Mechanising Hoare Logic

Given a Hoare triple ($\{\varphi\}C\{\psi\}$) rules are applied from the conclusion, assuming that the side conditions hold.

- If all side conditions hold, a proof can be build;
- If some side condition does not hold, the derivation tree is not a valid deduction, but is there an alternative derivation?

There is a strategy to build the derivation trees such that we can conclude (if some side conditions does not hold) that there is no derivation for the given Hoare triple.

Tableaux

- The tableaux system allows to obtain the derivation of a Hoare triple, that is the conclusion.
- The derivation is valid if the verification conditions are satisfiable.
- But if they are not, how to ensure that there is no other derivation?
- If there is no determinism one cannot mechanise the Hoare logic.
- We will see that the tableaux ensure that if the verification conditions are not satisfiable *no other* derivation exists.
- and the tableaux can be automated.

Subformula property and Ambiguity

Most rules of Hoare logic have the *subformula property*:

> *all the assertions that occur in the premises of a rule also occur in its conclusion.*

The exceptions are:

- The rule *comp*, which requires an intermediate condition;
- The rule *cons*, where the precondition and the postcondition must be guessed.

Other property that we want is that the choice of the rules is non ambiguous, but:

- The rule *cons*, can be applied to any Hoare triple. Thus it should be removed.

Hoare logic without the rule *cons*: system $\mathcal{H}_g$

$$\frac{}{\{\varphi\}\,\mathsf{skip}\,\{\psi\}} \text{ if } \models \varphi \to \psi$$

$$\frac{}{\{\varphi\}\,x \leftarrow E\,\{\psi\}} \text{ if } \models \varphi \to \psi[E/x]$$

$$\frac{\{\varphi\}\,C_1\,\{\eta\} \qquad \{\eta\}\,C_2\,\{\psi\}}{\{\varphi\}\,C_1; C_2\,\{\psi\}}$$

$$\frac{\{\varphi\ \wedge\ B\}\,C_1\,\{\psi\} \qquad \{\varphi\ \wedge\ \neg B\}\,C_2\,\{\psi\}}{\{\varphi\}\,\texttt{if}\,B\,\texttt{then}\,C_1\,\texttt{else}\,C_2\,\{\psi\}}$$

$$\frac{\{\eta\ \wedge\ B\}\,C\,\{\eta\}}{\{\varphi\}\,\texttt{while}\,B\,\texttt{do}\,\{\eta\}C\,\{\psi\}} \text{ if } \models \varphi \to \eta \text{ and } \models \eta\ \wedge\ \neg B \to \psi$$

In the $while_p$ rule the loop is annotated with the invariant η, to keep the subformula property. .

We can show that the *cons* is derivable in $\mathcal{H}_g$. Let Γ be a set of assertions.

Lema 7.1. *If* $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}$ *and* $\models \varphi' \to \varphi$, $\models \psi \to \psi'$, *then* $\Gamma \vdash_{\mathcal{H}_g} \{\varphi'\}C\{\psi'\}$.

Proof: By induction on the derivation of $\Gamma \vdash_{\mathcal{H}_g} \{\psi\}C\{\varphi\}$. We consider the case `skip` and sequence.

- For $C \equiv \texttt{skip}$, we have $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}\texttt{skip}\{\psi\}$, if $\models \varphi \to \psi$. We have $\models \varphi' \to \varphi$, $\models \varphi \to \psi$ and $\models \psi \to \psi'$, thus $\models \varphi' \to \psi'$, what means that $\Gamma \vdash_{\mathcal{H}_g} \{\varphi'\}\texttt{skip}\{\psi'\}$.
- For $C \equiv C_1; C_2$,we have $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C_1; C_2\{\psi\}$, if $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C_1\{\eta\}$ and $\Gamma \vdash_{\mathcal{H}_g} \{\eta\}C_2\{\psi\}$.

  By induction we have

  $$\Gamma \vdash_{\mathcal{H}_g} \{\varphi'\}C_1\{\eta\} \text{ as } \models \varphi' \to \varphi \text{ and } \models \eta \to \eta,$$
  $$\Gamma \vdash_{\mathcal{H}_g} \{\eta\}C_2\{\psi'\} \text{ as } \models \eta \to \eta \text{ and } \models \psi \to \psi',$$

  thus $\Gamma \vdash_{\mathcal{H}_g} \{\varphi'\}C_1; C_2\{\psi'\}$.

