Principles of Abstract Interpretation
MIT press
Ch. **12**, Relational and Transformer Semantics

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

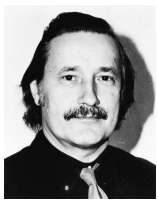
These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-12--relational-transformer-semantics-PrAbsInt.pdf

Chapter 12

Ch. **12**, Relational and Transformer Semantics

In this Chapter **12**, we study two ways of abstracting trace semantics:

- By a relation (as in denotational, relational, or natural semantics)
- By a property transformer (as in predicate transformer semantics)


Christopher Strachey


Dana Scott


Robin Milner


Mads Tofte


Gilles Kahn


Edsger Dijkstra

en.wikipedia.org/wiki/Denotational_semantics
en.wikipedia.org/wiki/Predicate_transformer_semantics

Relational Semantics

Infinitary relational semantics $\mathcal{S}^{\mathrm{R}}[\![\mathtt{S}]\!]$ of a statement S

- Abstraction of the maximal trace semantics $\mathcal{S}^{+\infty}[\![\mathtt{S}]\!]$ of Chapter **7**

$$\mathcal{S}^{\mathrm{R}}[\![\mathtt{S}]\!] \quad \triangleq \quad \alpha_{\mathrm{R}}(\mathcal{S}^{+\infty}[\![\mathtt{S}]\!]).$$

- homomorphic/partitioning abstraction $\langle \wp(\mathbb{T}^+ \to \mathbb{T}^{+\infty}), \subseteq \rangle \underset{\alpha_{\mathrm{R}}}{\overset{\gamma_{\mathrm{R}}}{\leftrightarrows}} \langle \wp(\mathbb{E}\mathtt{v} \times (\mathbb{E}\mathtt{v} \cup \{\bot\}), \subseteq \rangle$

$$\begin{array}{rcll} \alpha_{\mathrm{R}}\langle \pi_1, \pi_2 \rangle & \triangleq & \langle \varrho(\pi_1), \varrho(\pi_1 \frown \pi_2) \rangle & \pi_2 \in \mathbb{T}^+ \\ & \triangleq & \langle \varrho(\pi_1), \bot \rangle & \pi_2 \in \mathbb{T}^\infty \\ \alpha_{\mathrm{R}}(\mathcal{S}) & \triangleq & \{\alpha_{\mathrm{R}}\langle \pi_1, \pi_2 \rangle \mid \pi_1 \in \mathbb{T}^+ \wedge \pi_2 \in \mathcal{S}(\pi_1)\} & \end{array} \qquad (12.1)$$

- Example (factorial program P): $\mathcal{S}^{\mathrm{R}}[\![\mathtt{P}]\!] \triangleq \{\langle x, !x \rangle \mid x \geqslant 0\} \cup \{\langle x, \bot \rangle \mid x < 0\}$
- Useful to discuss program *total correctness* (takes non-termination into account)

  en.wikipedia.org/wiki/Correctness_(computer_science)

Denotational Semantics

Denotational Semantics $\mathcal{S}^\partial[\![\mathtt{S}]\!]$

- The denotational semantics $\mathcal{S}^\partial[\![\mathtt{S}]\!] \in \mathbb{E}\mathtt{v} \to \wp(\mathbb{E}\mathtt{v} \cup \{\bot\})$ is the right-image of the relational semantics

$$\mathcal{S}^\partial[\![\mathtt{P}]\!] \quad \triangleq \quad \rho \mapsto \{\rho' \mid \langle \rho, \rho' \rangle \in \mathcal{S}^R[\![\mathtt{P}]\!]\}$$

- $\mathcal{S}^\partial[\![\mathtt{S}]\!] \in \mathbb{E}\mathtt{v} \to \mathbb{E}\mathtt{v} \cup \{\bot\}$ for deterministic programs
- Example (factorial program P): $\mathcal{S}^\partial[\![\mathtt{P}]\!] \triangleq x \mapsto (\!| x \geqslant 0 \,?\, !x \,:\, \bot |\!)$

