Principles of Abstract Interpretation
MIT press
Ch. **26**, Hoare logic

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-26--Hoare-logic-PrAbsInt.pdf

Chapter 26

Ch. **26**, Hoare logic

The traditional presentation of Hoare logic $\{P\}S\{Q\}$

Empty statement axiom schema

$$\frac{}{\{P\}\textbf{skip}\{P\}}$$

Assignment axiom schema

$$\frac{}{\{P[E/x]\}x := E\{P\}}$$

$$\{x+1 \leq N\}x := x+1\{x \leq N\}$$

Rule of composition

$$\frac{\{P\}S\{Q\} \quad , \quad \{Q\}T\{R\}}{\{P\}S;T\{R\}}$$

Conditional rule

$$\frac{\{B \wedge P\}S\{Q\} \quad , \quad \{\neg B \wedge P\}T\{Q\}}{\{P\}\textbf{if } B \textbf{ then } S \textbf{ else } T \textbf{ endif}\{Q\}}$$

Consequence rule

$$\frac{P_1 \to P_2 \quad , \quad \{P_2\}S\{Q_2\} \quad , \quad Q_2 \to Q_1}{\{P_1\}S\{Q_1\}}$$

While rule

$$\frac{\{P \wedge B\}S\{P\}}{\{P\}\textbf{while } B \textbf{ do } S \textbf{ done}\{\neg B \wedge P\}}$$

en.wikipedia.org/wiki/Hoare_logic

This is an abstraction

- Assertional reachability semantics: $\widehat{\mathcal{S}}^{\vec{r}}[\![\mathsf{s}]\!]\,\mathcal{R}_0\,\ell$ is the set of reachable environments at ℓ by executions of s starting from $\mathcal{R}_0$ Chapter **19**
- Equational semantics: $\mathrm{lfp}^{\dot{\sqsubseteq}^{\vec{r}}}\,\mathsf{E}[\![\mathsf{P}]\!]\,\mathcal{R}_0 = \widehat{\mathcal{S}}^{\vec{r}}[\![\mathsf{P}]\!]\,\mathcal{R}_0$ Theorem 23.20
- Verification conditions: $\widehat{\mathcal{V}}^{\vec{r}}[\![\mathsf{s}]\!]\,\mathcal{R}_0\,\mathcal{I} \triangleq (\mathsf{E}[\![\mathsf{s}]\!]\,\mathcal{R}_0(\mathcal{I}) \dot{\sqsubseteq}^{\vec{r}} \mathcal{I})$, $\mathcal{I} \in \mathbb{L} \to \wp(\mathbb{E}\mathrm{v})$ (25.22)
- Inductive invariant: $\widehat{\mathcal{I}}^{\vec{r}}[\![\mathsf{s}]\!]\,\mathcal{I} \triangleq \widehat{\mathcal{V}}^{\vec{r}}[\![\mathsf{s}]\!]\,\mathcal{I}(\mathrm{at}[\![\mathsf{s}]\!])\,\mathcal{I}$ (25.30)
- Hoare triple abstraction:

$$\widehat{\mathsf{H}}^{\vec{r}}[\![\mathsf{s}]\!] \triangleq \alpha(\widehat{\mathcal{I}}^{\vec{r}}[\![\mathsf{s}]\!]) = \{\{\mathcal{I}(\mathrm{at}[\![\mathsf{s}]\!])\}\mathsf{s}\{\mathcal{I}(\mathrm{after}[\![\mathsf{s}]\!])\} \mid \mathcal{I} \in \mathbb{L} \to \wp(\mathbb{E}\mathrm{v}) \wedge \widehat{\mathcal{I}}^{\vec{r}}[\![\mathsf{s}]\!]\mathcal{I}\}$$

Since $\widehat{\mathcal{V}}^{\vec{r}}/\widehat{\mathcal{I}}^{\vec{r}}$ is defined structurally, $\widehat{\mathsf{H}}^{\vec{r}}$ can be defined structurally and the set $\widehat{\mathsf{H}}^{\vec{r}}[\![\mathsf{s}]\!]$ can be defined by rules

Informal introduction to Hoare logic

Introduction to classical Hoare logic

- Hoare logic can be used to prove a relation between initial and final states of a program component `S`.
- $\{\!|Q|\!\}$ `S` $\{\!|R|\!\}$ means that if execution of `S` starts in an initial state satisfying a precondition predicate Q and this execution terminates, then upon termination, if ever, the final state satisfies the postcondition predicate R.
- Examples: $\{\!|x = 0|\!\}$ `x = 1 ;` $\{\!|x = 1|\!\}$ and $\{\!|\mathtt{tt}|\!\}$ `if (x != 0) x = 0 ;` $\{\!|x = 0|\!\}$.
- Non-termination is expressible since $\{\!|\mathtt{tt}|\!\}$ `S` $\{\!|\mathtt{ff}|\!\}$ holds if and only if statement `S` never terminates.
- Example: $\{\!|\mathtt{tt}|\!\}$ `x = 0 ; while (x == 0) ;` $\{\!|\mathtt{ff}|\!\}$ and $\mathtt{ff} \Rightarrow (x = 42)$ so that $\{\!|\mathtt{tt}|\!\}$ `x = 0 ; while (x == 0) ;` $\{\!|x = 42|\!\}$ since anything holds on loop exit which is not reachable.
- Hoare logic is for partial correctness, termination is abstracted away hence not expressible.
- So the problem of proving $\{\!|Q|\!\}$ `S` $\{\!|R|\!\}$ is undecidable.

