# Abstract Hoare Logic

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

Radhia Cousot
di.ens.fr/~rcousot

# Concrete Hoare Logic

## (Set theoretical) Hoare triples

$$\{\,P\,\}\,\mathtt{S}\,\{\,Q\,\} \;\triangleq\; \forall \vec{v}', \vec{v} \in \vec{\mathcal{V}} : (P(\vec{v}') \wedge [\![\mathtt{S}]\!](\vec{v}', \vec{v})) \Longrightarrow Q(\vec{v}', \vec{v})\ .$$

## Hoare rules

- $\{\,\dot{\mathtt{false}}\,\}\,S\,\{\,Q\,\} = \mathtt{true}$.
- $\{\,P\,\}\,S\,\{\,\dot{\mathtt{true}}\,\} = \mathtt{true}$.
- $\dfrac{P \,\dot{\Longrightarrow}\, P' \wedge \{\,P'\,\}\,S\,\{\,Q'\,\} \wedge Q' \,\dot{\Longrightarrow}\, Q}{\{\,P\,\}\,S\,\{\,Q\,\}}$

## Implicit rules

- **Lemma 12** *The* disjunction rule *of Hoare logic*[3] *is*

$$\frac{\forall i \in \Delta : \{\,P_i\,\}\,S\,\{\,Q_i\,\}}{\{\,\dot{\exists} i \in \Delta : P_i\,\}\,S\,\{\,\dot{\exists} i \in \Delta : Q_i\,\}}\ .$$

- **Lemma 13** *The* conjunction rule *of Hoare logic is*[4]

$$\frac{\forall i \in \Delta : \{\,P_i\,\}\,S\,\{\,Q_i\,\}}{\{\,\dot{\forall} i \in \Delta : P_i\,\}\,S\,\{\,\dot{\forall} i \in \Delta : Q_i\,\}}$$

[3] This rule is not part of classical Hoare logic but can be proved by structural induction on S.
[4] idem.

# Unmodified variables

- **Lemma 14** *The fact that none of the variables in $\vec{g}$ are defined/modified/written by $S$ can be expressed in Hoare logic as*

$$\{\lambda(\vec{p},\vec{g})\bullet \mathtt{true}\}\, S\, \{\lambda(\vec{p}\,',\vec{g}\,'),(\vec{p},\vec{g})\bullet \vec{g}=\vec{g}\,'\}\,. \qquad \square$$

- Notation:

$$S\,|_{\vec{p}\setminus\vec{g}}$$



# Contracts

- **Definition 10 (Valid method contract)** The set of all *contracts for method* $\mathtt{M}$ is

$$C^{cc}[\![\mathtt{M}]\!] \triangleq \mathcal{P}[\![(\vec{\mathtt{p}},\vec{\mathtt{g}})]\!]\times\mathcal{P}[\![(\vec{\mathtt{p}},\vec{\mathtt{g}}),(\vec{\mathtt{p}},\vec{\mathtt{g}})]\!]\,.$$

  A contract $\langle P,\ Q\rangle \in C^{cc}[\![\mathtt{M}]\!]$ is *valid* for the method $\mathtt{M}$ if and only if $\{\,P\,\}\,\mathtt{S}\,|_{\vec{\mathtt{p}},\vec{\mathtt{g}}}\,\{\,Q\,\}$.

- $\langle P,\ Q\rangle \overset{cc}{\Longrightarrow} \langle P',\ Q'\rangle \ \triangleq\ (P' \overset{\cdot}{\Longrightarrow} P)\wedge(\lambda\vec{v}\,',\vec{v}\bullet P'(\vec{v}\,')\wedge Q(\vec{v}\,',\vec{v}) \overset{\cdot}{\Longrightarrow} Q')$

- **Lemma 18** *If* $\langle P,\ Q\rangle \overset{cc}{\Longrightarrow} \langle P',\ Q'\rangle$ *and* $\{\,P\,\}\,S\,\{\,Q\,\}$ *hold then* $\{\,P'\,\}\,S\,\{\,Q'\,\}$ *does hold.*