Natural Semantics

Finitary relational semantics (also called *natural semantics*) $\mathcal{S}^{\mathrm{R}^+}[\![\mathtt{S}]\!]$ of a statement S

$$\mathcal{S}^{\mathrm{R}^+}[\![\mathtt{S}]\!] \triangleq \{\langle \varrho(\pi_1), \varrho(\pi_1 \frown \pi_2)\rangle \mid \pi_1 \in \mathbb{T}^+ \wedge \pi_2 \in \mathcal{S}^+[\![\mathtt{S}]\!](\pi_1)\}.$$

- Example (factorial program P): $\mathcal{S}^{\mathrm{R}^+}[\![\mathtt{P}]\!] \triangleq \{\langle x, !x\rangle \mid x \geqslant 0\}$
- Useful to discuss program *partial correctness* (does not take non-termination into account)

en.wikipedia.org/wiki/Correctness_(computer_science)

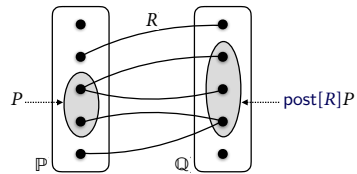
Transformer Semantics

Property transformers

- Isomorphic abstractions of relations (*e.g.*(in)finitary relational semantics)
- the *post-image* of a preproperty/precondition $P \in \wp(\mathbb{P})$ by relation $R \in \wp(\mathbb{P} \times \mathbb{Q})$ is $\mathrm{post}[R]P \in \wp(\mathbb{Q})$ such that

$$\mathrm{post}[R] \quad \triangleq \quad P \mapsto \{y \in \mathbb{Q} \mid \exists x \in P \,.\, \langle x,\ y\rangle \in R\} \tag{12.2}$$

(This is also called the *right-image* of P by R, also written $R[P]$ or even $R(P)$.)



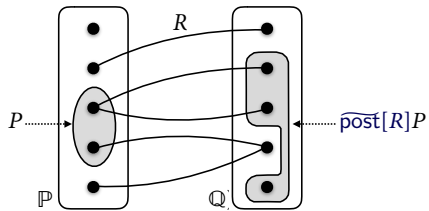
- $\langle \wp(\mathbb{P} \times \mathbb{Q}),\ \subseteq\rangle \underset{\mathrm{post}}{\overset{\mathrm{post}^{-1}}{\leftrightarrows}} \langle \wp(\mathbb{P}) \xrightarrow{\sqcup} \wp(\mathbb{Q}),\ \dot{\subseteq}\rangle$

where $\mathrm{post}^{-1}[T] \triangleq \{\langle x,\ y\rangle \in \mathbb{P} \times \mathbb{Q} \mid y \in T(\{x\})\}$

Property transformers

- The *dual post-image* of a preproperty $P \in \wp(\mathbb{P})$ by relation R is $\widetilde{\mathsf{post}}[R]P \in \wp(\mathbb{Q})$ such that

$$\begin{aligned} \widetilde{\mathsf{post}}[R] &\triangleq \neg \circ \mathsf{post}[R] \circ \neg \ ^{1} \\ &= P \mapsto \{y \in \mathbb{Q} \mid \forall x \in \mathbb{P} \,.\, \langle x,\ y\rangle \in R \Rightarrow x \in P\} \end{aligned} \tag{12.3}$$



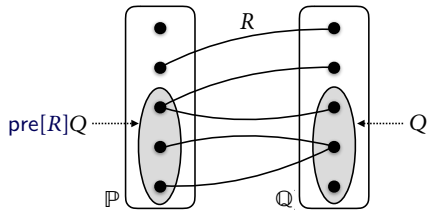
[1] We write $\neg P$ for $\mathbb{P} \setminus P$ and $\neg Q$ for $\mathbb{Q} \setminus Q$, the ambiguity being solved by considering the powerset to which the negated property belongs.

