondition

$\{P\}$ *prog* $\{Q\}$ expresses partial correctness
(does not rule out errors and non-termination)

Hoare triples serve as judgements in a proof system
(introduced in [Hoare69])

Language

$$\begin{array}{rcll} \mathit{stat} & ::= & X \leftarrow \mathit{expr} & (\mathit{assignment}) \\ & | & \textbf{skip} & (\mathit{do\ nothing}) \\ & | & \textbf{fail} & (\mathit{error}) \\ & | & \mathit{stat};\ \mathit{stat} & (\mathit{sequence}) \\ & | & \textbf{if}\ \mathit{expr}\ \textbf{then}\ \mathit{stat}\ \textbf{else}\ \mathit{stat} & (\mathit{conditional}) \\ & | & \textbf{while}\ \mathit{expr}\ \textbf{do}\ \mathit{stat} & (\mathit{loop}) \end{array}$$

- $X \in \mathbb{V}$: integer-valued variables
- *expr*: integer arithmetic expressions

  we assume that:

  - expressions are deterministic (for now)
  - expression evaluation does not cause error (only **fail** does)

    for instance, to avoid divisions by zero, we assume that all divisions are *explicitly* guarded
    as in : **if** $X = 0$ **then fail else** $\cdots/X\cdots$

Hoare rules: axioms

Axioms:

$$\frac{}{\{P\}\ \textbf{skip}\ \{P\}} \qquad\qquad \frac{}{\{P\}\ \textbf{fail}\ \{Q\}}$$

- any property true before **skip** is true afterwards
- any property is true after **fail**

Hoare rules: axioms

Assignment axiom: $$\frac{}{\{P[e/X]\}\ X \leftarrow e\ \{P\}}$$

for P over X to be true after $X \leftarrow e$
P must be true over e before the assignment

- $P[e/X]$ is P where all free occurrences of X are replaced with e
- e must be deterministic
- the rule is "backwards": P appears as a postcondition

examples:

$\{\text{true}\}\ X \leftarrow 5\ \{X = 5\}$

$\{Y = 5\}\ X \leftarrow Y\ \{X = 5\}$

$\{X + 1 \geq 0\}\ X \leftarrow X + 1\ \{X \geq 0\}$

$\{\text{false}\}\ X \leftarrow Y + 3\ \{Y = 0 \wedge X = 12\}$

$\{Y \in [0, 10]\}\ X \leftarrow Y + 3\ \{X = Y + 3 \wedge Y \in [0, 10]\}$

Hoare rules: consequence

Rule of consequence:

$$\frac{P \Rightarrow P' \qquad Q' \Rightarrow Q \qquad \{P'\}\ c\ \{Q'\}}{\{P\}\ c\ \{Q\}}$$

we can weaken a Hoare triple by:

weakening its postcondition $Q \Leftarrow Q'$

strengthening its precondition $P \Rightarrow P'$

we assume a logic system to be available to prove formulas on assertions, such as $P \Rightarrow P'$ (e.g., arithmetic, set theory, etc.)

examples:

- the axiom for **fail** can be replaced with $\dfrac{}{\{\text{true}\}\ \textbf{fail}\ \{\text{false}\}}$
  (as $P \Rightarrow \text{true}$ and $\text{false} \Rightarrow Q$ always hold)
- $\{X = 99 \wedge Y \in [1,10]\}\ X \leftarrow Y + 10\ \{X = Y + 10 \wedge Y \in [1,10]\}$
  (as $\{Y \in [1,10]\}\ X \leftarrow Y + 10\ \{X = Y + 10 \wedge Y \in [1,10]\}$ and $X = 99 \wedge Y \in [1,10] \Rightarrow Y \in [1,10]$)

Hoare rules: tests

Tests:

$$\frac{\{P \wedge e\}\ s\ \{Q\} \qquad \{P \wedge \neg e\}\ t\ \{Q\}}{\{P\}\ \textbf{if}\ e\ \textbf{then}\ s\ \textbf{else}\ t\ \{Q\}}$$

to prove that Q holds after the test
we prove that it holds after each branch (s, t)
under the assumption that the branch is executed (e, $\neg e$)

example:

$$\frac{\dfrac{\overline{\{X < 0\}\ X \leftarrow -X\ \{X > 0\}}}{\{(X \neq 0) \wedge (X < 0)\}\ X \leftarrow -X\ \{X > 0\}} \qquad \dfrac{\overline{\{X > 0\}\ \textbf{skip}\ \{X > 0\}}}{\{(X \neq 0) \wedge (X \geq 0)\}\ \textbf{skip}\ \{X > 0\}}}{\{X \neq 0\}\ \textbf{if}\ X < 0\ \textbf{then}\ X \leftarrow -X\ \textbf{else skip}\ \{X > 0\}}$$

Hoare rules: sequences

Sequences:

$$\frac{\{P\}\ s\ \{R\} \qquad \{R\}\ t\ \{Q\}}{\{P\}\ s; t\ \{Q\}}$$

to prove a sequence $s; t$
we must invent an intermediate assertion R
implied by P after s, and implying Q after t
(often denoted $\{P\}\ s\ \{R\}\ t\ \{Q\}$)

example:

$\{X = 1 \wedge Y = 1\}\ X \leftarrow X + 1\ \{X = 2 \wedge Y = 1\}\ Y \leftarrow Y - 1\ \{X = 2 \wedge Y = 0\}$

Hoare rules: loops

Loops:

$$\frac{\{P \land e\}\ s\ \{P\}}{\{P\}\ \textbf{while}\ e\ \textbf{do}\ s\ \{P \land \neg e\}}$$

P is a loop invariant :

