Compositional Property-oriented Semantics for Structured Specifications.

Another Old Story (with a Few New Twists)

Andrzej Tarlecki

Institute of Informatics, University of Warsaw

and

Institute of Computer Science, Polish Academy of Sciences

Warsaw, Poland

Thanks to: Don Sannella, and others. . .

Working within an arbitrary institution

$$\mathbf{I} = \langle \mathbf{Sign}, \mathbf{Sen}, \mathbf{Mod}, \langle \models_\Sigma \rangle_{\Sigma \in |\mathbf{Sign}|} \rangle$$

That is:

- a category $\mathbf{Sign}$ of *signatures*
- a functor $\mathbf{Sen} \colon \mathbf{Sign} \to \mathbf{Set}$
  ($\mathbf{Sen}(\Sigma)$ is the set of Σ-*sentences*, for $\Sigma \in |\mathbf{Sign}|$)
- a functor $\mathbf{Mod} \colon \mathbf{Sign}^{op} \to \mathbf{Cat}$
  ($\mathbf{Mod}(\Sigma)$ is the category of Σ-*models*, for $\Sigma \in |\mathbf{Sign}|$)
- for each $\Sigma \in |\mathbf{Sign}|$,
  Σ-*satisfaction relation* $\models_\Sigma \subseteq |\mathbf{Mod}(\Sigma)| \times \mathbf{Sen}(\Sigma)$

subject to the *satisfaction condition*:

$$M'|_\sigma \models_\Sigma \varphi \iff M' \models_{\Sigma'} \sigma(\varphi)$$

where $\sigma \colon \Sigma \to \Sigma'$ in $\mathbf{Sign}$, $M' \in |\mathbf{Mod}(\Sigma')|$, $\varphi \in \mathbf{Sen}(\Sigma)$, $M'|_\sigma$ stands for $\mathbf{Mod}(\sigma)(M')$, and $\sigma(\varphi)$ for $\mathbf{Sen}(\sigma)(\varphi)$.

With further notation/concepts, like:

- model class of a set of sentences:
  $Mod_\Sigma[\Phi]$
- theory of a model class:
  $Th_\Sigma[\mathcal{M}]$
- closure of a set of sentences:
  $Cl_\Sigma(\Phi) = Th_\Sigma[Mod_\Sigma[\Phi]]$
- semantic consequence $\Phi \models \varphi$:
  $\varphi \in Cl_\Sigma(\Phi)$

Specifications

$$\boxed{SP \in \mathit{Spec}}$$

Adopting the model-theoretic view of specifications

The meaning of any specification $SP \in \mathit{Spec}$ built over $\mathbf{I}$ is given by:

- its *signature* $\mathit{Sig}[SP] \in |\mathbf{Sign}|$, and
- a class of its *models* $\mathit{Mod}[SP] \subseteq |\mathbf{Mod}(\mathit{Sig}[SP])|$.

This yields the usual notions:

- semantic equivalence: $SP_1 \equiv SP_2$,
- semantic consequence: $SP \models \varphi$,
- theory of a specification: $\mathit{Th}[SP] = \{\varphi \mid SP \models \varphi\}$, etc

Standard structured specifications

Flat specification: $\langle \Sigma, \Phi \rangle$ — for $\Sigma \in |\mathbf{Sign}|$ and $\Phi \subseteq \mathbf{Sen}(\Sigma)$:

captures basic properties

$Sig[\langle \Sigma, \Phi \rangle] = \Sigma$

$Mod[\langle \Sigma, \Phi \rangle] = Mod[\Phi]$

Union: $SP_1 \cup SP_2$ — for SP_1 and SP_2 with $Sig[SP_1] = Sig[SP_2]$:

combines the constraints imposed

$Sig[SP_1 \cup SP_2] = Sig[SP_1]$

$Mod[SP_1 \cup SP_2] = Mod[SP_1] \cap Mod[SP_2]$

Translation: $\sigma(SP)$ — for any SP and $\sigma\colon Sig[SP] \to \Sigma'$:

renames and introduces new components

$Sig[\sigma(SP)] = \Sigma'$

$Mod[\sigma(SP)] = \{M' \in |\mathbf{Mod}(\Sigma')| \mid M'|_\sigma \in Mod[SP]\}$

Hiding: $SP'|_\sigma$ — for any SP' and $\sigma\colon \Sigma \to Sig[SP']$:

hides auxiliary components

$Sig[SP'|_\sigma] = \Sigma$

$Mod[SP'|_\sigma] = \{M'|_\sigma \mid M' \in Mod[SP']\}$

Proving semantic consequence

The standard compositional proof system

$$\frac{\varphi \in \Phi}{\langle \Sigma, \Phi \rangle \vdash \varphi} \qquad \frac{SP_1 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi} \qquad \frac{SP_2 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi}$$

$$\frac{SP \vdash \varphi}{\sigma(SP) \vdash \sigma(\varphi)} \qquad \frac{SP' \vdash \sigma(\varphi)}{SP'|_\sigma \vdash \varphi}$$

Plus a *structural rule*:

$$\frac{\text{for } i \in J, SP \vdash \varphi_i \qquad \{\varphi_i\}_{i \in J} \models \varphi}{SP \vdash \varphi}$$

Soundness & completeness

$$SP \vdash \varphi \implies SP \models \varphi$$

Fact: *If the category of signatures has pushouts, the institution admits amalgamation and interpolation (and has implication and . . .) then*

$$SP \vdash \varphi \iff SP \models \varphi$$

In general: there is *no* sound and complete *compositional* proof system for semantic consequence for structured specifications because:

Claim: *The best sound and compositional proof system one can have is given above.*

Really ?