# Abstract Properties



# Abstract predicates

**Hypotheses 1** *1. The abstract domain $\langle A[\![\vec{v}]\!],\ \sqsubseteq\rangle$ is an abstraction of unary predicates $\langle\mathcal{P}[\![\vec{v}]\!],\ \Longrightarrow\rangle$ which meaning is given by an increasing concretization $\gamma_1 \in \langle A[\![\vec{v}]\!],\ \sqsubseteq\rangle \to \langle\mathcal{P}[\![\vec{v}]\!],\ \Longrightarrow\rangle$;*

*2. The abstract domain $\langle B[\![\vec{v},\vec{v}]\!],\ \sqsubseteq\rangle$ is an abstraction of binary predicates $\langle\mathcal{P}[\![\vec{v},\vec{v}]\!],\ \Longrightarrow\rangle$ which meaning is given by a* finite-meet-preserving *concretization $\gamma_2 \in \langle B[\![\vec{v},\vec{v}]\!],\ \sqsubseteq\rangle \to \langle\mathcal{P}[\![\vec{v},\vec{v}]\!],\ \Longrightarrow\rangle$ (i.e. $\gamma_2(\overline{Q}\sqcap\overline{Q}') = \gamma_2(\overline{Q})\ \dot{\wedge}\ \gamma_2(\overline{Q}')$ which implies that $\gamma_2$ is increasing)[13];*

*3. Given variables $\vec{g}\subseteq\vec{v}$, then $\dot{=}[\![\vec{g}]\!]\in B[\![\vec{v},\vec{v}]\!]$ is the abstract statement that none of the values of the variables $\vec{g}$ has changed that is $\gamma_2(\dot{=}[\![\vec{g}]\!]) \triangleq \lambda\vec{v}\,',\vec{v}\bullet\forall\mathtt{x}\in\vec{g} : \vec{v}\,'(\mathtt{x}) = \vec{v}(\mathtt{x})$;*

*4. The unary abstract predicates $\overline{P}\in A[\![\vec{v}]\!]$ can be embedded into $B[\![\vec{v},\vec{v}]\!]$ as $\uparrow_1^2(\overline{P})$ such that*

$$\uparrow_1^2 \in A[\![\vec{v}]\!] \to B[\![\vec{v},\vec{v}]\!]$$
$$\forall\overline{P}\in A[\![\vec{v}]\!] : \forall\vec{v}\,',\vec{v}\in\vec{\mathcal{V}}[\![\vec{v}]\!] : \gamma_2(\uparrow_1^2(\overline{P}))(\vec{v}\,',\vec{v}) = \gamma_1(\overline{P})(\vec{v}\,')\,.$$

*We assume that $\uparrow_1^2$ is increasing that is for all $\overline{P},\overline{P}'\in A[\![\vec{v}]\!]$, $\overline{P}\sqsubseteq\overline{P}'$ implies that $\uparrow_1^2(\overline{P})\sqsubseteq\uparrow_1^2(\overline{P}')$.* $\square$

# Contract Abstraction

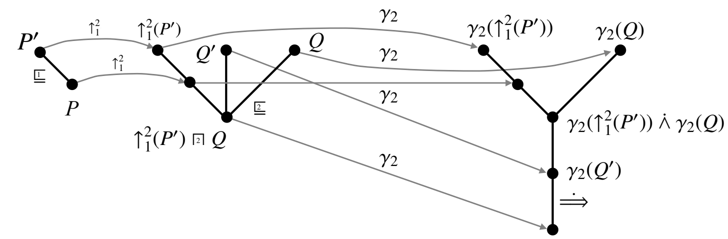
- $\gamma_{cc} \in \langle A[\![\vec{v}]\!] \times B[\![\vec{v}, \vec{v}]\!], \stackrel{cc}{\sqsubseteq} \rangle \rightarrow \langle C^{cc}[\![\vec{v}]\!], \stackrel{cc}{\Longrightarrow} \rangle$ where
- $\gamma_{cc}(\langle \overline{P}, \overline{Q} \rangle) \triangleq \langle \gamma_1(\overline{P}), \gamma_2(\overline{Q}) \rangle$
- $\langle \overline{P}, \overline{Q} \rangle \stackrel{cc}{\sqsubseteq} \langle \overline{P}', \overline{Q}' \rangle \triangleq \overline{P}' \sqsubseteq_1 \overline{P} \wedge \uparrow^2_1(\overline{P}') \sqcap_2 \overline{Q} \sqsubseteq_2 \overline{Q}'$ .