Hoare triples with exceptions, informally

- For break statements, $\{\!|Q|\!\}$ `S` $\{\!|R \mid T|\!\}$ states that precondition R holds upon normal termination of `S` while break condition T holds upon termination of program component `S` by a break outside this program component `S`.
- Examples:
  - $\{\!|\mathtt{tt}|\!\}$`if (x == 0) break ; else x = 1 ;`$\{\!|x = 1 \mid x = 0|\!\}$
  - $\{\!|\mathtt{tt}|\!\}$`x = 1 ;`$\{\!|x = 1 \mid \mathtt{ff}|\!\}$, and $\{\!|\mathtt{tt}|\!\}$`x = 1 ;`$\{\!|x = 1 \mid x = 42|\!\}$ since $\mathtt{ff} \Rightarrow (x = 42)$ so anything holds on an escape which is impossible.
- $\{\!|Q|\!\}$ `S` $\{\!|R|\!\}$ is an abbreviation for $\{\!|Q|\!\}$ `S` $\{\!|R \mid \mathtt{ff}|\!\}$ *i.e.* there is no possible termination by a break statement outside `S`.
- $T = \mathtt{ff}$ means that there is no possible escape from `S` by a break.
- This is the case if `S` has no break statement or its break statements are all captured by some iteration statement.

Relational Hoare triples, informally

- We would also like to express relations between initial and final values
- Example: $\{\!|x = x_0|\!\}$ `x = x + 1 ;` $\{\!|x = x_0 + 1|\!\}$.
- So we represent predicates by relations Q, R, T between environments.
- $\langle \rho_0, \rho \rangle \in R$ means that if ρ_0 is an initial environment (*i.e.* $\rho_0(\mathtt{x}) = x_0$) then ρ is the current environment at program point to which R is attached (*i.e.* $\rho(\mathtt{x}) = x$).

Differences with traditional Hoare triples

- We differ from the tradition [Hoare, 1969] in that

  (A) The T component accounts for possible **`break ;`** statements in the statement `S`. Notice that its presence (when $\mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{tt}$) or absence ($\mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{ff}$) is determined purely syntactically, without any reference to the semantics of statement `S`;

  (B) The properties $Q, R, T \in \wp(\mathbb{E}\mathbb{v}^{\mathcal{Q}})$ are represented by sets and not expressed in a first order logic.

  (C) We generalize to an arbitrary abstract domain, not necessarily $\wp(\mathbb{E}\mathbb{v}^{\mathcal{Q}})$.

en.wikipedia.org/wiki/Hoare_logic

Inexpressivity (1)

- "Inexpressivity" means that some program properties cannot be expressed in the logic
- The inexpressivity problem shows up in Hoare logic when using a logic to express invariants
- One reason for inexpressivity is the iteration.
- For example a logic with arithmetic addition operation $+$ by missing the multiplication $\times$ will be inexpressive because a program can compute a multiplication with an iteration using addition only.
  So $\times$ must be added to the logic for expressivity.
  But then exponentiation will be computable but not expressible in the logic, *etc*.

Inexpressivity (2)

- Another source of inexpressivity comes from the fact that properties of entities can be expressed in first order logic only by giving a name to these entities using an identifier.
- For example one can express "x is odd" is a first-order logic with 1, $+$, and $\times$ as $\exists k \,.\, x = 2 \times k + 1$. However, one cannot express "to be odd" in this logic.
- Some semantics can manipulate entities that are not named by an identifier or obtained by applying selection operations from an identifier.
- This is the case of [Jones and Muchnick, 1978] which directly leads to an inexpressivity result [Clarke Jr., 1979], which can be got around by reasoning directly on the semantic entities (the environment in our case).

Hoare logic is an abstract interpretation of the verification semantics

Hoare triples, formally

- The information on the semantics of a program component s provided by a Hoare triple $\{\!|Q|\!\}\ \mathsf{s}\ \{\!|R \mid T|\!\}$ is
  - Q attached to $\mathsf{at}[\![\mathsf{s}]\!]$,
  - R attached to $\mathsf{after}[\![\mathsf{s}]\!]$, and,
  - in case s has a break which escapes outside of s (so $\mathsf{escape}[\![\mathsf{s}]\!] = \mathtt{tt}$ and $\mathsf{break\text{-}to}[\![\mathsf{s}]\!] \neq \mathsf{after}[\![\mathsf{s}]\!]$ by Lemma 4.18), T is attached to its break label $\mathsf{break\text{-}to}[\![\mathsf{s}]\!]$.
  - Otherwise $\mathsf{escape}[\![\mathsf{s}]\!] = \mathtt{ff}$ and T is meaningless so can be chosen arbitrarily.