Property transformers

- The *pre-image* of a postproperty $Q \in \wp(\mathbb{Q})$ by relation $R \in \wp(\mathbb{P} \times \mathbb{Q})$ is $\mathrm{pre}[R]Q \in \wp(\mathbb{P})$ such that

$$\mathrm{pre}[R] \triangleq \mathrm{post}[R^{-1}] = Q \mapsto \{x \in \mathbb{P} \mid \exists y \in Q \,.\, \langle x,\, y\rangle \in R\} \tag{12.11}$$

(This is also called the *left-image* of P by R, also written $R^{-1}[P]$ or $R^{-1}(P)$.)



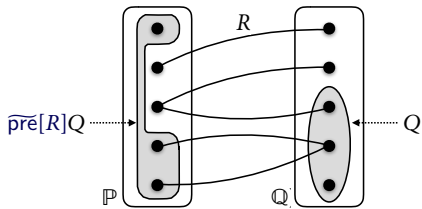
- $\langle \wp(\mathbb{P} \times \mathbb{Q}),\, \subseteq\rangle \underset{\mathrm{pre}}{\overset{\mathrm{pre}^{-1}}{\leftrightarrows}} \langle \wp(\mathbb{Q}) \xrightarrow{\sqcap} \wp(\mathbb{P}),\, \dot{\subseteq}\rangle$

where $\mathrm{pre}^{-1}[T] = \{\langle x,\, y\rangle \in \mathbb{P} \times \mathbb{Q} \mid x \in T(\{y\})\}$

Property transformers

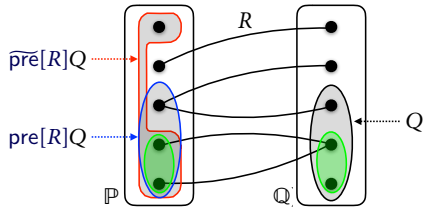
- The *dual pre-image* of a postproperty $Q \in \wp(\mathbb{Q})$ by relation $R \in \wp(\mathbb{P} \times \mathbb{Q})$ is is $\widetilde{\mathrm{pre}}[r]Q \in \wp(\mathbb{P})$ such that

$$\begin{aligned} \widetilde{\mathrm{pre}}[R] &\triangleq \neg \circ \mathrm{pre}[R] \circ \neg = \widetilde{\mathrm{post}}[R^{-1}] \\ &= Q \mapsto \{x \in \mathbb{P} \mid \forall y \in \mathbb{Q} \,.\, \langle x, y \rangle \in R \Rightarrow y \in Q\} \end{aligned} \tag{12.12}$$



Weakest precondition

- $\mathsf{pre}[R]Q \wedge \widetilde{\mathsf{pre}}[R]Q$



- If $P \subseteq \mathsf{pre}[R]Q \wedge \widetilde{\mathsf{pre}}[R]Q$ then it is guaranteed to reach Q from P through R

Galois connections between property transformers

If $R \in \wp(\mathbb{P} \times \mathbb{Q})$, we have the following Galois connections

$$\langle \wp(\mathbb{P}), \subseteq \rangle \underset{\mathsf{post}[R]}{\overset{\widetilde{\mathsf{pre}}[R]}{\leftrightarrows}} \langle \wp(\mathbb{Q}), \subseteq \rangle \tag{12.22}$$

$$\langle \wp(\mathbb{Q}), \subseteq \rangle \underset{\mathsf{pre}[R]}{\overset{\widetilde{\mathsf{post}}[R]}{\leftrightarrows}} \langle \wp(\mathbb{P}), \subseteq \rangle \tag{12.23}$$

Conclusion

Conclusion

- We rarely reason directly on the trace semantics of programs (too complicated)
- We reason on abstractions of the semantics of programs (much simpler)
- Important to understand this abstraction process
- Formalized by Galois connections between concrete and abstract properties (found everywhere)

The End, Thank you