Exerc. 7.1. *Complete the previous proof.*

Equivalence between $\mathcal{H}$ and $\mathcal{H}_g$

Lema 7.2. $\Gamma \vdash_{\mathcal{H}} \{\varphi\}C\{\psi\}$ *iff* $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}$

Proof:

($\Rightarrow$) By induction on the derivation of $\Gamma \vdash_{\mathcal{H}} \{\varphi\}C\{\psi\}$, using the lemma. We consider the case of assignment and consequence.

- we have $\Gamma \vdash_{\mathcal{H}} \{\varphi[E/x]\}x \leftarrow E\{\varphi\}$ and $\models \varphi[E/x] \rightarrow \varphi[E/x]$, thus $\Gamma \vdash_{\mathcal{H}_g} \{\varphi[E/x]\}x \leftarrow E\{\varphi\}$
- By the rule of consequence we have

$$\Gamma \vdash_{\mathcal{H}} \{\varphi\}C\{\psi\},$$

  if $\Gamma \vdash_{\mathcal{H}} \{\varphi'\}C\{\psi'\}$ and $\models \varphi \rightarrow \varphi'$, $\models \psi' \rightarrow \psi$.
  By induction we have $\Gamma \vdash_{\mathcal{H}_g} \{\varphi'\}C\{\psi'\}$, thus by the previous lemma we have $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}$.

($\Leftarrow$) By induction on the derivation of $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}$. We consider the case of assignment and conditional.

- we have

$$\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}x \leftarrow E\{\psi\} \text{ if } \models \varphi \rightarrow \psi[E/x].$$

  As

$$\Gamma \vdash_{\mathcal{H}} \{\psi[E/x]\}x \leftarrow E\{\psi\} \text{ and } \models \varphi \rightarrow \psi[E/x]$$

  and $\models \psi \rightarrow \psi$, by $cons_p$ rule, we have $\Gamma \vdash_{\mathcal{H}} \{\varphi\}x \leftarrow E\{\psi\}$.
- we have $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2\, \{\psi\}$, if

$$\Gamma \vdash_{\mathcal{H}_g} \{\varphi \wedge B\}C_1\{\psi\} \text{ and } \Gamma \vdash_{\mathcal{H}_g} \{\varphi \wedge \neg B\}C_2\{\psi\}.$$

  By induction $\Gamma \vdash_{\mathcal{H}} \{\varphi \wedge B\}C_1\{\psi\}$ and $\Gamma \vdash_{\mathcal{H}} \{\varphi \wedge \neg B\}C_2\{\psi\}$, thus $\Gamma \vdash_{\mathcal{H}} \{\varphi\}\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2\, \{\psi\}$

Exerc. 7.2. *Complete the previous proof.*

Pro and Cons

Advantages of $\mathcal{H}_g$:

- The ambiguity of rule *cons* was eliminated.

Drawbacks of $\mathcal{H}_g$:

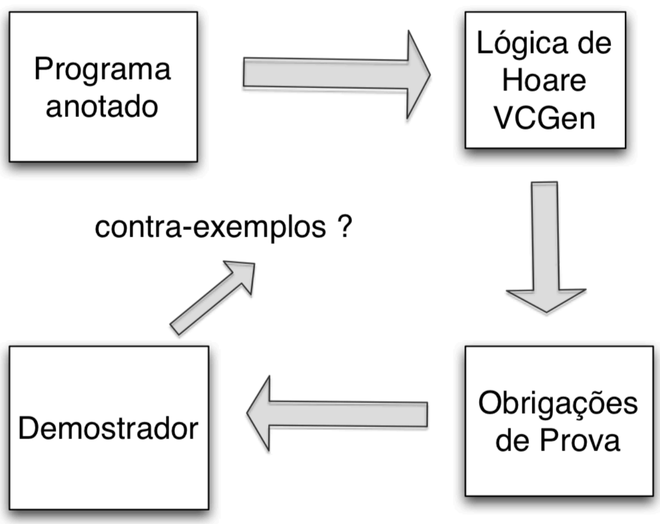
- Is still necessary to guess the intermediate preconditions in *comp*.