Abstract Hoare triples, formally

- We formalize Hoare logic for an arbitrary well-defined abstract domain

$$\mathbb{D}^\natural = \langle \mathbb{P}^\natural, \sqsubseteq^\natural, \bot^\natural, \sqcup^\natural, \mathsf{assign}_\natural[\![\mathtt{x}, \mathtt{A}]\!], \mathsf{test}^\natural[\![\mathtt{B}]\!], \overline{\mathsf{test}}^\natural[\![\mathtt{B}]\!] \rangle$$

  satisfying Definition 21.1, typically $\mathbb{P}^\natural = \wp(\mathbb{E}\mathbb{v}^{\vec{\mathtt{v}}})$.

- Therefore the extended Hoare triple notation is defined as

$$\{\!|Q|\!\}\ \mathtt{s}\ \{\!|R \mid T|\!\} \triangleq \{\langle Q, R, (\!|\, \mathsf{escape}[\![\mathtt{s}]\!] \mathbin{?} T \mathbin{:} U \,|\!)\rangle \mid U \in \mathbb{P}^\natural\} \tag{26.1}$$

- The domain $\mathbb{H}\mathrm{t}^\natural[\![\mathtt{s}]\!]$ of all Hoare triples is

$$\mathbb{H}\mathrm{t}^\natural[\![\mathtt{s}]\!] \triangleq \{\{\!|Q|\!\}\ \mathtt{s}\ \{\!|R \mid T|\!\} \mid Q, R, T \in \mathbb{P}^\natural\}.$$

Abstraction of an invariant into a Hoare triple

A Hoare triple is the abstraction $\alpha^{\mathsf{H}}[\![\mathsf{S}]\!](\mathcal{I})$ of an invariant $\mathcal{I} \in \mathsf{labx}[\![\mathsf{S}]\!] \to \mathbb{P}^{\natural}$ by

$$\alpha^{\mathsf{H}}[\![\mathsf{S}]\!] \quad \in \quad (\mathsf{labx}[\![\mathsf{S}]\!] \to \mathbb{P}^{\natural}) \to \mathbb{H}\mathbb{t}^{\natural}[\![\mathsf{S}]\!]$$

where the abstraction of an invariant $\mathcal{I}$ into a Hoare triple $\alpha^{\mathsf{H}}[\![\mathsf{S}]\!](\mathcal{I})$ is

$$\alpha^{\mathsf{H}}[\![\mathsf{S}]\!](\mathcal{I}) \quad \triangleq \quad \{\!|\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!])|\!\}\ \mathsf{S}\ \{\!|\mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]) \,;\, \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])|\!\} \tag{26.2}$$

Valid Hoare triples

- A Hoare triple is a specification that may be valid or invalid.
- For example, $\{\!\{\{\rho \mid \rho(\mathtt{x}) = 0\}\}\!\}$ `x = 1 ;` $\{\!\{\{\rho \mid \rho(\mathtt{x}) = 2\} \mid \varnothing\}\!\}$ is invalid since the value of variable `x` cannot be 2 after being assigned 1.
- A Hoare triple is valid if and only if it is the abstraction of an inductive invariant.
- The Hoare logic of a statement `s` is the set of all valid Hoare triples of this statement so

$$\widehat{\mathsf{H}}^{\natural}[\![\mathtt{s}]\!] \quad \triangleq \quad \{\alpha^{\mathsf{H}}[\![\mathtt{s}]\!](\mathcal{I}) \mid \widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathtt{s}]\!]\,\mathcal{I}\}. \tag{26.3}$$

where $\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathtt{s}]\!]\,\mathcal{I}$ checks that an invariant $\mathcal{I} \in \mathbb{L} \to \mathbb{P}^{\natural}$ is inductive.

$$\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathtt{s}]\!] \quad \in \quad (\mathbb{L} \to \mathbb{P}^{\natural}) \to \mathbb{B}$$

has been defined in (25.30) and (25.12) to (25.21).

Hoare logic is an abstract interpretation of the invariance semantics

- $\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!]$ is an abstract interpretation of the invariance semantics $\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{s}]\!]$ of a program component s

$$\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!] \quad \triangleq \quad \alpha^{\mathbb{Ht}}[\![\mathsf{s}]\!](\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{s}]\!]) \tag{26.3}$$

by the abstraction

$$\alpha^{\mathbb{Ht}}[\![\mathsf{s}]\!](\mathsf{I}) \quad \triangleq \quad \{\alpha^{\mathsf{H}}[\![\mathsf{s}]\!](\mathcal{I}) \mid \mathsf{I}(\mathcal{I})\}$$

such that

$$\langle \mathbb{P}^{\natural} \to (\mathbb{L} \to \mathbb{P}^{\natural}) \to \mathbb{B}, \Subset \rangle \underset{\alpha^{\mathbb{Ht}}[\![\mathsf{s}]\!]}{\overset{\gamma^{\mathbb{Ht}}[\![\mathsf{s}]\!]}{\leftrightarrows}} \langle \wp(\mathbb{Ht}^{\natural}[\![\mathsf{s}]\!]), \supseteq \rangle.$$

Hoare logic rules

Rule for a program $\mathtt{P} ::= \mathtt{Sl}$

$$\frac{\{\!|Q|\!\}\ \mathtt{Sl}\ \{\!|R \mid T|\!\}}{\{\!|Q|\!\}\ \mathtt{P}\ \{\!|R \mid T|\!\}} \tag{26.7}$$

