Principles of Abstract Interpretation

MIT press

Ch. **8**, Program properties

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-08--program-properties-PrAbsInt.pdf

Chapter 8

Ch. **8**, Program properties

Design of a verification/analysis method for a programming language by abstract interpretation

- Define the syntax and operational semantics of the language
- Define program properties and the collecting semantics $\leftarrow$ these slides
- Define an abstraction of properties (preferably by a Galois connection)
  $\nwarrow$ 2 examples in these slides
- Calculate a sound (and possibly complete) abstract semantics by abstraction of the collecting semantics
- Define an abstract inductive proof method/analysis algorithm

The [complete boolean lattice] of properties of entities

Formal property

- A property is the set of elements that satisfy this property.
- Examples:
  - $\{2k + 1 \mid k \in \mathbb{N}\}$ is the property "to be an odd natural"
  - $\{2k \mid k \in \mathbb{Z}\}$ is the property "to be an even integer"
- Formally:
  - $\mathfrak{E}$ is a set of entities
  - A property of these entities is an element of $\wp(\mathfrak{E})$
  - Examples:
    - $\emptyset$ is false (ff)
    - $\mathfrak{E}$ is true (tt)
    - $e \in P$, $P \in \wp(\mathfrak{E})$ means "e has property P"

Comparing formal properties

- $P, Q \in \wp(\mathfrak{E})$ properties of entities $\mathfrak{E}$
- $e \in P$, element e *satisfies* property P, e *has property* P
- $P \subseteq Q$
  - P *implies* Q
  - P is a *stronger* property than Q (*i.e.* fewer entities satisfy P than Q)
  - $\emptyset$ is the strongest property
  - $\{e\}$ is the strongest property of element $e \in \mathfrak{E}$
    (*i.e.* $\forall P \in \wp(\mathfrak{E}) \;.\; e \in P \Leftrightarrow \{e\} \subseteq P$)
  - Q is a *weaker* property than P (*i.e.* more entities satisfy Q than P)
  - $\mathfrak{E}$ is the weakest property
    (*i.e.* $\forall P \in \wp(\mathfrak{E}) \;.\; P \subseteq \mathfrak{E}$)

The [complete boolean lattice] of formal properties

$$\langle \wp(\mathfrak{E}),\ \subseteq,\ \varnothing,\ \mathfrak{E},\ \cup,\ \cap,\ \neg \rangle$$

- $\wp(\mathfrak{E})$ properties of entities belonging to $\mathfrak{E}$
- $\subseteq$ implication
- $\varnothing$ false
- $\mathfrak{E}$ true
- $\cup$ disjonction, or
- $\cap$ conjunction, and
- $\neg$ negation, $\neg P \triangleq \mathfrak{E} \setminus P$

Program properties

Syntactic and semantic properties of a program

- Syntactic property: a property of the program text (considered as a string of characters, a syntactic tree, *etc*.), software metrology.
- Semantic property: a property of the semantic of programs, *i.e*. of a formalization of their executions.
- By [program] property, we mean a semantic property.

Semantic program properties

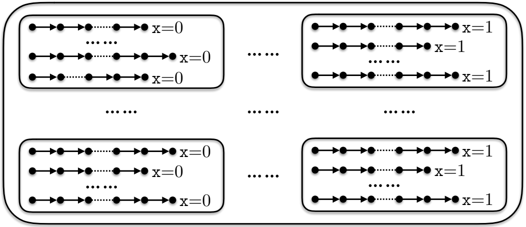
- The entities are semantics of program **P** *i.e.* sets of maximal traces $\mathfrak{S} = \wp(\mathbb{T}^{+\infty})$
- The *properties* are sets of semantics of program **P** *i.e.* *sets of sets of maximal traces* $\wp(\mathfrak{S}) = \wp(\wp(\mathbb{T}^{+\infty}))$

Example of semantic program property

$$\mathcal{P} \triangleq \wp(\{\pi \in \mathbb{T}^{+} \mid \varrho(\pi)\mathtt{x} = 0\}) \cup \wp(\{\pi \in \mathbb{T}^{+} \mid \varrho(\pi)\mathtt{x} = 1\}) \in \wp(\wp(\mathbb{T}^{+\infty}))$$

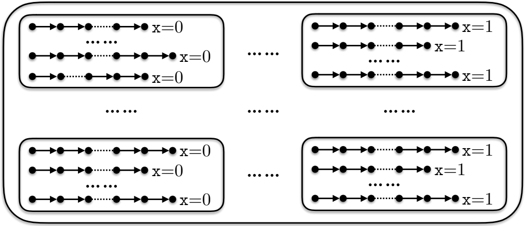
- "Program P has property $\mathcal{P}$" means "all executions of P always terminate with $\mathtt{x} = 0$ or all executions of P always terminate with $\mathtt{x} = 1$".

