Logic for Verification 1a

Nisansala Yatapanage
ANU Logic Summer School

My Background

80’s and 90’s – logic puzzles, BASIC programming.

BE in Software Engineering, UQ.

2004 – Research in formal methods, UQ and Griffith.

PhD, Griffith Uni.

Research in concurrency, Newcastle Uni, U.K.

Lecturer, De Montfort Uni, U.K.

Back home in Australia – ANU.

https://users.cecs.anu.edu.au/Nisansala.Yatapanage

What is verification?

Verification allows us to ensure that a program is correct according to its specification.

It's different to testing – testing cannot prove the absence of errors.

Types of verification include:

- model checking (automatically search the whole state space),
- program reasoning approaches (using theorem proving or manual reasoning).

Why do we need verification?

There are many examples of software that has gone wrong.

Some systems require a high degree of assurance, e.g. safety-critical systems, such as air-traffic control and industrial systems.

Other systems have security concerns, e.g. financial systems.

Even small, simple programs can have unexpected behaviour if the code and design are not verified properly.

Lecture Plan

Wednesday lectures: Hoare logic, concurrency, rely/guarantee.

Thursday lectures: Rely/guarantee, examples – concurrent garbage collection, problems with full separation vs. problems with interference.

Friday lectures: Temporal logic (LTL), model checking, verifying safety-critical applications including failure analysis.

Hoare Logic

A Hoare triple consists of:

- an assertion (pre condition p),
- an assertion (post condition q) and
- a program statement, S.

$$\{p\}\ S\ \{q\}$$

Hoare Triples

Examples:

$\{x = 0\}\ \ x := x + 1\ \ \{x = 1\}$

$\{x = 2 \wedge y = 4\}\ \ x := y\ \ \{x = 4\}$

$\{x = 2 \wedge y = 4\}\ \ x := y - 1\ \ \{x = 3\}$

Rules

$$\frac{\text{premise}}{\text{conclusion}}$$

If the premise holds, then the conclusion holds.

Assignment

Axiom of Assignment

$$\frac{}{\{P[e\backslash v]\}\ v := e\ \{P\}}$$

Example: To show: $\{x = 2\}\ \ x := x + 3\ \ \{x = 5\}$

$$\{x + 3 = 5\}\ \ x := x + 3\ \ \{x = 5\}$$

$$\{x = 2\}\ \ x := x + 3\ \ \{x = 5\}$$

Sequential Composition

Rule of Composition

$$\frac{\{P\}\ S\ \{R\} \qquad \{R\}\ T\ \{Q\}}{\{P\}\ S; T\ \{Q\}}$$

Example: To show: $\{x = 2 \wedge y = 4\}\ \ y := y + 1; x := y\ \{x = 5 \wedge y = 5\}$

$\{y = 5\}\ x := y\ \ \{x = 5 \wedge y = 5\}$ by the assignment axiom.

$\{x = 2 \wedge y = 5\}\ x := y\ \ \{x = 5 \wedge y = 5\}$ by the rule of consequence.

$\{x = 2 \wedge y = 4\}\ \ y := y + 1\ \ \{x = 2 \wedge y = 5\}$ by the assignment axiom.

Strengthening pre conditions and weakening post conditions

Rule of Consequence:

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

Example: To show: $\{x = 2\}\ \ x := x + 3\ \ \{x > 0\}$

$\{x = 2\}\ \ x := x + 3\ \ \{x = 5\}$ by the assignment axiom.

$\{x = 2\}\ \ x := x + 3\ \ \{x > 0\}$ by the rule of consequence.

Strengthening pre conditions and weakening post conditions

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

Example: To show: $\{x = 2 \land y = 4\}\ \ y := y + 1;\ x := y\ \{x = 5 \land y = 5\}$

$\{y = 5\}\ x := y\ \ \{x = 5 \land y = 5\}$ by the assignment axiom.

$\{x = 2 \land y = 5\}\ x := y\ \ \{x = 5 \land y = 5\}$ by the rule of consequence.

$\{x = 2 \land y = 4\}\ \ y := y + 1\ \ \{x = 2 \land y = 5\}$ by the assignment axiom.

While Rule

Rule of Iteration:

$$\frac{\{I \wedge C\}\ S\ \{I\}}{\{I\}\ \text{While } C\ \{\ S\ \}\ \{I \wedge \neg C\}}$$

- Need to find an *invariant* – it should hold every time the loop runs, i.e. $\{I \wedge C\}\ S\ \{I\}$

Note: Using the Rule of Consequence, we can show:

$\{P\}$ While C do S od $\{Q\}$ if $P \Rightarrow I$ and $I \wedge \neg C \Rightarrow Q$.