P holds before each loop iteration, before even testing e

Practical use:

actually, we would rather prove the triple: $\{P\}$ **while** e **do** s $\{Q\}$

it is sufficient to invent an assertion I that:

– holds when the loop start: $P \Rightarrow I$

– is invariant by the body s: $\{I \land e\}\ s\ \{I\}$

– implies the assertion when the loop stops: $(I \land \neg e) \Rightarrow Q$

we can derive the rule:

$$\frac{P \Rightarrow I \qquad I \land \neg e \Rightarrow Q \qquad \dfrac{\{I \land e\}\ s\ \{I\}}{\{I\}\ \textbf{while}\ e\ \textbf{do}\ s\ \{I \land \neg e\}}}{\{P\}\ \textbf{while}\ e\ \textbf{do}\ s\ \{Q\}}$$

Hoare rules: logical part

Hoare logic is parameterized by the choice of logical theory of assertions

the logical theory is used to:

- prove properties of the form $P \Rightarrow Q$ (rule of consequence)
- simplify formulas
  (replace a formula with a simpler one, equivalent in a logical sens: $\Leftrightarrow$)

Examples: (generally first order theories)

- booleans $(\mathbb{B}, \neg, \wedge, \vee)$
- bit-vectors $(\mathbb{B}^n, \neg, \wedge, \vee)$
- Presburger arithmetic $(\mathbb{N}, +)$
- Peano arithmetic $(\mathbb{N}, +, \times)$
- linear arithmetic on $\mathbb{R}$
- Zermelo-Fraenkel set theory $(\in, \{\})$
- theory of arrays (lookup, update)

theories have different expressiveness, decidability and complexity results
this is an important factor when trying to automate program verification

Hoare rules: summary

$$\frac{}{\{P\}\ \textbf{skip}\ \{P\}} \qquad \frac{}{\{\text{true}\}\ \textbf{fail}\ \{\text{false}\}} \qquad \frac{}{\{P[e/X]\}\ X \leftarrow e\ \{P\}}$$

$$\frac{\{P\}\ s\ \{R\} \qquad \{R\}\ t\ \{Q\}}{\{P\}\ s; t\ \{Q\}} \qquad \frac{\{P \wedge e\}\ s\ \{Q\} \qquad \{P \wedge \neg e\}\ t\ \{Q\}}{\{P\}\ \textbf{if}\ e\ \textbf{then}\ s\ \textbf{else}\ t\ \{Q\}}$$

$$\frac{\{P \wedge e\}\ s\ \{P\}}{\{P\}\ \textbf{while}\ e\ \textbf{do}\ s\ \{P \wedge \neg e\}}$$

$$\frac{P \Rightarrow P' \qquad Q' \Rightarrow Q \qquad \{P'\}\ c\ \{Q'\}}{\{P\}\ c\ \{Q\}}$$

Proof tree example

$$s \stackrel{\text{def}}{=} \textbf{while } I < N \textbf{ do } (X \leftarrow 2X;\ I \leftarrow I+1)$$

$$\dfrac{A \qquad B \qquad \dfrac{\dfrac{C \qquad \dfrac{}{\{P_3\}\ X \leftarrow 2X\ \{P_2\}} \qquad \dfrac{}{\{P_2\}\ I \leftarrow I+1\ \{P_1\}}}{\{P_1 \land I < N\}\ X \leftarrow 2X;\ I \leftarrow I+1\ \{P_1\}}}{\{P_1\}\ s\ \{P_1 \land I \geq N\}}}{\{X = 1 \land I = 0 \land N \geq 0\}\ s\ \{X = 2^N \land N = I \land N \geq 0\}}$$

$P_1 \stackrel{\text{def}}{=} X = 2^I \land I \leq N \land N \geq 0$

$P_2 \stackrel{\text{def}}{=} X = 2^{I+1} \land I+1 \leq N \land N \geq 0$

$P_3 \stackrel{\text{def}}{=} 2X = 2^{I+1} \land I+1 \leq N \land N \geq 0 \quad \equiv X = 2^I \land I < N \land N \geq 0$

$A : (X = 1 \land I = 0 \land N \geq 0) \Rightarrow P_1$

$B : (P_1 \land I \geq N) \Rightarrow (X = 2^N \land N = I \land N \geq 0)$

$C : P_3 \iff (P_1 \land I < N)$

Proof tree example

$s \stackrel{\text{def}}{=}$ **while** $I \neq 0$ **do** $I \leftarrow I - 1$

$$\dfrac{\dfrac{\overline{\{\text{true}\}\ I \leftarrow I - 1\ \{\text{true}\}}}{\{I \neq 0\}\ I \leftarrow I - 1\ \{\text{true}\}}}{\dfrac{\{\text{true}\}\ \textbf{while}\ I \neq 0\ \textbf{do}\ I \leftarrow I - 1\ \{\text{true} \wedge \neg(I \neq 0)\}}{\{\text{true}\}\ \textbf{while}\ I \neq 0\ \textbf{do}\ I \leftarrow I - 1\ \{I = 0\}}}$$

- in some cases, the program does not terminate
  (if the program starts with $I < 0$)
- the same proof holds for: $\{\text{true}\}$ **while** $I \neq 0$ **do** $J \leftarrow J - 1$ $\{I = 0\}$
- anything can be proven of a program that never terminates:

$$\dfrac{\dfrac{\overline{\{I = 1 \wedge I \neq 0\}\ J \leftarrow J - 1\ \{I = 1\}}}{\{I = 1\}\ \textbf{while}\ I \neq 0\ \textbf{do}\ J \leftarrow J - 1\ \{I = 1 \wedge I = 0\}}}{\{I = 1\}\ \textbf{while}\ I \neq 0\ \textbf{do}\ J \leftarrow J - 1\ \{\text{false}\}}$$