$\mathcal{P}$ =



Example of semantic program property (Cont'd)

P =



- Assume program P has this property so $\mathcal{S}^{+\infty}[\![\mathsf{P}]\!] \in P$.
- Executing program P once, we know the result of all other executions.
- If the execution terminates with $\mathsf{x} = 0$ (respectively $\mathsf{x} = 1$) the property P implies that all other possible executions will always terminate with $\mathsf{x} = 0$ (respectively $\mathsf{x} = 1$).

Collecting semantics

Collecting semantics

- The strongest semantic property of program P

$$\mathcal{S}^{\mathbb{C}}[\![\mathsf{P}]\!] \triangleq \{\mathcal{S}^{+\infty}[\![\mathsf{P}]\!]\} . \tag{8.6}$$

- Program P has property $P \in \wp(\wp(\mathbb{T}^{+\infty}))$ is
  - $\mathcal{S}^{+\infty}[\![\mathsf{P}]\!] \in P$, or equivalently
  - $\{\mathcal{S}^{+\infty}[\![\mathsf{P}]\!]\} \subseteq P$, or equivalently
  - $\mathcal{S}^{\mathbb{C}}[\![\mathsf{P}]\!] \subseteq P$ *i.e.* P is implied by the collecting semantics of program P.
- So we can use implication $\subseteq$ ($\Rightarrow$) instead of $\in$ (with no direct equivalent for predicates in logic).

Trace properties

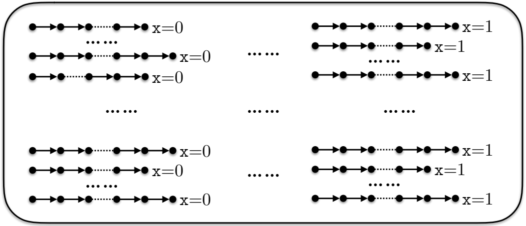
Trace properties

- By "program property" or "semantic property" most computer scientists refer to "trace properties"
- elements $\mathfrak{E} = \mathbb{T}^{+\infty}$, traces
- trace properties $\wp(\mathfrak{E}) = \wp(\mathbb{T}^{+\infty})$

Example of trace properties

- The program trace semantics $\mathcal{S}^{+\infty}[\![\mathsf{P}]\!] \triangleq \mathcal{S}^{+\infty}[\![\mathsf{P}]\!](\mathbb{T}^{+}) \in \wp(\mathbb{T}^{+\infty})$ is a trace property.
- $\{\pi \in \mathbb{T}^{+} \mid \varrho(\pi)\mathsf{x} = 0\} \in \wp(\mathbb{T}^{+\infty})$ is the trace property of "terminating with x=0".
- $\overline{P} = \{\pi \in \mathbb{T}^{+} \mid \varrho(\pi)\mathsf{x} \in \{0, 1\}\} \in \wp(\mathbb{T}^{+\infty})$ is the trace property of "terminating with x=0 or x=1".

$\overline{P}$ =

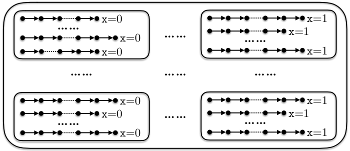


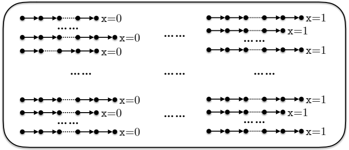
- Trace properties in $\wp(\mathbb{T}^{+\infty})$ are less expressive than semantic properties in $\wp(\wp(\mathbb{T}^{+\infty}))$

Abstraction of a semantic property into a trace property

- Any semantic property P can be abstracted into a less precise trace property $\alpha^{\mathbb{T}}(P)$ defined as

$$\begin{array}{rcl} \alpha^{\mathbb{T}} & \in & \wp(\wp(\mathbb{T}^{+\infty})) \rightarrow \wp(\mathbb{T}^{+\infty}) \\ \alpha^{\mathbb{T}}(P) & = & \bigcup P \end{array} \qquad \begin{array}{rcl} \gamma^{\mathbb{T}} & \in & \wp(\mathbb{T}^{+\infty}) \rightarrow \wp(\wp(\mathbb{T}^{+\infty})) \\ \gamma^{\mathbb{T}}(\overline{P}) & = & \wp(\overline{P}) \end{array}$$

$P =$ 

$\overline{P} = \alpha^{\mathbb{T}}(P) =$ 

- P and $\overline{P}$ both express that program executions always terminate with a boolean value for x.
- P is stronger since it expresses that the result is always the same while $\overline{P}$ doesn't.