While Rule

$\{x \geq 0 \wedge x = x_0\}$

```
y = 0;
while(x > 0) {
        y = y + x;
        x = x – 1;
}
```

$\{x = 0 \wedge y = x_0(x_0 + 1) / 2\}$

What is the invariant?

$y = 0; x = 5$

$y = 5; x = 4$

$y = 5 + 4; x = 3$

$y = 5 + 4 + 3; x = 2$

$y = 5 + 4 + 3 + 2; x = 1$

$y = 5 + 4 + 3 + 2 + 1; x = 0$

While Rule

What is the invariant?

$y = 0; x = 5$

$y = 5; x = 4$

$y = 5 + 4; x = 3$

$y = 5 + 4 + 3; x = 2$

$y = 5 + 4 + 3 + 2; x = 1$

$y = 5 + 4 + 3 + 2 + 1; x = 0$

Invariant: $(y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \wedge x \geq 0$

While Rule

Proof of $\{I \wedge C\}\ S\ \{I\}$:

$\{I \wedge C\}\ y := y + x;\ x := x - 1\ \{I\}$

$\{(y = x_0(x_0 + 1) / 2 - (x - 1)(x - 1 + 1) / 2) \wedge (x - 1) \geq 0\}$

$x := x - 1$

$\{(y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \wedge x \geq 0\}$

by the assignment axiom.

$\{(y = x_0(x_0 + 1) / 2 - (x - 1)(x - 1 + 1) / 2) \wedge (x - 1) \geq 0\}$

$\equiv \{(y = x_0(x_0 + 1) / 2 - x(x - 1) / 2) \wedge (x - 1) \geq 0\}$

$\equiv \{(y = x_0(x_0 + 1) / 2 - x(x - 1) / 2) \wedge x \geq 1\}$

While Rule

$\{(y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \land x \geq 0\}$

$y := y + x$

$\{y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \land x \geq 1\}$

Using the assignment axiom:

$\{y + x = x_0(x_0 + 1) / 2 - x(x - 1) / 2) \land x \geq 1\}$

$\equiv y = x_0(x_0 + 1) / 2 - x(x - 1) / 2 - x \land x \geq 1$

$\equiv y = x_0(x_0 + 1) / 2 - (x(x - 1) + 2x) / 2 \land x \geq 1$

$\equiv y = x_0(x_0 + 1) / 2 - (x^2 - x + 2x) / 2 \land x \geq 1$

$\equiv y = x_0(x_0 + 1) / 2 - (x^2 - x) / 2 \land x \geq 1$

$\equiv y = x_0(x_0 + 1) / 2 - x(x + 1) / 2 \land x \geq 0$

$x \geq 1 \Rightarrow x \geq 0$

While Rule

Proof of $I \wedge \neg C \Rightarrow Q$:

$\neg C$

$$(y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \wedge x \geq 0 \wedge x \leq 0$$

$$\equiv (y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \wedge x = 0$$

$$\equiv (y = x_0(x_0 + 1) / 2) \quad \text{because } x = 0$$

While Rule

$\{x \geq 0 \wedge x = x_0\}\ y := 0\ \{(y = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \wedge x \geq 0\}$

Using the assignment axiom:

$(0 = x_0(x_0 + 1) / 2 - x(x + 1) / 2) \wedge x \geq 0$

$\equiv (x_0(x_0 + 1) / 2 = x(x + 1) / 2) \wedge x \geq 0$

$\equiv x = x_0 \wedge x \geq 0$

While Rule

Therefore, by the Rule of Consequence:

$\{x \geq 0 \wedge x = x_0\}$

y = 0;

while(x > 0) do

    y = y + x;

    x = x – 1;

od

Exercise

Prove the following Hoare triple:

$$\{x = m \wedge m \geq 0 \wedge y = 1 \wedge z \neq 0\}$$

while $x > 0$ do

$y := y * z;$

$x := x - 1$

od

$$\{x = 0 \wedge m \geq 0 \wedge y = z^m \wedge z \neq 0\}$$

This problem is from:

de Roever, W.-P. *Concurrency. Introduction to Compositional and Non-compositional Methods*, Cambridge University Press, 2001. (Chapter 9 exercises).