Invariants and inductive invariants

Example: we wish to prove:

$\{X = Y = 0\}$ **while** $X < 10$ **do** $(X \leftarrow X + 1;\ Y \leftarrow Y + 1)$ $\{X = Y = 10\}$

we need to find an invariant assertion P for the **while** rule

Incorrect invariant: $P \stackrel{\text{def}}{=} X, Y \in [0, 10]$

- P indeed holds at each loop iteration (P is an invariant)
- but $\{P \wedge (X < 10)\}$ $X \leftarrow X + 1;\ Y \leftarrow Y + 1$ $\{P\}$ does not hold

  $P \wedge X < 10$ does not prevent $Y = 10$
  after $Y \leftarrow Y + 1$, P does not hold anymore

Invariants and inductive invariants

Example: we wish to prove:

$$\{X = Y = 0\}\ \textbf{while}\ X < 10\ \textbf{do}\ (X \leftarrow X + 1;\ Y \leftarrow Y + 1)\ \{X = Y = 10\}$$

we need to find an invariant assertion P for the **while** rule

Correct invariant: $P' \stackrel{\text{def}}{=} X \in [0, 10] \wedge X = Y$

- P' also holds at each loop iteration (P' is an invariant)
- $\{P' \wedge (X < 10)\}\ X \leftarrow X + 1;\ Y \leftarrow Y + 1\ \{P'\}$ can be proven
- P' is an **inductive invariant**

  (passes to the induction, stable by a loop iteration)

$\Longrightarrow$

to prove a loop invariant
it is often necessary to find a stronger inductive loop invariant

Auxiliary variables

Auxiliary variables:

mathematical variables that do not appear in the program
they are constant during program execution

Applications:

- simplify proofs
- express more properties (contracts, input-output relations)
- achieve (relative) completeness on extended languages
  (concurrency, recursive procedures)

Example: $\{X = x \wedge Y = y\}$ **if** $X < Y$ **then** $Y \leftarrow X$ **else skip** $\{Y = \min(x, y)\}$

- x and y retain the values of X and Y from the program entry
- $Y = \min(X, Y)$ is much less useful as a specification of a min function
  "$\{\text{true}\}$ **if** $X < Y$ **then** $Y \leftarrow X$ **else skip** $\{Y = \min(X, Y)\}$" holds, but
  "$\{\text{true}\}$ $X \leftarrow Y + 1$ $\{Y = \min(X, Y)\}$" also holds

Link with denotational semantics

Reminder: $\mathsf{S}[\![\, stat \,]\!] : \mathcal{P}(\mathcal{E}) \to \mathcal{P}(\mathcal{E})$ where $\mathcal{E} \stackrel{\text{def}}{=} \mathbb{V} \mapsto \mathbb{I}$

$$\mathsf{S}[\![\, \textbf{skip} \,]\!]\, R \stackrel{\text{def}}{=} R$$

$$\mathsf{S}[\![\, \textbf{fail} \,]\!]\, R \stackrel{\text{def}}{=} \emptyset$$

$$\mathsf{S}[\![\, s_1; s_2 \,]\!] \stackrel{\text{def}}{=} \mathsf{S}[\![\, s_2 \,]\!] \circ \mathsf{S}[\![\, s_1 \,]\!]$$

$$\mathsf{S}[\![\, X \leftarrow e \,]\!]\, R \stackrel{\text{def}}{=} \{\, \rho[X \mapsto v] \mid \rho \in R,\ v \in \mathsf{E}[\![\, e \,]\!]\, \rho \,\}$$

$$\begin{aligned}\mathsf{S}[\![\, \textbf{if } e \textbf{ then } s_1 \textbf{ else } s_2 \,]\!]\, R \stackrel{\text{def}}{=}\ & \mathsf{S}[\![\, s_1 \,]\!]\, \{\, \rho \in R \mid \text{true} \in \mathsf{E}[\![\, e \,]\!]\, \rho \,\} \cup \\ & \mathsf{S}[\![\, s_2 \,]\!]\, \{\, \rho \in R \mid \text{false} \in \mathsf{E}[\![\, e \,]\!]\, \rho \,\}\end{aligned}$$

$$\mathsf{S}[\![\, \textbf{while } e \textbf{ do } s \,]\!]\, R \stackrel{\text{def}}{=} \{\, \rho \in \operatorname{lfp} F \mid \text{false} \in \mathsf{E}[\![\, e \,]\!]\, \rho \,\}$$

where $F(X) \stackrel{\text{def}}{=} R \cup \mathsf{S}[\![\, s \,]\!]\, \{\, \rho \in X \mid \text{true} \in \mathsf{E}[\![\, e \,]\!]\, \rho \,\}$

Theorem

$$\{P\}\ c\ \{Q\} \stackrel{\text{def}}{\iff} \forall R \subseteq \mathcal{E} \colon R \models P \implies \mathsf{S}[\![\, c \,]\!]\, R \models Q$$

($A \models P$ means $\forall \rho \in A$, the formula P is true on the variable assignment ρ)

Link with denotational semantics

- Hoare logic reasons on formulas
- denotational semantics reasons on state sets

we can assimilate assertion formulas and state sets
(logical abuse: we assimilate formulas and models)

let $[R]$ be any formula representing the set R, then:

- $\{[R]\}\ c\ \{[\mathsf{S}[\![\, c \,]\!]\, R]\}$ is always valid
- $\{[R]\}\ c\ \{[R']\} \Rightarrow \mathsf{S}[\![\, c \,]\!]\, R \subseteq R'$