Rule for a statement list $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$

$$\frac{\{\!|Q|\!\}\ \mathtt{Sl}'\ \{\!|R \mid T|\!\},\quad \{\!|R|\!\}\ \mathtt{S}\ \{\!|S \mid T|\!\}}{\{\!|Q|\!\}\ \mathtt{Sl}\ \{\!|S \mid T|\!\}} \tag{26.8}$$

Rule for an empty statement list $\mathtt{Sl} ::= \epsilon$

$$\{\!|Q|\!\}\ \epsilon\ \{\!|Q \mid T|\!\} \tag{26.9}$$

Rule for an assignment statement $\mathtt{S ::= x = E ;}$

$$\frac{\mathsf{assign}_{\sqsupset}[\![x, \mathtt{E}]\!]\, Q \sqsubseteq^{\sqsupset} R}{\{\!|Q|\!\}\ \mathtt{x = E ;}\ \{\!|R \mid T|\!\}} \tag{26.10}$$

Rule for a skip statement $\mathtt{S ::= ;}$

$$\frac{Q \sqsubseteq^{\sqsupset} R}{\{\!|Q|\!\}\ \mathtt{;}\ \{\!|R \mid T|\!\}} \tag{26.11}$$

Rule for a conditional statement $\mathtt{S ::= if\ (B)\ S}_t$

$$\frac{\mathsf{test}^{\sqsupset}[\![\mathtt{B}]\!]\, Q \sqsubseteq^{\sqsupset} Q', \quad \{\!|Q'|\!\}\ \mathtt{S}_t\ \{\!|R \mid T|\!\}, \quad \overline{\mathsf{test}}^{\sqsupset}[\![\mathtt{B}]\!]\, Q \sqsubseteq^{\sqsupset} R}{\{\!|Q|\!\}\ \mathtt{if\ (B)\ S}_t\ \{\!|R \mid T|\!\}} \tag{26.12}$$

Rule for a conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t\ \mathtt{else\ S}_f$

$$\frac{\mathsf{test}^{\natural}[\![\mathtt{B}]\!]Q \sqsubseteq^{\natural} Q_t \wedge \{\!|Q_t|\!\}\ \mathtt{S}_t\ \{\!|R \mid T|\!\} \wedge \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]Q \sqsubseteq^{\natural} Q_f \wedge \{\!|Q_f|\!\}\ \mathtt{S}_f\ \{\!|R \mid T|\!\}}{\{\!|Q|\!\}\ \mathtt{S}\ \{\!|R \mid T|\!\}} \tag{26.13}$$

Rule for an iteration statement $\mathtt{S} ::= \mathtt{while}^{\ell}\ \mathtt{(B)\ S}_b$

$$\frac{\mathsf{test}^{\natural}[\![\mathtt{B}]\!]\ Q \sqsubseteq^{\natural} Q_b,\ \{\!|Q_b|\!\}\ \mathtt{S}_b\ \{\!|Q \mid R|\!\},\ \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!]\ Q \sqsubseteq^{\natural} R}{\{\!|Q|\!\}\ \mathtt{while\ (B)\ S}_b\ \{\!|R \mid T|\!\}} \tag{26.14}$$

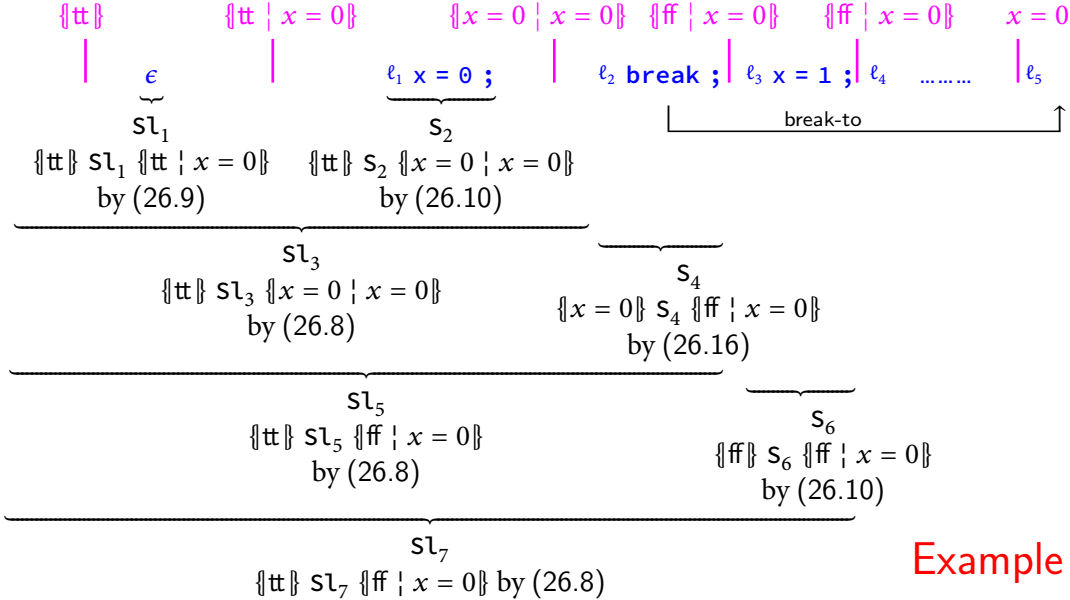
Rule for a break statement S ::= **break ;**

$$\frac{Q \sqsubseteq^{\natural} T}{\{\!|Q|\!\}\ \texttt{break ;}\ \{\!|R \mid T|\!\}} \tag{26.16}$$

Rule for a compound statement S ::= { Sl }

$$\frac{\{\!|Q|\!\}\ \texttt{Sl}\ \{\!|R \mid T|\!\}}{\{\!|Q|\!\}\ \texttt{\{ Sl \}}\ \{\!|R \mid T|\!\}} \tag{26.17}$$

No consequence rule (we know where to apply it!)