- **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 Logic



# Abstract Hoare Triples

- **Definition 15 (Abstract Hoare triple)**

$$\overline{\{}\bullet\overline{\}}\bullet\overline{\{}\bullet\overline{\}} \in A[\![\vec{v}]\!] \times \mathbb{S} \times B[\![\vec{v}, \vec{v}]\!] \rightarrow \mathbb{B}$$
$$\overline{\{}\overline{P}\overline{\}}\,\mathtt{S}\,\overline{\{}\overline{Q}\overline{\}} \triangleq \{\gamma_1(\overline{P})\}\,\mathtt{S}\,\{\gamma_2(\overline{Q})\}$$

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

- **Lemma 28** *If* $\overline{\{}\overline{P}\overline{\}}\, S|_{\vec{v}}\, \overline{\{}\overline{Q}\overline{\}}$ *then* $\overline{\{}\overline{P}\overline{\}}\, S|_{\vec{v}}\, \overline{\{}\uparrow^2_1(\overline{P}) \sqcap_2 \overline{Q}\overline{\}}$.

# Lemmata

- **Lemma 29 (Abstract post-condition strengthening)**

$$\frac{\bar{\{}\,\overline{P}\,\bar{\}}\, S\,|_{\vec{p}\backslash\vec{g}}\, \bar{\{}\,\overline{Q}\,\bar{\}}}{\bar{\{}\,\overline{P}\,\bar{\}}\, S\,|_{\vec{p}\backslash\vec{g}}\, \bar{\{}\, \uparrow_1^2(\overline{P}) \sqcap_2 \overline{Q} \sqcap_2 \dot{=}[\![\vec{g}\,]\!]\,\bar{\}}}$$

- **Lemma 30** *If $A$ has an infimum $\bot_A$ such that $\gamma_1(\bot_A) = \mathtt{false}$ then for all $\overline{Q} \in B$, $\bar{\{}\,\bot_A\,\bar{\}}\, S\, \bar{\{}\,\overline{Q}\,\bar{\}} = \mathtt{true}$.*

- **Lemma 31** *If $B$ has a supremum $\top_B$ such that $\gamma_2(\top_B) = \mathtt{true}$ then for all $\overline{P} \in A$, $\bar{\{}\,\overline{P}\,\bar{\}}\, S\, \bar{\{}\,\top_B\,\bar{\}} = \mathtt{true}$.*

- **Lemma 32** *The* abstract consequence rule *of Hoare logic*

$$\frac{\overline{P} \sqsubseteq_1 \overline{P}' \wedge \bar{\{}\,\overline{P}'\,\bar{\}}\, S\, \bar{\{}\,\overline{Q}'\,\bar{\}} \wedge \overline{Q}' \sqsubseteq_2 \overline{Q}}{\bar{\{}\,\overline{P}\,\bar{\}}\, S\, \bar{\{}\,\overline{Q}\,\bar{\}}}$$

*is sound.*

# Remarks

- $\dfrac{\forall i \in \Delta : \bar{\{}\,\overline{P}_i\,\bar{\}}\, \mathtt{S}\, \bar{\{}\,\overline{Q}\,\bar{\}}}{\bar{\{}\, \underset{i\in\Delta}{\sqcap_1} \overline{P}_i\,\bar{\}}\, \mathtt{S}\, \bar{\{}\,\overline{Q}\,\bar{\}}}$ is sound if the glb exists

- $\dfrac{\forall i \in \Delta : \bar{\{}\,\overline{P}\,\bar{\}}\, \mathtt{S}\, \bar{\{}\,\overline{Q}_i\,\bar{\}}}{\bar{\{}\,\overline{P}\,\bar{\}}\, \mathtt{S}\, \bar{\{}\, \underset{i\in\Delta}{\sqcap_1} \overline{Q}_i\,\bar{\}}}$ may be invalid since $\gamma_1(\underset{i\in\Delta}{\sqcap_1} \overline{P}_i) \overset{\cdot}{\Longrightarrow} \underset{i\in\Delta}{\dot{\bigwedge}} \gamma_1(\overline{P}_i)$ but not inversely when $\gamma_1$ is increasing.