$\implies [\mathsf{S}[\![\, c \,]\!]\, R]$ provides the best valid postcondition

Link with denotational semantics

Loop invariants

- **Hoare:**
  to prove $\{P\}$ **while** e **do** s $\{P \wedge \neg e\}$ we must prove $\{P \wedge e\}$ s $\{P\}$
  i.e., P is an inductive invariant

- **Denotational semantics:**
  we must find lfp F where $F(X) \stackrel{\text{def}}{=} R \cup \mathsf{S}[\![s]\!] \{ \rho \in X \mid \rho \models e \}$
  - lfp $F = \cap \{ X \mid F(X) \subseteq X \}$ (Tarski's theorem)
  - $F(X) \subseteq X \iff ([R] \Rightarrow [X]) \wedge \{[X \wedge e]\}$ s $\{[X]\}$

    $R \subseteq X$ means $[R] \Rightarrow [X]$,
    $\mathsf{S}[\![s]\!] \{ \rho \in X \mid \rho \models e \} \subseteq X$ means $\{[X \wedge e]\}$ s $\{[X]\}$

As a consequence:

- any X such that $F(X) \subseteq X$ gives an inductive invariant
- lfp F gives the best inductive invariant
- any X such that lfp $F \subseteq X$ gives an invariant
  (not necessarily inductive)

(see [Cousot02])

Predicate calculus

Dijkstra's weakest liberal preconditions

Principle: **predicate calculus**

- calculus to derive preconditions from postconditions
- order and mechanize the search for intermediate assertions

  (easier to go backwards, mainly due to assignments)

Weakest liberal precondition $\quad wlp : (prog \times Prop) \to Prop$

$wlp(c, P)$ is the weakest, i.e. most general, precondition
ensuring that $\{wlp(c, P)\}\ c\ \{P\}$ is a Hoare triple

(greatest state set that ensures that the computation ends up in P)

formally: $\quad \{P\}\ c\ \{Q\} \iff (P \Rightarrow wlp(c, Q))$

"liberal" means that we do not care about termination and errors

Examples:

$wlp(X \leftarrow X + 1,\ X = 1) =$
$wlp(\textbf{while}\ X < 0\ X \leftarrow X + 1,\ X \geq 0) =$
$wlp(\textbf{while}\ X \neq 0\ X \leftarrow X + 1,\ X \geq 0) =$

(introduced in [Dijkstra75])

Dijkstra's weakest liberal preconditions

Principle: **predicate calculus**

- calculus to derive preconditions from postconditions
- order and mechanize the search for intermediate assertions

(easier to go backwards, mainly due to assignments)

Weakest liberal precondition $\quad wlp : (prog \times Prop) \to Prop$

$wlp(c, P)$ is the weakest, i.e. most general, precondition ensuring that $\{wlp(c, P)\}\ c\ \{P\}$ is a Hoare triple

(greatest state set that ensures that the computation ends up in P)

formally: $\quad \{P\}\ c\ \{Q\} \iff (P \Rightarrow wlp(c, Q))$

"liberal" means that we do not care about termination and errors

Examples:

$$wlp(X \leftarrow X + 1, X = 1) = (X = 0)$$
$$wlp(\textbf{while } X < 0\ X \leftarrow X + 1, X \geq 0) = \text{true}$$
$$wlp(\textbf{while } X \neq 0\ X \leftarrow X + 1, X \geq 0) = \text{true}$$

(introduced in [Dijkstra75])

A calculus for wlp

wlp is defined by induction on the syntax of programs:

$wlp(\textbf{skip}, P) \stackrel{\text{def}}{=} P$

$wlp(\textbf{fail}, P) \stackrel{\text{def}}{=} \text{true}$

$wlp(X \leftarrow e, P) \stackrel{\text{def}}{=} P[e/X]$

$wlp(s; t, P) \stackrel{\text{def}}{=} wlp(s, wlp(t, P))$

$wlp(\textbf{if } e \textbf{ then } s \textbf{ else } t, P) \stackrel{\text{def}}{=} (e \Rightarrow wlp(s, P)) \wedge (\neg e \Rightarrow wlp(t, P))$

$wlp(\textbf{while } e \textbf{ do } s, P) \stackrel{\text{def}}{=} I \wedge ((e \wedge I) \Rightarrow wlp(s, I)) \wedge ((\neg e \wedge I) \Rightarrow P)$

- $e \Rightarrow Q$ is equivalent to $Q \vee \neg e$
  weakest property that matches Q when e holds
  but says nothing when e does not hold
- **while** loops require providing an invariant predicate I
  intuitively, *wlp* checks that I is an inductive invariant implying P
  if so, it returns I; otherwise, it returns false

  wlp is the weakest precondition only if I is well-chosen...

Wlp computation example

$$
\begin{aligned}
&\textcolor{blue}{wlp}(\textbf{if } X < 0 \textbf{ then } Y \leftarrow -X \textbf{ else } Y \leftarrow X,\ Y \geq 10) = \\
&\quad (X < 0 \Rightarrow \textcolor{blue}{wlp}(Y \leftarrow -X, Y \geq 10)) \wedge (X \geq 0 \Rightarrow \textcolor{blue}{wlp}(Y \leftarrow X, Y \geq 10)) \\
&\quad (X < 0 \Rightarrow -X \geq 10) \wedge (X \geq 0 \Rightarrow X \geq 10) = \\
&\quad (X \geq 0 \vee -X \geq 10) \wedge (X < 0 \vee X \geq 10) = \\
&\quad X \geq 10 \vee X \leq -10
\end{aligned}
$$

wlp generates complex formulas

it is important to simplify them from time to time

Properties of wlp

- $\color{blue}{wlp}(c, \text{false}) \equiv \text{false}$ (excluded miracle)
- $\color{blue}{wlp}(c, P) \land \color{blue}{wlp}(\cancel{d}\,c, Q) \equiv \color{blue}{wlp}(c, P \land Q)$ (distributivity)
- $\color{blue}{wlp}(c, P) \lor \color{blue}{wlp}(\cancel{d}\,c, Q) \equiv \color{blue}{wlp}(c, P \lor Q)$ (distributivity)