Example

Calculational design of Hoare logic rules

Principle of the calculational design of Hoare logic rules

- By (26.3), we have $\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!] \triangleq \alpha^{\mathbb{Ht}}[\![\mathsf{s}]\!](\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{s}]\!])$ so we can infer Hoare logic structural rules by calculational design.
- This consists in calculating the set of all valid Hoare triples $\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!] \triangleq \alpha^{\mathbb{Ht}}[\![\mathsf{s}]\!](\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{s}]\!])$ from the structural definition of $\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{s}]\!]$ of a program component s.
- We proceed by structural induction on this program component s.
- We get a definition of $\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!]$ as a function of the subcomponents $\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}']\!]$, $\mathsf{s}' \lhd \mathsf{s}$.
- Expressing this definition of $\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!]$ as a structural rule-based Definition 16.23. (There is no need for fixpoint/inductive definitions which have already been eliminated in Chapter **25** for $\widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{s}]\!]$ using the fixpoint induction Theorem 24.1.)

Rule for an assignment statement $\mathsf{S} ::= \mathsf{x} = \mathsf{E}\ ;$

$$\frac{\mathsf{assign}_{\natural}[\![x, \mathsf{E}]\!]\ Q \sqsubseteq^{\natural} R}{\{\!|Q|\!\}\ \mathsf{x} = \mathsf{E}\ ;\ \{\!|R \mid T|\!\}} \tag{26.10}$$

Proof of (26.10)

$\widehat{\mathsf{H}}^{\natural}[\![\mathsf{S}]\!]$

$= \{\alpha^{\mathsf{H}}[\![\mathsf{S}]\!](\mathcal{I}) \mid \widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{S}]\!]\ \mathcal{I}\}$ ⟅(26.3)⟆

$= \{\{\!|\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!])|\!\}\ \mathsf{S}\ \{\!|\mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]) \mid \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])|\!\} \mid \widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{S}]\!]\ \mathcal{I}\}$ ⟅(26.2)⟆

$= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\mathsf{escape}[\![\mathsf{S}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!]) \mathbin{:} U|\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{S}]\!]\ \mathcal{I}\}$ ⟅(26.1)⟆

$= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\mathsf{escape}[\![\mathsf{S}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!]) \mathbin{:} U|\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \mathsf{assign}_{\natural}[\![x, \mathsf{E}]\!]\ \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\natural} \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\}$ ⟅(25.30) and (25.14)⟆

$= \{\{\langle Q,\ R,\ (\!|\mathsf{escape}[\![\mathsf{S}]\!] \mathbin{?} T \mathbin{:} U|\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \mathsf{assign}_{\natural}[\![x, \mathsf{E}]\!]\ Q \sqsubseteq^{\natural} R \wedge T \in \mathbb{P}^{\natural}\}$

⟅letting $Q = \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!])$, $R = \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])$, $T = \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])$, and $\mathsf{escape}[\![\mathsf{S}]\!] = \mathsf{ff}$⟆

$= \{\{\!|Q|\!\}\ \mathsf{S}\ \{\!|R \mid T|\!\} \mid \mathsf{assign}_{\natural}[\![x, \mathsf{E}]\!]\ Q \sqsubseteq^{\natural} R \wedge T \in \mathbb{P}^{\natural}\}$ ⟅(26.1)⟆ □

Rule for a break statement $\mathtt{S} ::= \mathtt{break}\ \mathtt{;}$

$$\frac{Q \sqsubseteq^{\natural} T}{\{\!|Q|\!\}\ \mathtt{break}\ \mathtt{;}\ \{\!|R \mid T|\!\}} \tag{26.16}$$

$\Big($defining $\widehat{\mathsf{H}}^{\natural}[\![\mathtt{S}]\!]$ by the inference rules $\left\{\dfrac{\varnothing}{\{\!|Q|\!\}\ \mathtt{break}\ \mathtt{;}\ \{\!|R \mid T|\!\}} \;\middle|\; Q \sqsubseteq^{\natural} T\right\}\Big)$.

