Abstract Hoare Logic

Patrick Cousot  
di.ens.fr/~cousot  
cims.nyu.edu/~pcousot

Radhia Cousot  
di.ens.fr/~rcousot

Concrete Hoare Logic

Implicit rules

- **Lemma 12** The disjunction rule of Hoare logic\(^3\) is

\[
\forall i \in \Delta : \{ P_i \} S \{ Q_i \} \quad \frac{\exists i \in \Delta : P_i \quad \exists i \in \Delta : Q_i}{\{ Q \}}
\]

- **Lemma 13** The conjunction rule of Hoare logic is\(^4\)

\[
\forall i \in \Delta : \{ P_i \} S \{ Q_i \} \quad \frac{\forall i \in \Delta : P_i \quad \forall i \in \Delta : Q_i}{\{ Q \}}
\]

\(^3\) This rule is not part of classical Hoare logic but can be proved by structural induction on S.

\(^4\) Idem.

(Set theoretical) Hoare triples

\[\{ P \} S \{ Q \} \triangleq \forall \vec{v}', \vec{v} \in \vec{V} : (P(\vec{v}') \land [S](\vec{v}', \vec{v})) \Rightarrow Q(\vec{v}', \vec{v})\,.

**Hoare rules**

- \(\{ \text{false} \} S \{ Q \} = \text{true.}\)
- \(\{ P \} S \{ \text{true} \} = \text{true.}\)
- \(P \Rightarrow P' \land \{ P' \} S \{ Q' \} \land Q' \Rightarrow Q
\]

\(\{ P \} S \{ Q \}\)
Unmodified variables

- **Lemma 14** The fact that none of the variables in \( \bar{g} \) are defined/modified/written by \( S \) can be expressed in Hoare logic as
  \[
  \langle \lambda (\bar{p} \cdot \bar{g}) \cdot \text{true} \rangle S \langle \lambda (\bar{p}' \cdot \bar{g}') \cdot \bar{g} = \bar{g}' \rangle.
  \]

**Notation:**
\[
S \mid \bar{p} \setminus \bar{g}
\]

Contracts

- **Definition 10 (Valid method contract)** The set of all contracts for method \( M \) is
  \[
  C^r[M] \triangleq \mathcal{P}[[\bar{p}, \bar{g}]] \times \mathcal{P}[[\bar{p}', \bar{g}'], (\bar{p}^*, \bar{g}^*)].
  \]
  A contract \( \langle P, Q \rangle \in C^r[M] \) is valid for the method \( M \) if and only if \( \{ P \} S \mid \bar{p}, \bar{g} \{ Q \} \).

- **Lemma 18** If \( \langle P, Q \rangle \xrightarrow{cc} \langle P', Q' \rangle \) and \( \{ P \} S \{ Q \} \) hold then \( \{ P' \} S \{ Q' \} \) does hold.

Abstract predicates

**Hypotheses 1.** The abstract domain \( A[\bar{v}] \), \( \subseteq \) is an abstraction of unary predicates \( \mathcal{P}[\bar{v}] \), \( \implies \) which meaning is given by an increasing concretization \( \gamma_1 \in \langle A[\bar{v}] \rangle \), \( \subseteq \rightarrow \langle \mathcal{P}[\bar{v}] \rangle \), \( \implies \):  

1. The abstract domain \( B[\bar{v}, \bar{v}] \), \( \subseteq \) is an abstraction of binary predicates \( \mathcal{P}[\bar{v}, \bar{v}] \), \( \implies \) which meaning is given by a finite-meet-preserving concretization \( \gamma_2 \in \langle B[\bar{v}, \bar{v}] \rangle \), \( \subseteq \rightarrow \langle \mathcal{P}[\bar{v}, \bar{v}] \rangle \), \( \implies \) (i.e. \( \gamma_2(Q \cap Q') = \gamma_2(Q) \land \gamma_2(Q') \)) which implies that \( \gamma_2 \) is increasing;  
2. Given variables \( \bar{g} \subseteq \bar{v} \), then \( \gamma_2[\bar{g}] \in B[\bar{v}, \bar{v}] \) is the abstract statement that none of the values of the variables \( \bar{g} \) has changed that is \( \gamma_2[\bar{g}] \triangleq \lambda \bar{v}' \cdot \forall x \in \bar{g} : v'(x) = v(x) \);  
3. The unary abstract predicate \( \bar{T} \in A[\bar{v}] \) can be embedded into \( B[\bar{v}, \bar{v}] \) as \( \bar{T}_1(\bar{T}) \) such that  
   \[
   \bar{T}_1 \in A[\bar{v}] \rightarrow B[\bar{v}, \bar{v}] \\
   \forall \bar{P} \in A[\bar{v}] : \forall \bar{v}', \bar{v}'' \in \bar{v}[\bar{v}] : \gamma_2(\bar{T}_1(\bar{P}) \bar{v}', \bar{v}'') = \gamma_1(\bar{P}(\bar{v}')).
   \]
   We assume that \( \bar{T}_1 \) is increasing that is for all \( \bar{P}, \bar{F} \in A[\bar{v}] \), \( \bar{P} \subseteq \bar{F} \) implies that \( \bar{T}_1(\bar{P}) \subseteq \bar{T}_1(\bar{F}) \).
**Contract Abstraction**