The weakest precondition strategy:tableaux

We already saw that for building a derivation for $\{\varphi\}C\{\psi\}$, where φ can or not be known (we write $\{?\}C\{\psi\}$).

1. if φ is known, we apply the unique rule of $\mathcal{H}_g$. if C is $C_1; C_2$, we build a subproof of the form $\{?\}C_2\{\psi\}$. when the proof terminates we can go on with $\{\varphi\}C_1\{\theta\}$, with θ obtained in the previous sub-derivation.
2. if φ is unknown, the construction proceeds as before, except that, in the rules for skip, assignment and loops, with a side condition $\varphi \to \theta$, we tale the precondition φ to be θ (which is exactly the $wp(C.\psi)$.

Two phases verification



Verification condition generator, VCG

Given $\{\varphi\}C\{\psi\}$ to compute $VC(C, \psi)$ we have to:

- Compute the weakest precondition $wp(C, \psi)$
- we have that $\varphi \to wp(C, \psi)$ is a verification condition (VC)
- The remaining VC are collected from the conditions introduced in the loops **while**.

Computation of the weakest preconditions (wp)

Given a program C and a postcondition ψ, we can compute $wp(C,\psi)$ such that $\{wp(C,\psi)\}C\{\psi\}$ is valid and if $\{\varphi\}C\{\psi\}$is valid for any φ then $\varphi \rightarrow wp(C,\psi)$.

$$\begin{array}{rcl} wp(\mathbf{skip},\psi) & = & \psi \\ wp(x \leftarrow E,\psi) & = & \psi[E/x] \\ wp(C_1;C_2,\psi) & = & wp(C_1,wp(C_2,\psi)) \\ wp(\texttt{if}\, B\, \mathbf{then}\, C_1\, \mathbf{else}\, C_2,\psi) & = & (B \rightarrow wp(C_1,\psi)) \\ & & \wedge(\neg B \rightarrow wp(C_2,\psi)) \\ wp(\mathbf{while}\, B\, \mathbf{do}\, \{\eta\}C,\psi) & = & \eta \end{array}$$

Properties of wp and VCG

Given a program C and an assertion ψ if $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}$, for any precondition φ, then

Lema 7.3.

1. $\Gamma \vdash_{\mathcal{H}_g} \{wp(C,\psi)\}C\{\psi\}$
2. $\Gamma \models \varphi \rightarrow wp(C,\psi)$

Proof: By induction on C. We consider the cases of `skip` and `while`.

- For $C \equiv \texttt{skip}$, we have $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}\texttt{skip}\{\psi\}$ if $\models \varphi \rightarrow \psi$. Note that $wp(\texttt{skip},\psi) = \psi$.
    1. Trivially we have $\Gamma \vdash_{\mathcal{H}_g} \{\psi\}\texttt{skip}\{\psi\}$, as $\models \psi \rightarrow \psi$.
    2. By hypothesis we have $\Gamma \models \varphi \rightarrow \psi = wp(\texttt{skip},\psi)$.
- $C \equiv \texttt{while}\, B\, \texttt{do}\, C$, we have

  $$\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}\, \texttt{while}\, B\, \texttt{do}\, \{\eta\}C\, \{\psi\} \text{ if } \Gamma \vdash_{\mathcal{H}_g} \{\eta \wedge B\}C\{\eta\}$$

  and $\models \varphi \rightarrow \eta$, $\models \eta \wedge \neg B \rightarrow \psi$.
  Note that $wp(\texttt{while}\, B\, \texttt{do}\, \{\eta\}C,\psi) = \eta$
    1. As $\models \eta \rightarrow \eta$, and by hypothesis $\models \eta \wedge \neg B \rightarrow \psi$ and $\Gamma \vdash_{\mathcal{H}_g} \{\eta \wedge B\}C\{\eta\}$, then

       $$\Gamma \vdash_{\mathcal{H}_g} \{\eta\}\, \texttt{while}\, B\, \texttt{do}\, \{\eta\}C\, \{\psi\}$$
    2. by hypothesis we have $\Gamma \models \varphi \rightarrow \eta = wp(\texttt{while}\, B\, \texttt{do}\, \{\eta\}C\, \psi)$.