Proof of (26.16)

$$
\begin{aligned}
&\widehat{\mathsf{H}}^{\natural}[\![\mathsf{s}]\!] \\
&= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{s}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{s}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{s}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{s}]\!]) \mathbin{:} U\ |\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \widehat{\mathscr{F}}^{\natural}[\![\mathsf{s}]\!]\ \mathcal{I}\} \\
&\qquad\qquad \text{⁅(26.3), (26.2), and (26.1)⁆} \\
&= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{s}]\!]), \mathcal{I}(\mathsf{after}[\![\mathsf{s}]\!]), (\!|\ \mathsf{escape}[\![\mathsf{s}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{s}]\!]) \mathbin{:} U\ |\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \widehat{\mathscr{V}}^{\vec{\mathrm{e}}}[\![\mathsf{s}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{s}]\!])\mathcal{I}\} \\
&\qquad\qquad \text{⁅(25.30)⁆} \\
&= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{s}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{s}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{s}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{s}]\!]) \mathbin{:} U\ |\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \mathcal{I}(\mathsf{at}[\![\mathsf{s}]\!]) \sqsubseteq^{\natural} \\
&\quad \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{s}]\!])\} \qquad\qquad \text{⁅(25.20′)⁆} \\
&= \{\langle Q,\ R,\ (\!|\ \mathsf{escape}[\![\mathsf{s}]\!] \mathbin{?} T \mathbin{:} \varnothing\ |\!)\rangle \mid Q \sqsubseteq^{\natural} T\} \\
&\qquad\qquad \text{⁅letting } Q = \mathcal{I}(\mathsf{at}[\![\mathsf{s}]\!]),\ R = \mathcal{I}(\mathsf{after}[\![\mathsf{s}]\!]), \text{ and } T = \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{s}]\!])\text{⁆} \\
&= \{\{\!|Q|\!\}\ \texttt{break}\ \texttt{;}\ \{\!|R \mid T|\!\} \mid Q \sqsubseteq^{\natural} T\} \qquad\qquad \text{⁅(26.1)⁆}\ \square
\end{aligned}
$$

Rule for an iteration statement $\mathtt{S} ::= \mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$

$$\frac{\mathrm{test}^{\natural}[\![\mathtt{B}]\!]\, Q \sqsubseteq^{\natural} Q_b,\ \{\!|Q_b|\!\}\ \mathtt{S}_b\ \{\!|Q \mid R|\!\},\ \overline{\mathrm{test}}^{\natural}[\![\mathtt{B}]\!]\, Q \sqsubseteq^{\natural} R}{\{\!|Q|\!\}\ \mathtt{while\ (B)}\ \mathtt{S}_b\ \{\!|R \mid T|\!\}} \tag{26.14}$$

- This defines $\widehat{\mathrm{H}}^{\natural}[\![\mathtt{S}]\!]$ by the inference rules

$$\left\{ \frac{\varnothing}{\{\!|Q|\!\}\ \mathtt{S}\ \{\!|R \mid T|\!\}} \;\middle|\; \mathrm{test}^{\natural}[\![\mathtt{B}]\!]\, Q \sqsubseteq^{\natural} Q_b \wedge \{\!|Q_b|\!\}\ \mathtt{S}_b\ \{\!|Q|\!\} \in \widehat{\mathrm{H}}^{\natural}[\![\mathtt{S}_b]\!] \wedge \overline{\mathrm{test}}^{\natural}[\![\mathtt{B}]\!]\, Q \sqsubseteq^{\natural} R \right\}$$

Proof of (26.14)

$$
\begin{aligned}
&\widehat{\mathsf{H}}^{\natural}[\![\mathsf{S}]\!] \\
&= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!]) \mathbin{:} U\ |\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \widehat{\boldsymbol{\mathcal{F}}}^{\natural}[\![\mathsf{S}]\!]\,\mathcal{I}\} \\
&\qquad\qquad \text{〈(26.3), (26.2), and (26.1)〉} \\
&= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]), \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]), (\!|\ \mathsf{escape}[\![\mathsf{S}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!]) \mathbin{:} U\ |\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \widehat{\boldsymbol{\mathcal{V}}}^{\vec{e}}[\![\mathsf{S}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!])\mathcal{I}\} \\
&\qquad\qquad \text{〈(25.30)〉} \\
&= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!] \mathbin{?} \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!]) \mathbin{:} U\ |\!)\rangle \mid U \in \mathbb{P}^{\natural}\} \mid \\
&\quad\ \mathsf{test}^{\natural}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\natural} \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \widehat{\boldsymbol{\mathcal{V}}}^{\natural}[\![\mathsf{S}_b]\!](\mathsf{test}^{\natural}[\![\mathsf{B}]\!]\mathcal{I}_{\mathsf{at}[\![\mathsf{S}]\!]})\ \mathcal{I} \wedge \overline{\mathsf{test}}^{\natural}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\natural} \\
&\quad\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\} \\
&\qquad\qquad \text{〈(25.19′)〉}
\end{aligned}
$$

$\{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!]\ ?\ \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])\ :\ U\ |\!)\rangle \mid U \in \mathbb{P}^{\rm o}\} \mid \mathsf{test}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \widehat{\mathscr{V}}^{\rm o}[\![\mathsf{S}_b]\!](\mathsf{test}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}_{\mathsf{at}[\![\mathsf{S}]\!]})\ \mathcal{I} \wedge \overline{\mathsf{test}}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\}$

$= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!]\ ?\ \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])\ :\ U\ |\!)\rangle \mid U \in \mathbb{P}^{\rm o}\} \mid \mathsf{test}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \widehat{\mathscr{F}}^{\rm o}[\![\mathsf{S}_b]\!]\ \mathcal{I} \wedge \overline{\mathsf{test}}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\}$