- \( \gamma_{cc} \in (A[\vec{v}] \times B[\vec{v}], \vec{c}) \rightarrow (C[\vec{v}], \vec{c}) \) where
- \( \gamma_{cc}(\langle P, Q \rangle) \triangleq \langle \gamma_1(P), \gamma_2(Q) \rangle \)
- \( \langle P, Q \rangle \preccurlyeq \langle P', Q' \rangle \triangleq P' \subseteq P \land \uparrow_1^2(P') \sqsupseteq Q \subseteq Q' \).

**Lemma 27** \( \gamma_{cc} \) is increasing.

---

**Concretization must preserve meets**

**Remark 7** Observe that if \( \gamma_2 \) is increasing but not meet-preserving then the property that an abstract contract is more precise than another one may not be preserved in the concrete. Here is a counter-example.

**Abstract Hoare Triples**

- **Definition 15** (Abstract Hoare triple)
  \[
  \{ \bullet \} \{ \bullet \} \in A[\vec{v}] \times S \times B[\vec{v}] \rightarrow B.
  \]
  \[
  \{ P \} S \{ Q \} \triangleq \{ \gamma_1(P) \} S \{ \gamma_2(Q) \}.
  \]

  The concrete rules of Hoare logic are sound, if not complete, in the abstract.

- **Lemma 28** If \( \{ P \} S \{ Q \} \) then \( \{ P \} S \{ \uparrow_1^2(P) \sqcap Q \} \).
Lemma 29 (Abstract post-condition strengthening)
\[ \frac{[P] \mathcal{S}[\delta] \mathcal{Q}}{[\bigwedge_{i \in \Delta} P_i] \mathcal{S}[\bigwedge_{i \in \Delta} \mathcal{Q}]} \]

Lemma 30 If $A$ has an infimum $\bot_A$, then for all $Q \in B$, $[\bot_A] \mathcal{S}[\mathcal{Q}] = \text{true}$.

Lemma 31 If $B$ has a supremum $\top_B$, then for all $P \in A$, $[\mathcal{P}] \mathcal{S}[\top_B] = \text{true}$.

Lemma 32 The abstract consequence rule of Hoare logic
\[ \frac{P \in \mathcal{P} \land [P] \mathcal{S}[\mathcal{Q}] \land \mathcal{Q} \in \mathcal{Q}}{[P] \mathcal{S}[\mathcal{Q}]} \]
is sound.

Remarks
- $\forall i \in \Delta : [P_i] \mathcal{S}[Q_i] \quad \text{is sound if the glb exists}$
- $\forall i \in \Delta : \bigwedge_{i \in \Delta} P_i \mathcal{S}[\bigwedge_{i \in \Delta} Q_i]$ may be invalid since $\gamma_1(\bigwedge_{i \in \Delta} P_i) \not\Rightarrow \bigwedge_{i \in \Delta} \gamma_1(P_i)$ but not inversely when $\gamma_1$ is increasing.
- $\forall i \in \Delta : [P_i] \mathcal{S}[Q_i]$ is sound if the lub exists
- $\forall i \in \Delta : \bigvee_{i \in \Delta} P_i \mathcal{S}[\bigvee_{i \in \Delta} Q_i]$ is in general invalid

Counter-example

\[ P = \begin{cases} \text{true} & \text{if } x \geq 0 \\ \text{false} & \text{if } x < 0 \end{cases} \]
\[ Q = \begin{cases} \text{true} & \text{if } x \leq 0 \\ \text{false} & \text{if } x > 0 \end{cases} \]

We have
- $[x \geq 0] x = -x \{x \leq 0\}$
- $[x \leq 0] x = -x \{x \geq 0\}$

but definitely not
- $[x \geq 0 \land x \leq 0] x = -x \{x \leq 0 \land x \geq 0\}$

which is
- $[x = 0] x = -x \{\text{false}\}$

when $\gamma_2(\text{false}) = \text{false}$.