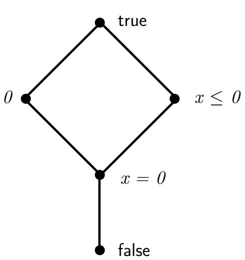
- $\dfrac{\forall i \in \Delta : \bar{\{}\,\overline{P}\,\bar{\}}\, \mathtt{S}\, \bar{\{}\,\overline{Q}_i\,\bar{\}}}{\bar{\{}\,\overline{P}\,\bar{\}}\, \mathtt{S}\, \bar{\{}\, \underset{i\in\Delta}{\sqcup_2} \overline{Q}_i\,\bar{\}}}$ is sound if the lub exists

- $\dfrac{\forall i \in \Delta : \bar{\{}\,\overline{P}_i\,\bar{\}}\, \mathtt{S}\, \bar{\{}\,\overline{Q}_i\,\bar{\}}}{\bar{\{}\, \underset{i\in\Delta}{\sqcup_1} \overline{P}_i\,\bar{\}}\, \mathtt{S}\, \bar{\{}\, \underset{i\in\Delta}{\sqcup_2} \overline{Q}_i\,\bar{\}}}$ is in general invalid

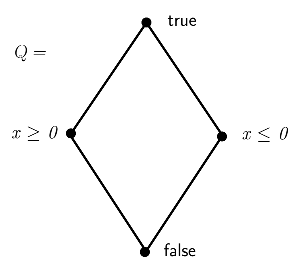
 

# Counter-example

$P =$




$Q =$




We have

$$\bar{\{}\,x \geq 0\,\bar{\}}\, \mathtt{x} = \mathtt{-x}\, \bar{\{}\,x \leq 0\,\bar{\}}$$
$$\bar{\{}\,x \leq 0\,\bar{\}}\, \mathtt{x} = \mathtt{-x}\, \bar{\{}\,x \geq 0\,\bar{\}}$$

but definitely not

$$\bar{\{}\,x \geq 0 \sqcap_1 x \leq 0\,\bar{\}}\, \mathtt{x} = \mathtt{-x}\, \bar{\{}\,x \leq 0 \sqcap_2 x \geq 0\,\bar{\}}$$

which is

$$\bar{\{}\,x = 0\,\bar{\}}\, \mathtt{x} = \mathtt{-x}\, \bar{\{}\,\mathsf{false}\,\bar{\}}$$

when $\gamma_2(\mathsf{false}) = \mathtt{false}$.

# Abstract conjunction rule

**Lemma 33 (Abstract conjunction rule)** *If $\gamma_1$ is increasing, the glbs do exist, and $\underset{i\in\Delta}{\dot{\bigwedge}} \gamma_2(\overline{Q}_i) = \gamma_2(\underset{i\in\Delta}{\sqcap_2} \overline{Q}_i)$*[14] *then the* abstract conjunction rule *of Hoare logic*

$$\frac{\forall i \in \Delta : \bar{\{}\,\overline{P}_i\,\bar{\}}\, S\, \bar{\{}\,\overline{Q}_i\,\bar{\}}}{\bar{\{}\, \underset{i\in\Delta}{\sqcap_1} \overline{P}_i\,\bar{\}}\, S\, \bar{\{}\, \underset{i\in\Delta}{\sqcap_2} \overline{Q}_i\,\bar{\}}}$$

*is sound.* □

[14] e.g. either $\Delta$ is finite and $\gamma_2$ is finite-meet-preserving or else $\gamma_2$ is meet-preserving (equivalently upper-adjoints of Galois connections)

# Consequence rule

**Lemma 34** *If* $\bar{\{}\,\overline{P}\,\bar{\}}\, S\, \bar{\{}\,\overline{Q}\,\bar{\}}$ *and* $\langle \overline{P},\ \overline{Q} \rangle \stackrel{cc}{\sqsubseteq} \langle \overline{P}',\ \overline{Q}' \rangle$ *then* $\bar{\{}\,\overline{P}'\,\bar{\}}\, S\, \bar{\{}\,\overline{Q}'\,\bar{\}}$.

# Postcondition strengthening

**Lemma 35** *If* $\gamma_2$ *is finite-meet-preserving then* $\bar{\{}\,\overline{P}\,\bar{\}}\, S|_{\vec{p}\setminus\vec{g}}\, \bar{\{}\,\overline{Q}\,\bar{\}}$ *if and only if* $\bar{\{}\,\overline{P}\,\bar{\}}\, S|_{\vec{p}\setminus\vec{g}}\, \bar{\{}\,\overline{Q} \sqcap_2 \dot{=}[\![\vec{g}]\!]\,\bar{\}}$.