$\wr$ **Lemma 25.31** $\widehat{\mathscr{V}}^{\vec{\rm o}}[\![\mathsf{S}]\!]\ \mathcal{R}_0\ \mathcal{I} = \mathcal{R}_0 \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \wedge \widehat{\mathscr{F}}^{\vec{\rm o}}[\![\mathsf{S}]\!]\ \mathcal{I}.$ $\int$

$= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!]\ ?\ \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])\ :\ U\ |\!)\rangle \mid U \in \mathbb{P}^{\rm o}\} \mid \mathsf{test}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \alpha^{\rm H}[\![\mathsf{S}_b]\!](\mathcal{I}) \in \widehat{\rm H}^{\rm o}[\![\mathsf{S}_b]\!] \wedge \overline{\mathsf{test}}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\}$

$\wr$(26.3)$\int$

$= \{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!]\ ?\ \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])\ :\ U\ |\!)\rangle \mid U \in \mathbb{P}^{\rm o}\} \mid \mathsf{test}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \{\!|\mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!])|\!\}\ \mathsf{S}_b\ \{\!|\mathcal{I}(\mathsf{after}[\![\mathsf{S}_b]\!]) \mid \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}_b]\!])|\!\} \in \widehat{\rm H}^{\rm o}[\![\mathsf{S}_b]\!] \wedge \overline{\mathsf{test}}^{\rm o}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\rm o} \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\}$

$\wr$(26.2)$\int$

$$\{\{\langle \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]),\ \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]),\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!]\ ?\ \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!])\ :\ U\ |\!)\rangle \mid U \in \mathbb{P}^{\sqsupset}\} \mid \mathsf{test}^{\sqsupset}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\sqsupset} \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \{\!|\mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!])|\!\}\ \mathsf{S}_b\ \{\!|\mathcal{I}(\mathsf{after}[\![\mathsf{S}_b]\!])\ ;\ \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}_b]\!])|\!\} \in \widehat{\mathsf{H}}^{\sqsupset}[\![\mathsf{S}_b]\!] \wedge \overline{\mathsf{test}}^{\sqsupset}[\![\mathsf{B}]\!]\mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) \sqsubseteq^{\sqsupset} \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!])\}$$

$$= \{\{\langle Q,\ R,\ (\!|\ \mathsf{escape}[\![\mathsf{S}]\!]\ ?\ T\ :\ U\ |\!)\rangle \mid U \in \mathbb{P}^{\sqsupset}\} \mid \mathsf{test}^{\sqsupset}[\![\mathsf{B}]\!]Q \sqsubseteq^{\sqsupset} Q_b \wedge \{\!|Q_b|\!\}\ \mathsf{S}_b\ \{\!|Q\ ;\ R|\!\} \in \widehat{\mathsf{H}}^{\sqsupset}[\![\mathsf{S}_b]\!] \wedge \overline{\mathsf{test}}^{\sqsupset}[\![\mathsf{B}]\!]Q \sqsubseteq^{\sqsupset} R\}$$

$$\text{〖letting } Q = \mathcal{I}(\mathsf{at}[\![\mathsf{S}]\!]) = \mathcal{I}(\mathsf{after}[\![\mathsf{S}_b]\!]),\ T = \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}]\!]),\ R = \mathcal{I}(\mathsf{after}[\![\mathsf{S}]\!]) = \mathcal{I}(\mathsf{break\text{-}to}[\![\mathsf{S}_b]\!]),\ Q_b = \mathcal{I}(\mathsf{at}[\![\mathsf{S}_b]\!]) \text{ 〗}$$

$$= \{\{|Q|\}\ \mathsf{S}\ \{|R\ ;\ T|\} \mid \mathsf{test}^{\sqsupset}[\![\mathsf{B}]\!]\ Q \sqsubseteq^{\sqsupset} Q_b \wedge \{\!|Q_b|\!\}\ \mathsf{S}_b\ \{\!|Q\ ;\ R|\!\} \in \widehat{\mathsf{H}}^{\sqsupset}[\![\mathsf{S}_b]\!] \wedge \overline{\mathsf{test}}^{\sqsupset}[\![\mathsf{B}]\!]\ Q \sqsubseteq^{\sqsupset} R\}$$

〖(26.1)〗 □

Auxiliary rules

- Derived from existing rules by structural induction
- Consequence rule (sound, already integrated in our rules)

$$\frac{Q' \sqsubseteq^{\natural} Q, \quad \{\!|Q|\!\} \; \mathsf{s} \; \{\!|R \mid T|\!\}, \quad R \sqsubseteq^{\natural} R', \quad T \sqsubseteq^{\natural} T'}{\{\!|Q'|\!\} \; \mathsf{s} \; \{\!|R' \mid T'|\!\}}.$$

- Disjunction and conjunction rule (sound for $\wp(\mathbb{E}^{\vec{\mathscr{Q}}})$ but not in general [P. Cousot, R. Cousot, Logozzo, and Barnett, 2012])

$$\frac{\forall i \in \Delta \,.\, \{\!|Q_i|\!\} \; \mathsf{s} \; \{\!|R_i|\!\}}{\{\!|\bigcup_{i\in\Delta} Q_i|\!\} \; \mathsf{s} \; \{\!|\bigcup_{i\in\Delta} R_i|\!\}} \qquad \frac{\forall i \in \Delta \,.\, \{\!|Q_i|\!\} \; \mathsf{s} \; \{\!|R_i|\!\}}{\{\!|\bigcap_{i\in\Delta} Q_i|\!\} \; \mathsf{s} \; \{\!|\bigcap_{i\in\Delta} R_i|\!\}}$$

