Fondament de la programmation: Completeness of Hoare's logic

Giovanni Coray - Vincenzo Pallotta

May 4, 2000

Abstract

In this chapter we outline the proof of relative completeness (in the sense of Cook) for Hoare's calculus.

References:

- Chapter 7 of "The Formal Semantics of Programming Languages: An Introduction" - Glynn Winskel, MIT Press.
- "Verification of Sequential and Concurrent Programs" - K. Apt & E.R. Olderog, Springer.

The Hoare's Calculus

The proof system PD for partial correctness is given by the following rules:

Skip $\vdash \{p\}\mathbf{skip}\{p\}$

Assignement $\vdash \{p[x \mapsto t]\}x := t\{p\}$

Composition

$$\frac{\vdash \{p\}S_1\{r\},\ \vdash \{r\}S_2\{q\}}{\vdash \{p\}S_1; S_2\{q\}}$$

Conditional

$$\frac{\vdash \{p \wedge B\}S_1\{q\},\ \vdash \{p \wedge \neg B\}S_2\{q\}}{\vdash \{p\}\mathbf{if}\ B\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2\ \mathbf{fi}\{q\}}$$

While

$$\frac{\vdash \{p \wedge B\}S\{p\}}{\vdash \{p\}\mathbf{while}\ B\ \mathbf{do}(S)\{p \wedge \neg B\}}$$

Consequence

$$\frac{\models p \rightarrow p_1,\ \vdash \{p_1\}S\{q_1\},\ \models q_1 \rightarrow q}{\vdash \{p\}S\{q\}}$$

Theorem. *Soundess and (relative) Completeness*

$$\models \{p\}S\{q\}\ \mathbf{iff}\ \vdash \{p\}S\{q\}$$

Observe that in the consequence rule we assume validity of assertions thus avoiding the Gödel incompleteness theorem!

Problems with Hoare's Calculus

Theorem. *Gödel's incompleteness Theorem (1931): There is no effective proof system for* $\mathbf{Assn}$ *such that the theorems coincide with the valid assertions of* $\mathbf{Assn}$.

This means in terms of Hoare's logic that there is non effective proof system which allows us to prove $\models \{true\}\mathbf{skip}\{B\}$ for all $B \in \mathbf{Assn}$.

The other way arround we can show that there is no effective proof system for partial correctness assertions observing that $\models \{true\}c\{false\}$ means having an effective general proof for non-termination of the command c.

More on the backgrounds...

- Recall here the semantics of boolean expressions: We write $\sigma \models^{\mathcal{I}} p$ to denote the truth value of a boolean expresion p with respect to a given structure $\mathcal{S} = (\mathcal{D}, \mathcal{I})$, that is:

$$\sigma \models^{\mathcal{I}} p\ \mathbf{iff}\ \mathcal{S}[\![p]\!]\sigma = true$$

- Partial correctness assertions are of the form: $\{p\}S\{q\}$ where p, q are assertions and S is an instruction. The validity for a partial correctness assertion with respect to a given structure $\mathcal{S} = (\mathcal{D}, \mathcal{I})$ is defined as:

$$\forall \sigma \in \Sigma : (\sigma \models^{\mathcal{I}} p\ \mathbf{and}\ \mathcal{C}[\![S]\!]\sigma \neq \perp) \Rightarrow \mathcal{C}[\![S]\!]\sigma \models^{\mathcal{I}} q$$

  which can be written as: $\models^{\mathcal{I}} \{p\}S\{q\}$.

  We are rather interested on a more interpretation indipendent notion of validity where we consider validity in all interpretations: $\models \{p\}S\{q\}$.

Soundness of Hoare's Calculus (1)

To be *sound* for a calculus means that every deduction rule should preserve validity, in the sense that if the assumptions in the rule's premise are valid then so is its conclusion. A rule which satisfies the above requirement is called *sound*.