  ($\Rightarrow$ always true, $\Leftarrow$ only true for deterministic, error-free programs)
- if $P \Rightarrow Q$, then $\color{blue}{wlp}(c, P) \Rightarrow \color{blue}{wlp}(c, Q)$ (monotonicity)

$A \equiv B$ means that the formulas A and B are equivalent
i.e., $\forall \rho$: $\rho \models A \iff \rho \models B$

(stronger that syntactic equality)

Strongest liberal postconditions

we can define $slp : (Prop \times prog) \to Prop$

- $\{P\}\ c\ \{slp(P,c)\}$ (postcondition)
- $\{P\}\ c\ \{Q\} \iff (slp(P,c) \Rightarrow Q)$ (strongest postcondition)
  (corresponds to the smallest state set)
- $slp(P,c)$ does not care about non-termination (liberal)
- allows forward reasoning

we have a duality:

$$(P \Rightarrow wlp(c,Q)) \iff (slp(P,c) \Rightarrow Q)$$

proof: $(P \Rightarrow wlp(c,Q)) \iff \{P\}\ c\ \{Q\} \iff (slp(P,c) \Rightarrow Q)$

Calculus for slp

$$slp(P, \textbf{skip}) \stackrel{\text{def}}{=} P$$

$$slp(P, \textbf{fail}) \stackrel{\text{def}}{=} \text{false}$$

$$slp(P, X \leftarrow e) \stackrel{\text{def}}{=} \exists v\colon P[v/X] \land X = e[v/X]$$

$$slp(P,\ s; t) \stackrel{\text{def}}{=} slp(slp(P, s), t)$$

$$slp(P,\ \textbf{if } e \textbf{ then } s \textbf{ else } t) \stackrel{\text{def}}{=} slp(P \land e, s) \lor slp(P \land \neg e, t)$$

$$slp(P,\ \textbf{while } e \textbf{ do } s) \stackrel{\text{def}}{=} (P \Rightarrow I) \land (slp(I \land e, s) \Rightarrow I) \land (\neg e \land I)$$

(the rule for $X \leftarrow e$ makes *slp* much less attractive than *wlp*)

Verification conditions

Verification condition approch to program verification

How can we automate program verification using logic?

- Hoare logic: deductive system
  can only automate the checking of proofs
- predicate transformers: *wlp*, *slp* calculus
  construct (big) formulas mechanically
  invention is still needed for loops
- verification condition generation
  take as input a program with annotations
  (at least contracts and loop invariants)

  generate mechanically logic formulas ensuring the correctness
  (reduction to a mathematical problem, no longer any reference to a program)

  use an automatic SAT/SMT solver to prove (discharge) the formulas
  or an interactive theorem prover

(the idea of logic-based automated verification appears as early as [King69])

Language

$$\begin{array}{lcl} stat & ::= & X \leftarrow expr \\ & | & \textbf{skip} \\ & | & stat;\ stat \\ & | & \textbf{if}\ expr\ \textbf{then}\ stat\ \textbf{else}\ stat \\ & | & \textbf{while}\ \{Prop\}\ expr\ \textbf{do}\ stat \\ & | & \textbf{assert}\ expr \end{array}$$

$$prog \quad ::= \quad \{Prop\}\ stat\ \{Prop\}$$

- loops are annotated with loop invariants
- optional assertions at any point
- programs are annotated with a contract
  (precondition and postcondition)

Verification condition generation algorithm

$\underline{\text{vcg}_p : prog \rightarrow \mathcal{P}(Prop)}$

$\text{vcg}_p(\{P\}\ c\ \{Q\}) \stackrel{\text{def}}{=} \text{let } (R, C) = \text{vcg}_s(c,\ Q) \text{ in } C \cup \{P \Rightarrow R\}$

$\underline{\text{vcg}_s : (stat \times Prop) \rightarrow (Prop \times \mathcal{P}(Prop))}$

$\text{vcg}_s(\textbf{skip},\ Q) \stackrel{\text{def}}{=} (Q, \emptyset)$

$\text{vcg}_s(X \leftarrow e,\ Q) \stackrel{\text{def}}{=} (Q[e/X], \emptyset)$

$\text{vcg}_s(s; t,\ Q) \stackrel{\text{def}}{=} \text{let } (R, C) = \text{vcg}_s(t,\ Q) \text{ in let } (P, D) = \text{vcg}_s(s,\ R) \text{ in } (P, C \cup D)$

$\text{vcg}_s(\textbf{if } e \textbf{ then } s \textbf{ else } t,\ Q) \stackrel{\text{def}}{=}$

$\quad \text{let } (S, C) = \text{vcg}_s(s,\ Q) \text{ in let } (T, D) = \text{vcg}_s(t,\ Q) \text{ in}$

$\quad ((e \Rightarrow S) \wedge (\neg e \Rightarrow T), C \cup D)$

$\text{vcg}_s(\textbf{while } \{I\}\ e \textbf{ do } s,\ Q) \stackrel{\text{def}}{=}$

$\quad \text{let } (R, C) = \text{vcg}_s(s,\ I) \text{ in } (I, C \cup \{(I \wedge e) \Rightarrow R, (I \wedge \neg e) \Rightarrow Q\})$

$\text{vcg}_s(\textbf{assert } e,\ Q) \stackrel{\text{def}}{=} (e \Rightarrow Q, \emptyset)$

We use *wlp* to infer assertions automatically when possible.