Abstraction of a semantic property into a trace property (Cont'd)

- Galois connection $\langle\wp(\wp(\mathbb{T}^{+\infty})), \subseteq\rangle \xrightleftharpoons[\alpha^{\mathbb{T}}]{\gamma^{\mathbb{T}}} \langle\wp(\mathbb{T}^{+\infty}), \subseteq\rangle$
- Proof:

$$
\begin{array}{lll}
& \alpha^{\mathbb{T}}(P) \subseteq \overline{P} & \\
\Leftrightarrow & \bigcup P \subseteq \overline{P} & \wr\text{def. } \alpha^{\mathbb{T}}\wr \\
\Leftrightarrow & \{x \mid \exists X \in P \,.\, x \in X\} \subseteq \overline{P} & \wr\text{def. } \bigcup\wr \\
\Leftrightarrow & \forall X \in P \,.\, \forall x \in X \,.\, x \in \overline{P} & \wr\text{def. } \subseteq\wr \\
\Leftrightarrow & \forall X \in P \,.\, X \subseteq \overline{P} & \wr\text{def. } \subseteq\wr \\
\Leftrightarrow & P \subseteq \{X \mid X \subseteq \overline{P}\} & \wr\text{def. } \subseteq\wr \\
\Leftrightarrow & P \subseteq \wp(\overline{P}) & \wr\text{def. } \wp\wr \\
\Leftrightarrow & P \subseteq \gamma^{\mathbb{T}}(\overline{P}) & \wr\text{def. } \gamma^{\mathbb{T}}.\wr
\end{array}
$$

- $\alpha^{\mathbb{T}}$ is surjective (since $\alpha^{\mathbb{T}}(\{\overline{P}\}) = \overline{P}$).

Terminology

- trace properties are often called properties
- semantic properties are often called hyperproperties

Reachability properties

Reachability property

A relation $\mathcal{I}(\ell)$ between values of variables attached to each program point ℓ that holds whenever the program point ℓ is reached during execution

```
ℓ1  /* x = 0 */
    x = x + 1 ;
    while ℓ2 (tt) /* 1 ⩽ x ⩽ 2 */ {
ℓ3      /* 1 ⩽ x ⩽ 2 */
        x = x + 1 ;
        if ℓ4 (x > 2) /* 2 ⩽ x ⩽ 3 */
ℓ5          /* x = 3 */
            break ;
    }
ℓ6  /* x = 3 */
    ;
ℓ7  /* x = 3 */
```

$$\mathcal{I}(\ell_1) \triangleq \{\rho \in \mathbb{E}\mathrm{v} \mid \rho(\mathrm{x}) = 0\}$$
$$\mathcal{I}(\ell_2) \triangleq \mathcal{I}(\ell_3) \triangleq \{\rho \in \mathbb{E}\mathrm{v} \mid 1 \leqslant \rho(\mathrm{x}) \leqslant 2\}$$
$$\mathcal{I}(\ell_4) \triangleq \{\rho \in \mathbb{E}\mathrm{v} \mid 2 \leqslant \rho(\mathrm{x}) \leqslant 3\}$$
$$\mathcal{I}(\ell_5) \triangleq \mathcal{I}(\ell_6) \triangleq \mathcal{I}(\ell_7) \triangleq \{\rho \in \mathbb{E}\mathrm{v} \mid \rho(\mathrm{x}) = 3\}$$

Abstraction of a trace property into a reachability property

$$
\begin{array}{rcl}
\alpha^{\mathbb{I}} & \in & \wp(\mathbb{T}^{+\infty}) \longrightarrow (\mathbb{L} \longrightarrow \wp(\mathbb{E}\mathbb{v})) \\
\alpha^{\mathbb{I}}(\Pi) & \triangleq & \ell \mapsto \{\boldsymbol{\varrho}(\pi^{\ell}) \mid \exists \pi' \,.\, \pi^{\ell}\pi' \in \Pi\}
\end{array}
\tag{8.14}
$$

collects at each program point ℓ of each trace the possible values of the variables at that point.