Theorem. (Soundness) *For every partial correctness assertion* $\{p\}S\{q\}$ *then:*

$$\models \{p\}S\{q\} \,\textbf{if}\, \vdash \{p\}S\{q\}.$$

Proof. By rule-induction we can see that every theorem is valid.

skip: $\models \{p\}\mathbf{skip}\{p\}$

assignment rule: $\vdash \{p[x \mapsto t]\}x := t\{p\}$

Consider the statement $x := a$ where a is an espression of the same type as the variable x. Let $\mathcal{I}$ be an interpretation. We want to show that $\models^{\mathcal{I}} \{p[x \mapsto a]\}x := a\{p\}$ that is for all $\sigma \in \Sigma$:

$$\sigma \models^{\mathcal{I}} p[x \mapsto a] \Rightarrow \mathcal{C}[\![x := a]\!]\sigma \models^{\mathcal{I}} p.$$

This is true by the substitution lemma which states that:

$$\sigma \models p[x \mapsto a] \,\textbf{iff}\, \sigma[x \mapsto \sigma(a)] \models p$$

and $\mathcal{C}[\![x := a]\!]\sigma = \sigma[x \mapsto \sigma(a)]$. □

Soundness of Hoare's Calculus (2)

Proof. (cont.)

sequential composition:

$$\frac{\vdash \{p\}S_1\{r\}, \vdash \{r\}S_2\{q\}}{\vdash \{p\}S_1; S_2\{q\}}$$

By inductive hypothesis we have that for all $\sigma, \sigma' \in \Sigma$ and for all interpretation $\mathcal{I}$:

$$\sigma \models \{p\}S_1\{r\} \,\textbf{iff}\, (\sigma \models^{\mathcal{I}} p \,\textbf{and}\, \mathcal{C}[\![S_1]\!]\sigma \models^{\mathcal{I}} r)$$

and

$$\sigma' \models \{r\}S_2\{q\} \,\textbf{iff}\, (\sigma' \models^{\mathcal{I}} r \,\textbf{and}\, \mathcal{C}[\![S_2]\!]\sigma' \models^{\mathcal{I}} q)$$

provided that S_1, S_2 are not diverging. Then the state generated by the semantics of the sequential composition of statements

$$\mathcal{C}[\![S_1; S_2]\!]\sigma = \mathcal{C}[\![S_2]\!](\mathcal{C}[\![S_1]\!]\sigma) \models^{\mathcal{I}} q$$

and hence:

$$\models \{p\}S_1; S_2\{q\}.$$

□

Soundness of Hoare's Calculus (3)

Proof. (cont.)

conditionals:

$$\frac{\vdash \{p \wedge B\}S_1\{q\}, \vdash \{p \wedge \neg B\}S_2\{q\}}{\vdash \{p\}\mathbf{if}\, B\, \mathbf{then}\, S_1\, \mathbf{else}\, S_2\, \mathbf{fi}\{q\}}$$

By the inductive hypothesis we have that for all interpretation $\mathcal{I}$:
$\models^{\mathcal{I}} \{p \wedge B\}S_1\{q\}$ and $\models^{\mathcal{I}} \{p \wedge \neg B\}S_2\{q\}$
provided that S_1, S_2 are not diverging.
Consider a state σ such that $\sigma \models^{\mathcal{I}} p$. We can have only two mutually exclusive cases: either $\sigma \models^{\mathcal{I}} B$ or $\sigma \models^{\mathcal{I}} \neg B$.
In the former case:

$$\sigma \models^{\mathcal{I}} (p \wedge B) \,\textbf{and}\, \mathcal{C}[\![S_1]\!]\sigma \models^{\mathcal{I}} q$$

in the latter case:

$$\sigma \models^{\mathcal{I}} (p \wedge \neg B) \,\textbf{and}\, \mathcal{C}[\![S_2]\!]\sigma \models^{\mathcal{I}} q$$

This ensures that the resulting state will satisfy the same post-conditions regardless which branch of the conditional being chosen. □

Soundness of Hoare's Calculus (4)

Proof. (cont.)

While:

$$\frac{\vdash \{p \wedge B\}S\{p\}}{\vdash \{p\}\mathbf{while}\, B\, \mathbf{do}(S)\{p \wedge \neg B\}}$$

The assertion p is an *invariant* with respect to the body step S. The denotational semantics of **while** (w.r.t. a given structure $\mathcal{S} = (\mathcal{D}, \mathcal{I})$) can be expressed in the following manner: $\mathcal{C}[\![\mathbf{while}\, B\, \mathbf{do}\,(S)]\!]^{\mathcal{S}} = fix(\Gamma)$ where

$$\Gamma(\theta) = \lambda\sigma.Cond(\mathcal{S}[\![B]\!]\sigma = true, \theta(\mathcal{C}[\![S]\!]^{\mathcal{S}}\sigma), \sigma)$$