# Method call

**Hypotheses 2 (Abstract projection and antiprojection)** *1. An* abstract projection $\downarrow_{\vec{p}\setminus\vec{g}} \in A[\![\vec{p}, \vec{g}]\!] \to A[\![\vec{p}]\!]$ *such that*

$$\forall \overline{P} \in A : \overline{P} \quad \sqsubseteq_1 \quad \downarrow_{\vec{p}\setminus\vec{g}}(\overline{P}) \tag{a}$$

$$(\dot{\exists}\vec{g} : \gamma_1(\overline{P})|_{\vec{p},\vec{g}}) \quad = \quad \gamma_1(\downarrow_{\vec{p}\setminus\vec{g}}(\overline{P}|_{\vec{p},\vec{g}})) \tag{b}$$

$$(\dot{\exists}\vec{g} : \gamma_2(\overline{Q})|_{(\vec{p},\vec{g}),(\vec{p},\vec{g})}) \quad \stackrel{\cdot}{\Longrightarrow} \quad \gamma_2(\downarrow_{\vec{p}\setminus\vec{g}}(\overline{Q}|_{(\vec{p},\vec{g}),(\vec{p},\vec{g})}))$$

$$\downarrow_{\vec{p}\setminus\vec{g}} \text{ is increasing} \tag{c}$$

2. *An* abstract antiprojection $\uparrow_{\vec{p}\setminus\vec{g}} \in B[\![\vec{p}, \vec{p}]\!] \to B[\![(\vec{p}, \vec{g}), (\vec{p}, \vec{g})]\!]$ *such that*

$$\lambda((\vec{q}\,', \vec{g}\,'), (\vec{q}, \vec{g})) \bullet \gamma_2(\overline{Q})|_{\vec{q},\vec{q}}(\vec{q}\,', \vec{q}) \wedge \vec{g} = \vec{g}\,' \quad \stackrel{\cdot}{\Longrightarrow} \quad \gamma_2\big(\uparrow_{\vec{p}\setminus\vec{g}}(\overline{Q}|_{\vec{q},\vec{q}})|_{(\vec{q},\vec{g}),(\vec{q},\vec{g})}\big)\,.$$

3. *We leave variable renaming implicit, identifying* $A[\![\vec{p}]\!]$ *and* $A[\![\vec{q}]\!]$ *whenever* $\vec{\mathcal{V}}[\![\vec{q}]\!] = \vec{\mathcal{V}}[\![\vec{p}]\!]$. □



# Method call

**Theorem 7 (Soundness of the abstract separate method call analysis rule)** *Let* $\mathtt{M}(\vec{p})\{\, S \,\}$ *be a method definition where* $\vec{p}$ *is the list of in/out formal parameters and* $S|_{\vec{p}\setminus\vec{g}}$ *is the body such that* $\vec{p} \cap \vec{g} = \emptyset$, $S|_{\vec{p}\setminus\vec{g}}$ *may read and modify the parameters* $\vec{p}$, *but* $S|_{\vec{p}\setminus\vec{g}}$ *does not modify any of the global variables* $\vec{g}$. *Let* $\mathtt{M}(\vec{q})$ *be a method call where the actual parameters* $\vec{q}$ *are variables such that* $\vec{\mathcal{V}}[\![\vec{q}]\!] = \vec{\mathcal{V}}[\![\vec{p}]\!]$. *In the context of the context abstraction of Sec. 13, the following* abstract separate method call analysis rule

$$\frac{\bar{\{}\downarrow_{\vec{p}\setminus\vec{g}}(\overline{P}|_{\vec{p},\vec{g}})\bar{\}}\, S|_{\vec{p}\setminus\vec{g}}\, \bar{\{}\,\overline{Q}|_{\vec{p},\vec{p}}\,\bar{\}}}{\bar{\{}\,\overline{P}|_{\vec{q},\vec{g}}\,\bar{\}}\, \mathtt{M}(\vec{q})\, \bar{\{}\uparrow_{\vec{p}\setminus\vec{g}}(\overline{Q}|_{\vec{q},\vec{q}})\bar{\}}}$$

*is sound.* □



# The End