$\text{vcg}_s(c, P) = (P', C)$ propagates postconditions backwards
and accumulates into C verification conditions (from loops).

Verification condition generation example

Consider the program:

$$\begin{array}{ll} \{N \geq 0\} & X \leftarrow 1; I \leftarrow 0; \\ & \textbf{while } \{X = 2^I \land 0 \leq I \leq N\} \; I < N \textbf{ do} \\ & \qquad (X \leftarrow 2X;\; I \leftarrow I + 1) \\ \{X = 2^N\} & \end{array}$$

we get three verification conditions:

$$C_1 \stackrel{\text{def}}{=} (X = 2^I \land 0 \leq I \leq N) \land I \geq N \Rightarrow X = 2^N$$

$$C_2 \stackrel{\text{def}}{=} (X = 2^I \land 0 \leq I \leq N) \land I < N \Rightarrow 2X = 2^{I+1} \land 0 \leq I + 1 \leq N$$

(from $(X = 2^I \land 0 \leq I \leq N)[I + 1/I, 2X/X]$)

$$C_3 \stackrel{\text{def}}{=} N \geq 0 \Rightarrow 1 = 2^0 \land 0 \leq 0 \leq N$$

(from $(X = 2^I \land 0 \leq I \leq N)[0/I, 1/X]$)

which can be checked independently

What about real languages?

In a real language such as C, the rules are not so simple

Example: the assignment rule $\dfrac{}{\{P[e/X]\}\ X \leftarrow e\ \{P\}}$

requires that

- e has no effect (memory write, function calls)
- there is no pointer aliasing
- e has no run-time error

moreover, the operations in the program and in the logic may not match:

- integers: logic models $\mathbb{Z}$, computers use $\mathbb{Z}/2^n\mathbb{Z}$ (wrap-around)
- continuous:
  logic models $\mathbb{Q}$ or $\mathbb{R}$, programs use floating-point numbers
  (rounding error)
- a logic for pointers and dynamic allocation is also required
  (separation logic)

(see for instance the tool Why, to see how some problems can be circumvented)

Termination

Total correctness

Hoare triple: $[P]$ *prog* $[Q]$

- if P holds before *prog* is executed
- then *prog* always terminates
- and Q holds after the execution of *prog*

Rules: we only need to change the rule for **while**

$$\frac{\forall t \in W\colon [P \land e \land u = t]\ s\ [P \land u \prec t]}{[P]\ \textbf{while}\ e\ \textbf{do}\ s\ [P \land \neg e]} \quad ((W,\prec) \text{ is well-founded})$$

- $(W,\prec)$ well-founded $\overset{\text{def}}{\iff}$ every $V \subseteq W$, $V \neq \emptyset$ has a minimal element for $\prec$

  ensures that we cannot decrease infinitely by $\prec$ in W
  generally, we simply use $(\mathbb{N}, <)$
  (also useful: lexicographic orders, ordinals)

- in addition to the loop invariant P
  we invent an expression u that strictly decreases by s

  u is called a "ranking function"
  often $\neg e \implies u = 0$: u counts the number of steps until termination

Total correctness

To simplify, we can decompose a proof of total correctness into:

- a proof of partial correctness $\{P\}\ c\ \{Q\}$
  ignoring termination
- a proof of termination $[P]\ c\ [\text{true}]$
  ignoring the specification

  we must still include the precondition P
  as the program may not terminate for all inputs

indeed, we have: $$\frac{\{P\}\ c\ \{Q\} \qquad [P]\ c\ [\text{true}]}{[P]\ c\ [Q]}$$

Total correctness example

We use a simpler rule for integer ranking functions $((W, \prec) \stackrel{\text{def}}{=} (\mathbb{N}, \leq))$ using an integer expression r over program variables:

$$\frac{\forall n\colon [P \wedge e \wedge (r = n)]\ s\ [P \wedge (r < n)] \qquad (P \wedge e) \Rightarrow (r \geq 0)}{[P]\ \textbf{while}\ e\ \textbf{do}\ s\ [P \wedge \neg e]}$$

Example: $p \stackrel{\text{def}}{=} \textbf{while}\ I < N\ \textbf{do}\ I \leftarrow I + 1;\ X \leftarrow 2X\ \textbf{done}$

we use $r \stackrel{\text{def}}{=} N - I$ and $P \stackrel{\text{def}}{=}$ true

$$\frac{\begin{array}{c}\forall n\colon [I < N \wedge N - I = n]\ I \leftarrow I + 1;\ X \leftarrow 2X\ [N - I = n - 1] \\ I < N \Rightarrow N - I \geq 0\end{array}}{[\text{true}]\ p\ [I \geq N]}$$

Weakest precondition

Weakest precondition $wp(prog, Prop) : Prop$

- similar to *wlp*, but also additionally imposes termination
- $[P]\ c\ [Q] \iff (P \Rightarrow wp(c, Q))$

As before, only the definition for **while** needs to be modified:

$$\begin{aligned} wp(\textbf{while } e \textbf{ do } s,\ P) \stackrel{\text{def}}{=}\ & I \land \\ & (I \Rightarrow v \geq 0) \land \\ & \forall n: ((e \land I \land v = n) \Rightarrow wp(s, I \land v < n)) \land \\ & ((\neg e \land I) \Rightarrow P) \end{aligned}$$

the invariant predicate I is combined with a variant expression v

v is positive (this is an invariant: $I \Rightarrow v \geq 0$)

v decreases at each loop iteration

and similarly for strongest postconditions

Non-determinism

Non-determinism in Hoare logic

We model non-determinism with the statement $X \leftarrow ?$
meaning: X is assigned a random value