Abstract conjunction rule

Lemma 33 (Abstract conjunction rule) If $\gamma_1$ is increasing, the glbs do exist, and $\bigwedge_{i \in \Delta} \gamma_1(Q_i)$, then the abstract conjunction rule of Hoare logic
\[ \forall i \in \Delta : [P_i] \mathcal{S}[Q_i] \quad \bigwedge_{i \in \Delta} P_i \mathcal{S}[\bigwedge_{i \in \Delta} Q_i] \]
is sound.

\[\text{^14 e.g. either } \Delta \text{ is finite and } \gamma_2 \text{ is finite-meet-preserving or else } \gamma_2 \text{ is meet-preserving (equivalently upper-adjoints of Galois connections)}\]
Consequence rule

Lemma 34 If $\{ P \} S \{ Q \}$ and $\langle P', Q \rangle \subseteq \langle P, Q \rangle$ then $\{ P' \} S \{ Q \}$.

Postcondition strengthening

Lemma 35 If $\gamma_2$ is finite-meet-preserving then $\{ P \} S \{ Q \}$ if and only if $\{ P \} S \{ Q \}$ if and only if $\{ g \}$

Method call

Hypotheses 2 (Abstract projection and antiprojection)

1. An abstract projection $\downarrow_{\beta, g} \in A[\bar{\beta}, \bar{g}] \rightarrow A[\bar{\beta}]$ such that

\[
\begin{align*}
& \forall P \in A : P \subseteq \downarrow_{\beta, g}(P) \quad (a) \\
& (\exists \gamma : \gamma_1(P)_{\beta, g} = \gamma_1(\downarrow_{\beta, g}(P)_{\beta, g})) \quad (b) \\
& (\exists \gamma : \gamma_2(\downarrow_{\beta, g}(P)_{\beta, g}, g) \Rightarrow \gamma_2(\downarrow_{\beta, g}(P)_{\beta, g}, g)) \quad (c)
\end{align*}
\]

2. An abstract antiprojection $\uparrow_{\beta, g} \in B[\bar{\beta}, \bar{g}] \rightarrow B[\bar{\beta}, \bar{g}]$ such that

\[
\begin{align*}
& A(\langle \bar{\gamma}', \bar{\gamma}' \rangle, \langle \bar{\gamma}, \bar{\gamma} \rangle) \triangleq \gamma_2(\downarrow_{\beta, g}(q', q') \land \bar{\gamma} = \bar{\gamma}' \quad \Rightarrow \quad \gamma_2(\downarrow_{\beta, g}(q', q') \land \bar{\gamma} = \bar{\gamma}')) .
\end{align*}
\]

3. We leave variable renaming implicit, identifying $A[\bar{\beta}]$ and $A[\bar{\beta}]$ whenever $\check{\gamma}[\bar{\gamma}] = \check{\gamma}[\bar{\gamma}]$.

\[\Box\]

Theorem 7 (Soundness of the abstract separate method call analysis rule) Let $\mathcal{M}(\bar{\beta}) \{ S \}$ be a method definition where $\bar{\beta}$ is the list of in/out formal parameters and $S_{\beta, g}$ is the body such that $\bar{\beta} \land \bar{g} = \emptyset$, $S_{\beta, g}$ may read and modify the parameters $\bar{\beta}$, but $S_{\beta, g}$ does not modify any of the global variables $\bar{g}$. Let $\mathcal{M}(\bar{q})$ be a method call where the actual parameters $\bar{q}$ are variables such that $\check{\gamma}[\bar{q}] = \check{\gamma}[\bar{\beta}]$. In the context of the abstraction of Sec. 13, the following abstract separate method call analysis rule

\[
\begin{align*}
\frac{\downarrow_{\beta, g}(P)_{\beta, g} \quad S_{\beta, g} \quad \check{\gamma}(q) \quad \uparrow_{\beta, g}(q)_{\beta, g}}{\text{is sound.}}
\end{align*}
\]