and $\theta : \Sigma_\perp \to \Sigma_\perp$. We can compute this fixpoint as the least upper bound $\bigsqcup_{n\in\omega} \theta^n$ of approximating states transformations defined by the following definition:
$\theta^0 = \lambda\sigma.\perp$
$\theta^{n+1} = \lambda\sigma.Cond(\mathcal{S}[\![B]\!]\sigma = true, \theta^n(\mathcal{C}[\![S]\!]^{\mathcal{S}}\sigma), \sigma)$.
Consider now the predicate: $P(n) \Leftrightarrow_{def}$
$\forall\sigma, \sigma' \in \Sigma : \sigma' = \theta^n(\sigma) \,\textbf{and}\, \sigma \models^{\mathcal{I}} p \Rightarrow \sigma' \models^{\mathcal{I}} (p \wedge \neg B)$.
If $P(n)$ holds for all $n \in \omega$, then for all $\sigma \in \Sigma$:

$$\sigma \models^{\mathcal{I}} p \Rightarrow \mathcal{C}[\![\mathbf{while}\, B\, \mathbf{do}\,(S)]\!]^{\mathcal{S}}\sigma \models^{\mathcal{I}} (p \wedge \neg B)$$

and hence $\models \{p\}\mathbf{while}\, B\, \mathbf{do}\,(S)\{p \wedge \neg B\}$.
□

Soundness of Hoare's Calculus (5)

Proof. (cont.)
Let's prove by induction that for all $n \in \omega$: $P(n) \Leftrightarrow_{def}$

$$\forall \sigma, \sigma' \in \Sigma : \sigma' = \theta^n(\sigma) \,\mathbf{and}\, \sigma \models^{\mathcal{I}} p \Rightarrow \sigma' \models^{\mathcal{I}} (p \wedge \neg B).$$

<u>Base case:</u>
$P(0) \Leftrightarrow \forall \sigma \in \Sigma : \sigma \models^{\mathcal{I}} p \Rightarrow \bot \models^{\mathcal{I}} (p \wedge \neg B)$ which is true since the consequence does not depend on the premise and it is in turn true.
<u>Inductive case:</u> Suppose $P(n)$ holds for $n \geq 0$. Let's prove $P(n+1)$:
Assuming that $\sigma' = \theta^{n+1}(\sigma) \,\mathbf{and}\, \sigma \models^{\mathcal{I}} p$ we want to show that $\sigma' \models^{\mathcal{I}} (p \wedge \neg B)$.
We distinguish two mutually exclusive cases: either

$$\mathcal{S}[\![B]\!]\sigma = true \,\mathbf{and}\, \sigma' = \theta^n(\mathcal{C}[\![S]\!]^{\mathcal{S}}\sigma)$$

or

$$\mathcal{S}[\![B]\!]\sigma = false \,\mathbf{and}\, \sigma' = \sigma.$$

In the former case we have that $\sigma \models^{\mathcal{I}} (p \wedge B)$ and $(\mathcal{C}[\![S]\!]^{\mathcal{S}}\sigma) \models^{\mathcal{I}} p$. Since $\sigma' = \theta^n(\mathcal{C}[\![S]\!]^{\mathcal{S}}\sigma)$ applying the inductive hypothesis we get $\sigma' \models^{\mathcal{I}} (p \wedge \neg B)$.
In the latter case we have that $\sigma \models^{\mathcal{I}} (p \wedge \neg B)$ and $\sigma = \sigma'$. □

Soundness of Hoare's Calculus (6)

Proof. (cont.)
Consequence rule:

$$\frac{\models p \rightarrow p_1, \vdash \{p_1\}S\{q_1\}, \models q_1 \rightarrow q}{\vdash \{p\}S\{q\}}$$

By inductive hypothesis we have that

$$\models p \rightarrow p_1 \wedge \models \{p_1\}S\{q_1\} \wedge \models q_1 \rightarrow q.$$

We want to show that

$$\forall \sigma \in \Sigma : \sigma \models^{\mathcal{I}} p \Rightarrow \mathcal{C}[\![S]\!]\sigma \models^{\mathcal{I}} q.$$

Suppose $\sigma \models^{\mathcal{I}} p$ for an arbitrary σ. Then by the inductive hypothesis follows that:

$$\mathcal{C}[\![S]\!]\sigma \models^{\mathcal{I}} q_1$$

and hence

$$\mathcal{C}[\![S]\!]\sigma \models^{\mathcal{I}} q$$

since $\models q_1 \rightarrow q$. □

Completeness of Hoare's Calculus (1)