($X \leftarrow [a, b]$ can be modeled as: $X \leftarrow ?; \textbf{if } X < a \vee X > b \textbf{ then fail};$)

Hoare axiom: $$\frac{}{\{\forall X\colon P\}\ X \leftarrow ?\ \{P\}}$$

if P is true after assigning X to random
then P must hold whatever the value of X before

often, X does not appear in P and we get simply: $\frac{}{\{P\}\ X \leftarrow ?\ \{P\}}$

Example:

$$\frac{\{Y = x\}\ X \leftarrow ?\ \{Y = x\} \qquad \dfrac{\{X = x\}\ Y \leftarrow X\ \{Y = x\}}{\{Y = x\}\ X \leftarrow Y\ \{X = x\}}}{\{X = x\}\ Y \leftarrow X; X \leftarrow ?; X \leftarrow Y\ \{X = x\}}$$

Non-determinism in predicate calculus

Predicate transformers:

- $wlp(X \leftarrow ?,\ P) \stackrel{\text{def}}{=} \forall X: P$

  (P must hold whatever the value of X before the assignment)

- $slp(P,\ X \leftarrow ?) \stackrel{\text{def}}{=} \exists X: P$

  (if P held for one value of X, $\exists x.P$ holds for all values of X after the assignment)

Link with operational semantics (as transition systems)

predicates P as sets of states $P \subseteq \Sigma$
commands c as transition relations $c \subseteq \Sigma \times \Sigma$

we define:

$$\text{post}[\tau](P) \stackrel{\text{def}}{=} \{\, \sigma' \mid \exists \sigma \in P: (\sigma, \sigma') \in \tau \,\}$$

$$\widetilde{\text{pre}}[\tau](P) \stackrel{\text{def}}{=} \{\, \sigma \mid \forall \sigma' \in \Sigma: (\sigma, \sigma') \in \tau \implies \sigma' \in P \,\}$$

then:

$$slp(P, c) = \text{post}[c](P)$$

$$wlp(c, P) = \widetilde{\text{pre}}[c](P)$$

Arrays

Array syntax

We enrich our language with:

- a set $\mathbb{A}$ of array variables
- array access in expressions: $A(expr)$, $A \in \mathbb{A}$
- array assignment: $A(expr) \leftarrow expr$, $A \in \mathbb{A}$
  (arrays have unbounded size here, we do not care about overflow)

Issue:

a natural idea is to generalize the assignment axiom:

$$\frac{}{\{P[f/A(e)]\}\ A(e) \leftarrow f\ \{P\}}$$

but this is not sound, due to aliasing

example:

we would derive the invalid triple: $\{A(J) = 1 \wedge I = J\}\ A(I) \leftarrow 0\ \{A(J) = 1 \wedge I = J\}$
as $(A(J) = 1)[0/A(I)] = (A(J) = 1)$

Hoare logic rule for arrays

Solution: use a specific theory of arrays (McCarthy 1962)

- enrich the assertion language with expressions $A\{e \mapsto f\}$

  meaning: the array equal to A except that index e maps to value f

- add the axiom $$\overline{\{P[A\{e \mapsto f\}/A]\}\ A(e) \leftarrow f\ \{P\}}$$

  intuitively, we use "functional arrays" in the logic world

- add logical axioms to reason about our arrays in assertions

$$\overline{A\{e \mapsto f\}(e) = f} \qquad \overline{(e \neq e') \Rightarrow (A\{e \mapsto f\}(e') = A(e'))}$$

Arrays: example

Example: swap

given the program $p \stackrel{\text{def}}{=} T \leftarrow A(I);\ A(I) \leftarrow A(J);\ A(J) \leftarrow T$

we wish to prove: $\{A(I) = x \wedge A(J) = y\}\ p\ \{A(I) = y \wedge A(J) = x\}$

by propagating $A(I) = y$ backwards by the assignment rule, we get

$A\{\,J \mapsto T\,\}(I) = y$
$A\{\,I \mapsto A(J)\,\}\{\,J \mapsto T\,\}(I) = y$
$A\{\,I \mapsto A(J)\,\}\{\,J \mapsto A(I)\,\}(I) = y$

we consider two cases:

if $I = J$, then $A\{\,I \mapsto A(J)\,\}\{\,J \mapsto A(I)\,\} = A$
so, $A\{\,I \mapsto A(J)\,\}\{\,J \mapsto A(I)\,\}(I) = A(I) = A(J)$

if $I \neq J$, then $A\{\,I \mapsto A(J)\,\}\{\,J \mapsto A(I)\,\}(I) = A\{\,I \mapsto A(J)\,\}(I) = A(J)$

in both cases, we get $A(J) = y$ in the precondition

likewise, $A(I) = x$ in the precondition

Concurrent programs

Concurrent program syntax

Language

add a parallel composition statement: *stat* $||$ *stat*

semantics: $s_1 \,||\, s_2$

- execute s_1 and s_2 in parallel
- allowing an arbitrary interleaving of atomic statements
  (expression evaluation or assignments)
- terminates when both s_1 and s_2 terminate