Conclusion

Conclusion

- The success of Turing/Floyd/Naur invariance verification method of Chapter **25** is that it is the most abstract, sound, and complete invariance proof method.
  - Being the most abstract, it cannot be further simplified.
  - Being sound, it is infallible.
  - Being complete, it is always applicable and never fails.
- The success of Hoare logic of Chapter **26** is that it is a logical reformulation and, compared to previous formulations of invariance proofs, that it is by structural induction on programs.
- However, no one uses Hoare logic to make derivations like in a deductive definition of Chapter **16** (Fixpoint, deductive, inductive, structural, coinductive, and bi-inductive definitions), since as shown in his Hoare logic formal proof example, this would be too heavy
- So everybody use invariants and the simple verification conditions of Chapter **25**, which we have shown to be perfectly equivalent

Conclusion (cont'd)

- The original definition of Hoare logic [Hoare, 1969] postulated rules to prove that a Hoare triple $\{\!\{Q\}\!\}$ s $\{\!\{R\}\!\}$ is valid, by structural induction on the statement s.
- These rules where later proved sound and relatively complete [Cook, 1978, 1981] where the "relative" means that the considered first-order logic can express the inductive invariant.
- The Hoare logic that we calculated is different from the classical one [Hoare, 1969, 1983, 2009] because of the **`break ;`**.

Conclusion (cont'd)

- Postulating rules to derive inductive invariants [Floyd, 1967] or valid Hoare triples [Hoare, 1969] is a way to "assign meaning to programs" [Floyd, 1967] that is to define their semantics (called the "axiomatic semantics").
- However this axiomatic semantics is often too abstract for many applications such as static analysis.
- For example [Jourdan, Laporte, Blazy, Leroy, and Pichardie, 2015] do not consider execution traces so cannot fully account for the soundness of Astrée [Bertrane, P. Cousot, R. Cousot, Feret, Mauborgne, Miné, and Rival, 2015].

Conclusion (cont'd)

- We have inferred structural Hoare logic rules defining the set $\widehat{\mathsf{H}}^{\natural}[\![\mathtt{s}]\!]$ of all valid Hoare triples for a statement $\mathtt{s}$ by calculational design using an abstraction $\alpha^{\mathbb{Htt}}[\![\mathtt{s}]\!](\widehat{\mathscr{F}}^{\natural}[\![\mathtt{s}]\!])$ of the structural reachability semantics $\widehat{\mathscr{F}}^{\natural}[\![\mathtt{s}]\!]$.

- Although this calculational design methodology might appear superfluous for an already known logic, it is effective to design an invariance proof methods for new languages or semantic models [Alglave and P. Cousot, 2017].

Bibliography I

Alglave, Jade and Patrick Cousot (2017). "Ogre and Pythia: an invariance proof method for weak consistency models". In: *POPL*. ACM, pp. 3–18.

Bertrane, Julien, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, and Xavier Rival (2015). "Static Analysis and Verification of Aerospace Software by Abstract Interpretation". *Foundations and Trends in Programming Languages* 2.2-3, pp. 71–190.

Clarke Jr., Edmund M. (1979). "Programming Language Constructs for Which It Is Impossible To Obtain Good Hoare Axiom Systems". *J. ACM* 26.1, pp. 129–147.

Cook, Stephen A. (1978). "Soundness and Completeness of an Axiom System for Program Verification". *SIAM J. Comput.* 7.1, pp. 70–90.

— (1981). "Corrigendum: Soundness and Completeness of an Axiom System for Program Verification". *SIAM J. Comput.* 10.3, p. 612.

Bibliography II

Cousot, Patrick, Radhia Cousot, Francesco Logozzo, and Michael Barnett (2012). "An abstract interpretation framework for refactoring with application to extract methods with contracts". In: *OOPSLA*. ACM, pp. 213–232.

Floyd, Robert W. (1967). "Assigning meaning to programs". In: J.T. Schwartz, ed. *Proc. Symp. in Applied Math.* Vol. 19. Amer. Math. Soc., pp. 19–32.

Hoare, Charles Antony Richard (1969). "An Axiomatic Basis for Computer Programming". *Commun. ACM* 12.10, pp. 576–580. URL: http://doi.acm.org/10.1145/363235.363259.

— (1983). "An Axiomatic Basis for Computer Programming (Reprint)". *Commun. ACM* 26.1, pp. 53–56.

— (2009). "Viewpoint — Retrospective: an axiomatic basis for computer programming". *Commun. ACM* 52.10, pp. 30–32.

Bibliography III

Jones, Neil D. and Steven S. Muchnick (1978). "The Complexity of Finite Memory Programs with Recursion". *J. ACM* 25.2, pp. 312–321.

Jourdan, Jacques-Henri, Vincent Laporte, Sandrine Blazy, Xavier Leroy, and David Pichardie (2015). "A Formally-Verified C Static Analyzer". In: *POPL*. ACM, pp. 247–259.

Home work

Read Ch. **26** "Hoare logic" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you