Exerc. 7.3. *Complete the previous proof.*

Algorithm VCG

First one computes $VC(C, \psi)$ without consider the preconditions

$$
\begin{array}{rcl}
VC(\texttt{skip}, \psi) & = & \emptyset \\
VC(x \leftarrow E, \psi) & = & \emptyset \\
VC(C_1; C_2, \psi) & = & VC(C_1, wp(C_2, \psi)) \cup VC(C_2, \psi) \\
VC(\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2, \psi) & = & VC(C_1, \psi) \cup VC(C_2, \psi) \\
VC(\texttt{while}\, B\, \texttt{do}\, \{\eta\} C, \psi) & = & \{(\eta \ \wedge \ B) \rightarrow wp(C, \eta)\} \cup \\
 & & \{(\eta \ \wedge \ \neg B) \rightarrow \psi\} \cup VC(C, \eta)
\end{array}
$$

Next one considers the precondition:

$$VCG(\{\varphi\}C\{\psi\}) = \{\varphi \rightarrow wp(C, \psi)\} \cup VC(C, \psi)$$

Example

let fact be the program:

$f \leftarrow 1; i \leftarrow 1;$
while $i \leq n$ **do**
  $\{f = (i-1)! \wedge i \leq n+1\}$ ▷ Invariante
  $f \leftarrow f * i;$
  $i \leftarrow i + 1;$

We compute

$$\text{VCG}(\{n \geq 0\}\mathsf{fact}\{f = n!\})$$

with

$$
\begin{array}{rcl}
\theta & = & f = (i-1)! \wedge i \leq n+1 \\
C_w & = & f \leftarrow f * i; i \leftarrow i + 1
\end{array}
$$

$$
\begin{aligned}
& VC(\texttt{fact}, f = n!) \\
= \quad & VC(f \leftarrow 1; i \leftarrow 1, wp(\textbf{while } i \leq n \textbf{ do}\{\theta\}C_w, f = n!)) \\
& \cup VC(\textbf{while } i \leq n \texttt{ do}\{\theta\}C_w, f = n!) \\
= \quad & VC(f \leftarrow 1; i \leftarrow 1, \theta) \cup \{\theta \wedge i \leq n \rightarrow wp(C_w, \theta)\} \\
& \cup \{\theta \wedge i > n \rightarrow f = n!\} \cup VC(C_w, \theta) \\
= \quad & VC(f \leftarrow 1, wp(i \leftarrow 1, \theta)) \cup VC(i \leftarrow 1, \theta) \\
& \cup \{f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow wp(f \leftarrow f * i; i \leftarrow i+1, \theta)\} \\
& \cup \{f = (i-1)! \wedge i \leq n+1 \wedge i > n \rightarrow f = n!\} \\
& \cup VC(f = f * i, wp(i \leftarrow i+1, \theta)) \cup VC(i \leftarrow i+1, \theta) \\
= \quad & \emptyset \cup \emptyset \cup \{f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \\
& \qquad \rightarrow wp(f \leftarrow f * i, f = (i+1-1)! \wedge i+1 \leq n+1)\} \\
& \cup \{f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f = n!\} \cup \emptyset \cup \emptyset \\
= \quad & \{f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f * i = (i+1-1)! \\
& \wedge i+1 \leq n+1, f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f = n!\}
\end{aligned}
$$

$$
\begin{aligned}
& VCG(\{n \geq 0\}\mathsf{fact}\{f = n!\}) \\
= \quad & \{n \geq 0 \rightarrow wp(\mathsf{fact}, f = n!)\} \cup VC(\mathsf{fact}, f = n!) \\
= \quad & \{n \geq 0 \rightarrow wp(f \leftarrow 1; i \leftarrow 1; wp(\textbf{while } i \leq n \textbf{ do}\{\theta\}C_w, f = n!), \\
& f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f * i = (i+1-1)! \\
& \wedge i+1 \leq n+1, f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f = n!\} \\
= \quad & \{n \geq 0 \rightarrow wp(f \leftarrow 1; i \leftarrow 1; \theta), \\
& f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f * i = (i+1-1)! \\
& \wedge i+1 \leq n+1, f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f = n!\}
\end{aligned}
$$