Hoare logic: extended by Owicki and Gries [Owicki76]

first idea:
$$\frac{\{P_1\}\ s_1\ \{Q_1\} \qquad \{P_2\}\ s_2\ \{Q_2\}}{\{P_1 \wedge P_2\}\ s_1 \,||\, s_2\ \{Q_1 \wedge Q_2\}}$$

but this is unsound

Concurrent programs: rule soundness

Issue:

$$\frac{\{P_1\}\ s_1\ \{Q_1\} \qquad \{P_2\}\ s_2\ \{Q_2\}}{\{P_1 \wedge P_2\}\ s_1 \mid\mid s_2\ \{Q_1 \wedge Q_2\}}$$ is not always sound

example:

given $s_1 \stackrel{\text{def}}{=} X \leftarrow 1$ and $s_2 \stackrel{\text{def}}{=}$ **if** $X = 0$ **then** $Y \leftarrow 1$, we derive:

$$\frac{\overline{\{X = Y = 0\}\ s_1\ \{X = 1 \wedge Y = 0\}} \qquad \overline{\{X = Y = 0\}\ s_2\ \{X = 0 \wedge Y = 1\}}}{\{X = Y = 0\}\ s_1 \mid\mid s_2\ \{\text{false}\}}$$

Solution:

the proofs of $\{P_1\}\ s_1\ \{Q_1\}$ and $\{P_2\}\ s_2\ \{Q_2\}$ must not interfere

Concurrent programs: rule soundness

interference freedom

given proofs Δ_1 and Δ_2 of $\{P_1\}\ s_1\ \{Q_1\}$ and $\{P_2\}\ s_2\ \{Q_2\}$

Δ_1 does not interfere with Δ_2 if:

for any Φ appearing before a statement in Δ_1
for any $\{P_2'\}\ s_2'\ \{Q_2'\}$ appearing in Δ_2
$\{\Phi \wedge P_2'\}\ s_2'\ \{\Phi\}$ holds
and moreover $\{Q_1 \wedge P_2'\}\ s_2'\ \{Q_1\}$

i.e.: the assertions used to prove $\{P_1\}\ s_1\ \{Q_1\}$ are stable by s_2

example:

given $s_1 \stackrel{\text{def}}{=} X \leftarrow 1$ and $s_2 \stackrel{\text{def}}{=}$ **if** $X = 0$ **then** $Y \leftarrow 1$, we derive:

$$\dfrac{\overline{\{X = 0 \wedge Y \in [0,1]\}\ s_1\ \{X = 1 \wedge Y \in [0,1]\}} \quad \overline{\{X \in [0,1] \wedge Y = 0\}\ s_2\ \{X \in [0,1] \wedge Y \in [0,1]\}}}{\{X = Y = 0\}\ s_1 \,||\, s_2\ \{X = 1 \wedge Y \in [0,1]\}}$$

Concurrent programs: rule completeness

Issue: incompleteness

$\{X = 0\}\ X \leftarrow X + 1 \mid\mid X \leftarrow X + 1\ \{X = 2\}$ is valid

but no proof of it can be derived

Solution: auxiliary variables

introduce explicitly program points and program counters

example:

$^{\ell 1}\, X \leftarrow X + 1\, ^{\ell 2} \mid\mid {}^{\ell 3}\, X \leftarrow X + 1\, ^{\ell 4}$

with auxiliary variables $pc_1 \in \{1, 2\}$, $pc_2 \in \{3, 4\}$

we can now express that a process is at a given control point
and distinguish assertions based on the location of other processes

$s_1 \stackrel{\text{def}}{=} {}^{\ell 1}\, X \leftarrow X + 1\, ^{\ell 2}$, $s_2 \stackrel{\text{def}}{=} {}^{\ell 3}\, X \leftarrow X + 1\, ^{\ell 4}$

$\{(pc_2 = 3 \wedge X = 0) \vee (pc_2 = 4 \wedge X = 1)\}\ s_1\ \{(pc_2 = 3 \wedge X = 1) \vee (pc_2 = 4 \wedge X = 2)\}$

$\{(pc_1 = 1 \wedge X = 0) \vee (pc_1 = 2 \wedge X = 1)\}\ s_2\ \{(pc_1 = 1 \wedge X = 1) \vee (pc_1 = 2 \wedge X = 2)\}$

$\Longrightarrow \{pc_1 = 1 \wedge pc_2 = 3 \wedge X = 0\}\ s_1 \mid\mid s_2\ \{pc_1 = 2 \wedge pc_2 = 4 \wedge X = 1\}$

in fact, auxiliary variables make the proof method complete

Conclusion

Conclusion

- logic allows us to reason about program correctness
- verification can be reduced to proofs of simple logic statements

Issue: automation

- annotations are required (loop invariants, contracts)
- verification conditions must be proven

to scale up to realistic programs, we need to automate as much as possible

Some solutions:

- automatic logic solvers to discharge proof obligations
  SAT / SMT solvers
- abstract interpretation to approximate the semantics
  - fully automatic
  - able to infer invariants

Bibliography

[Apt81] **K. Apt**. *Ten Years of Hoare's logic: A survey* In ACM TOPLAS, 3(4):431–483, 1981.

[Cousot02] **P. Cousot**. *Constructive design of a hierarchy of semantics of a transition system by abstract interpretation.* In TCS, 277(1–2):47–103, 2002.

[Dijkstra76] **E.W. Dijkstra**. *Guarded commands, nondeterminacy and formal derivation of program* In Comm. ACM, 18(8):453–457, 1975.

[Floyd67] **R. Floyd**. *Assigning meanings to programs* In In Proc. Sympos. Appl. Math., Vol. XIX, pages 19–32, 1967.

[Hoare69] **C.A.R. Hoare**. *An axiomatic basis for computer programming* In Commun. ACM 12(10), 1969.

[King69] **J.C. King**. *A program verifier* In PhD thesis, Dept. of Computer Science, Carnegie-Mellon University, 1969.

[Owicki76] **S. Owicki & D. Gries**. *An axiomatic proof technique for parallel programs I* In Acta Informatica, 6(4):319–340, 1976.