Abstraction of a trace property into a reachability property (Cont'd)

- Galois connection $\langle \wp(\mathbb{T}^{+\infty}), \subseteq \rangle \xrightleftharpoons[\alpha^{\mathbb{I}}]{\gamma^{\mathbb{I}}} \langle (\mathbb{L} \to \wp(\mathbb{E}\mathbb{v})), \dot{\subseteq} \rangle$
- Proof:

$$
\begin{array}{lll}
 & \alpha^{\mathbb{I}}(\Pi) \dot{\subseteq} \mathcal{I} & \\
\Leftrightarrow & \ell \mapsto \{\varrho(\pi\ell) \mid \exists \pi' \,.\, \pi\ell\pi' \in \Pi\} \dot{\subseteq} \mathcal{I} & \text{(def. } \alpha^{\mathbb{I}}\text{)} \\
\Leftrightarrow & \forall \ell \,.\, \{\varrho(\pi\ell) \mid \exists \pi' \,.\, \pi\ell\pi' \in \Pi\} \subseteq \mathcal{I}(\ell) & \text{(pointwise def. } \dot{\subseteq}\text{)} \\
\Leftrightarrow & \forall \ell \,.\, \{\varrho(\pi\ell) \mid \exists \overline{\pi} \in \Pi \,.\, \exists \pi' \,.\, \overline{\pi} = \pi\ell\pi'\} \subseteq \mathcal{I}(\ell) & \text{(def. } \in\text{)} \\
\Leftrightarrow & \forall \ell \,.\, \forall \overline{\pi} \in \Pi \,.\, \forall \pi' \,.\, \overline{\pi} = \pi\ell\pi' \Rightarrow \varrho(\pi\ell) \in \mathcal{I}(\ell) & \text{(def. } \subseteq\text{)} \\
\Leftrightarrow & \forall \overline{\pi} \in \Pi \,.\, \forall \pi' \,.\, \forall \ell \,.\, \overline{\pi} = \pi\ell\pi' \Rightarrow \varrho(\pi\ell) \in \mathcal{I}(\ell) & \text{(def. } \forall\text{)} \\
\Leftrightarrow & \Pi \subseteq \{\overline{\pi} \mid \forall \pi' \,.\, \forall \ell \,.\, \overline{\pi} = \pi\ell\pi' \Rightarrow \varrho(\pi\ell) \in \mathcal{I}(\ell)\} & \text{(def. } \subseteq\text{)} \\
\Leftrightarrow & \Pi \subseteq \gamma^{\mathbb{I}}(\mathcal{I}) &
\end{array}
$$

by defining $\gamma^{\mathbb{I}}(\mathcal{I}) \triangleq \{\overline{\pi} \mid \forall \pi' \,.\, \forall \ell \,.\, \overline{\pi} = \pi\ell\pi' \Rightarrow \varrho(\pi\ell) \in \mathcal{I}(\ell)\}$.

Hierarchy of program properties

Hierarchy of program properties/semantics

$$
\begin{tikzcd}
\mathbb{L} \to \wp(\mathbb{E}\mathbb{v}) \arrow[d, bend right, "\gamma^{\mathbb{I}}"'] \arrow[dd, bend right=60, "\gamma^{\mathbb{T}} \circ \gamma^{\mathbb{I}}"'] \\
\wp(\mathbb{T}^{+\infty}) \arrow[u, bend right, "\alpha^{\mathbb{I}}"'] \arrow[d, bend right, "\gamma^{\mathbb{T}}"'] \\
\wp(\wp(\mathbb{T}^{+\infty})) \arrow[u, bend right, "\alpha^{\mathbb{T}}"'] \arrow[uu, bend right=60, "\alpha^{\mathbb{I}} \circ \alpha^{\mathbb{T}}"']
\end{tikzcd}
$$

$$
\begin{aligned}
\mathcal{S}^{\mathbb{I}}[\![\mathsf{P}]\!] &= \alpha^{\mathbb{I}}(\mathcal{S}^{\mathbb{T}}[\![\mathsf{P}]\!]) \\
&= \alpha^{\mathbb{I}} \circ \alpha^{\mathbb{T}}(\mathcal{S}^{\mathbb{C}}[\![\mathsf{P}]\!])
\end{aligned}
$$

invariance/ reachability semantics

$$
\begin{aligned}
\mathcal{S}^{\mathbb{T}}[\![\mathsf{P}]\!] &= \mathcal{S}^{+\infty}[\![\mathsf{P}]\!] \\
&= \alpha^{\mathbb{T}}(\mathcal{S}^{\mathbb{C}}[\![\mathsf{P}]\!])
\end{aligned}
$$

trace semantics

$\mathcal{S}^{\mathbb{C}}[\![\mathsf{P}]\!] \triangleq \{\mathcal{S}^{+\infty}[\![\mathsf{P}]\!]\}$, collecting semantics

Home work

- Read Ch. **8** "Program properties" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you