Definition. *(Weakest precondition) Let $S \in \mathbf{Instr}$ and $p \in \mathbf{Assn}$. Let $\mathcal{S} = (\mathcal{D}, \mathcal{I})$ be a structure.The weakest precondition of p with respect to S in $\mathcal{I}$ is defined by:*

$$wp^{\mathcal{I}}[\![S, p]\!] = \{\sigma \in \Sigma_\bot : \mathcal{C}[\![S]\!]\sigma \models^{\mathcal{I}} p\}.$$

The following relation holds:

$$\models^{\mathcal{I}} \{p\}S\{q\} \,\mathbf{iff}\, [\![p]\!]^{\mathcal{I}} \subseteq wp^{\mathcal{I}}[\![S, q]\!]$$

and if for all $\mathcal{I}$: $[\![p']\!]^{\mathcal{I}} = wp^{\mathcal{I}}[\![S, q]\!]$ then

$$\models^{\mathcal{I}} \{p\}S\{q\} \,\mathbf{iff}\, \models^{\mathcal{I}} p \Rightarrow p'$$

and thus $\models \{p\}S\{q\} \,\mathbf{iff}\, \models p \Rightarrow p'$.
Definition. *$\mathbf{Assn}$ is expressive if and only if for every $S \in \mathbf{Instr}$ and assertion $q \in \mathbf{Assn}$ there is an assertion p such that*

$$[\![p]\!]^{\mathcal{I}} = wp^{\mathcal{I}}[\![S, q]\!]$$

for any interpretation $\mathcal{I}$.

Completeness of Hoare's Calculus (2)

Theorem. $\mathbf{Assn}$ *is expressive.*
Proof. by induction on the structure of $S \in \mathbf{Instr}$. For all assertions $p \in \mathbf{Assn}$ it is possible to construct an assertion $w(S, p)$ such that for all interpretations $\mathcal{I}$:

$$wp^{\mathcal{I}}[\![S, p]\!] = [\![w(S, p)]\!]^{\mathcal{I}}$$

or equivalently:

$$\sigma \models^{\mathcal{I}} w(S, p) \,\mathbf{iff}\, \mathcal{C}[\![S]\!]\sigma \models^{\mathcal{I}} p.$$

The assertion $w(S, p)$ is unique up to logical equivalence.
<u>case $S \equiv x := a$</u>: We define $w(x := a, p) \equiv p[x \mapsto a]$. Then

$$\begin{aligned} \sigma \in wp^{\mathcal{I}}[\![S, p]\!] \quad &\mathbf{iff} \quad \sigma[x \mapsto \sigma(a)] \models^{\mathcal{I}} p \\ &\mathbf{iff} \quad \sigma \models^{\mathcal{I}} p[x \mapsto a] \\ &\mathbf{iff} \quad \sigma \models^{\mathcal{I}} w(x := a, p). \end{aligned}$$

□

Completeness of Hoare's Calculus (3)

Lemma. *For $S \in \mathbf{Instr}$ and $p \in \mathbf{Assn}$, let $w(S, p)$ (an arbitrary one) such that $wp^{\mathcal{I}}[\![S, p]\!] = [\![w(S, p)]\!]^{\mathcal{I}}$. Then:*

$$\vdash \{w(S, p)\}S\{p\}.$$

Proof. by structural induction on S.
<u>case</u> $S \equiv x := a$: Since $\models w(x := a, p) \Leftrightarrow p[x \mapsto a]$ we can apply the consequence rule and obtain

$$\vdash \{w(x := a, p)\}S\{p\}.$$

□

Theorem. *The proof system for partial correctness is relative complete, i.e. for any partial correctness assertion $\{p\}S\{q\}$:*

$$\vdash \{p\}S\{q\} \,\mathbf{if}\, \models \{p\}S\{q\}.$$

Proof. Suppose $\models \{p\}S\{q\}$. Then for the above lemma, for any interpretation $\mathcal{I}$ there exists an assertion $w(S, q)$ such that $[\![w(S, q)]\!]^{\mathcal{I}} = wp^{\mathcal{I}}[\![S, q]\!]$.
Thus as $\models^{\mathcal{I}} (p \Rightarrow w(S, q))$, by applying the consequence rule we obtain $\vdash \{p\}S\{q\}$.
□