We have the following proof obligations:

1. $n \geq 0 \rightarrow 1 = (1-1)! \wedge 1 \leq n+1$
2. $f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f * i = (i+1-1)! \wedge i+1 \leq n+1)$
3. $f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \rightarrow f = n!$

Teorema 7.1 (Adequacy of VCG)**.** *Let $\{\varphi\}C\{\psi\}$ a Hoare triple and Γ a set of assertions.*

$$\Gamma \models VCG(\{\varphi\}C\{\psi\}) \textit{ iff } \Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}.$$

Proof:

($\Rightarrow$) By induction on the derivation of C. We consider the case of assignment and sequence

- For $C \equiv x \leftarrow E$, we have

$$\begin{aligned} VCG(\{\varphi\}X \leftarrow E\{\psi\}) &= \{\varphi \rightarrow wp(X \leftarrow E, \psi)\} \cup VC(x \leftarrow E, \psi) \\ &= \{\varphi \rightarrow \psi[E/x]\}. \end{aligned}$$

If $\Gamma \models \varphi \rightarrow \psi[E/x]$, then by the assignment rule

$$\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C\{\psi\}.$$

- For $C \equiv C_1; C_2$, we have

$$\begin{aligned} VCG(\{\varphi\}C_1; C_2\{\psi\}) &= \{\varphi \rightarrow wp(C_1; C_2, \psi)\} \cup VC(C_1; C_2, \psi) \\ &= \{\varphi \rightarrow wp(C_1, wp(C_2, \psi))\} \\ &\quad \cup VC(C_1, wp(C_2, \psi)) \cup VC(C_2, \psi). \end{aligned}$$

Let $\eta = wp(C_2, \psi)$. As

$$\Gamma \models \varphi \rightarrow wp(C_1, \eta) \cup VC(C_1, \eta) = VCG(\{\varphi\}C_1\{\eta\}),$$

by induction $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C_1\{\eta\}$.
Also $\Gamma \models \eta \rightarrow \eta \cup VC(C_2, \psi) = VCG(\{\eta\}C_2\{\psi\})$, by induction $\Gamma \vdash_{\mathcal{H}_g} \{\eta\}C_2\{\psi\}$, thus $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}C_1; C_2\{\psi\}$.

($\Leftarrow$) By induction on the derivation of $\Gamma \vdash_{\mathcal{H}_g} \{\psi\}C\{\varphi\}$. We consider the case `skip` and conditional.

- $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}\texttt{skip}\{\psi\}$, if $\Gamma \models \varphi \rightarrow \psi = VCG(\{\varphi\}\texttt{skip}\{\psi\})$.

- $\Gamma \vdash_{\mathcal{H}_g} \{\varphi\}\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2\, \{\psi\}$ if $\Gamma \vdash_{\mathcal{H}_g} \{\varphi \wedge B\}C_1\{\psi\}$ e $\Gamma \vdash_{\mathcal{H}_g} \{\varphi \wedge \neg B\}C_2\{\psi\}$. By induction

$$\Gamma \models VCG(\{\varphi \wedge B\}C_1\{\psi\}) = \{(\varphi \wedge B) \rightarrow wp(C_1, \psi)\} \cup VC(C_1, \psi)$$

and

$$\Gamma \models VCG(\{\varphi \wedge \neg B\}C_2\{\psi\}) = \{(\varphi \wedge \neg B) \rightarrow wp(C_2, \psi)\} \cup VC(C_2, \psi).$$

Note that,

$$wp(\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2, \psi) = B \rightarrow wp(C_1, \psi) \wedge \neg B \rightarrow wp(C_2, \psi)\},$$

thus,

$$\Gamma \models \{\varphi \rightarrow wp(\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2, \psi)\}.$$

Thus, $\Gamma \models \{\varphi \rightarrow wp(\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2, \psi)\} \cup VC(C_1, \psi) \cup VC(C_2, \psi) = VCG(\{\varphi\}\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2\{\psi\})$.

Exerc. 7.4. *Complete the previous proof.*

References

[AFPMdS11] José Bacelar Almeida, Maria João Frade, Jorge Sousa Pinto, and Simão Melo de Sousa. *Rigorous Software Development: An Introduction to Program Verification*. Springer, 2011.