Property-oriented semantics

$$\mathcal{T}\colon Spec \to SenSets$$

such that for $SP \in Spec$, if $Sig[SP] = \Sigma$ then $\mathcal{T}(SP) \subseteq \mathbf{Sen}(\Sigma)$.

Functoriality not assumed!

Example: $Th\colon Spec \to SenSets$ *given by* $Th(SP) = Th[SP]$.

Would be perfect in principle, but is not compositional

The standard compositional property-oriented semantics

$$\mathcal{T}_0 \colon \mathit{Spec} \to \mathit{SenSets}$$

The standard property-oriented semantics that assigns a Σ-theory $\mathcal{T}_0(SP)$ to any well-formed structured Σ-specification SP built from flat specifications using union, translation and hiding is given by:

$$\mathcal{T}_0(\langle\Sigma, \Phi\rangle) = Cl_\Sigma(\Phi)$$

$$\mathcal{T}_0(SP \cup SP') = Cl_{Sig[SP]}(\mathcal{T}_0(SP) \cup \mathcal{T}_0(SP'))$$

$$\mathcal{T}_0(\sigma(SP)) = Cl_\Sigma(\sigma(\mathcal{T}_0(SP)))$$

$$\mathcal{T}_0(SP|_\sigma) = \sigma^{-1}(\mathcal{T}_0(SP))$$

Getting there...

The standard compositional property-oriented semantics is determined by the compositional proof system as given above:

$$\varphi \in \mathcal{T}_0(SP) \quad \text{iff} \quad SP \vdash \varphi$$

for $\varphi \in \mathbf{Sen}(Sig[SP])$.

Claim: $\mathcal{T}_0$ *is the best sound and compositional property-oriented semantics for all specifications built from flat specifications using union, translation and hiding.*

Really ?

Specification-building operations

We work with specifications built by *specification-building operations*:

$$\frac{\mathbf{sbo}\colon \mathit{Spec}(\Sigma_1) \times \cdots \times \mathit{Spec}(\Sigma_n) \to \mathit{Spec}(\Sigma)}{[\![\mathbf{sbo}]\!]\colon 2^{|\mathbf{Mod}(\Sigma_1)|} \times \cdots \times 2^{|\mathbf{Mod}(\Sigma_n)|} \to 2^{|\mathbf{Mod}(\Sigma)|}}$$

where $\mathit{Spec}(\Sigma) = \{SP \in \mathit{Spec} \mid \mathit{Sig}[SP] = \Sigma\}$.

Specifications in Spec are built using a family of **sbo***'s*

For instance:

- $\_ \cup \_ \colon \mathit{Spec}(\Sigma) \times \mathit{Spec}(\Sigma) \to \mathit{Spec}(\Sigma)$, for each $\Sigma \in |\mathbf{Sign}|$
- $\sigma(\_)\colon \mathit{Spec}(\Sigma) \to \mathit{Spec}(\Sigma')$, for each $\sigma\colon \Sigma \to \Sigma'$
- $\_|_\sigma \colon \mathit{Spec}(\Sigma') \to \mathit{Spec}(\Sigma)$, for each $\sigma\colon \Sigma \to \Sigma'$
- $\langle \Sigma, \Phi \rangle\colon \ \to \mathit{Spec}(\Sigma)$, for each $\Sigma \in |\mathbf{Sign}|$, $\Phi \subseteq \mathbf{Sen}(\Sigma)$

the model-class semantics is compositional,
sbo*'s as functions on model classes are monotone*

About property-oriented semantics

$$\mathcal{T} : Spec \to SenSets$$

- $\mathcal{T}$ is *theory-oriented* if $\mathcal{T}(SP) = Cl_{Sig[SP]}(\mathcal{T}(SP))$.
- $\mathcal{T}$ is *compositional* if $\mathcal{T}(\mathbf{sbo}(SP)) = \mathcal{T}(\mathbf{sbo}(SP'))$ when $\mathcal{T}(SP) = \mathcal{T}(SP')$.
- $\mathcal{T}$ is *monotone* if $\mathcal{T}(\mathbf{sbo}(SP)) \subseteq \mathcal{T}(\mathbf{sbo}(SP'))$ when $\mathcal{T}(SP) \subseteq \mathcal{T}(SP')$.
- $\mathcal{T}$ is *sound* if $\mathcal{T}(SP) \subseteq Th[SP]$.
- (sound) $\mathcal{T}$ is *complete* if $\mathcal{T}(SP) = Th[SP]$.
- (sound) $\mathcal{T}$ is ~~*one step*~~ *closed complete* (for **sbo**) if $\mathcal{T}(\mathbf{sbo}(SP)) = Th[\mathbf{sbo}(SP)]$ when $Mod_{Sig[SP]}[\mathcal{T}(SP)] = Mod[SP]$; or a bit stronger:
  - $\mathcal{T}(\mathbf{sbo}(SP)) = Th[[\![\mathbf{sbo}]\!](Mod_{Sig[SP]}[\mathcal{T}(SP)])]$.
- $\mathcal{T}$ is *non-absent-minded* if $\Phi \subseteq \mathcal{T}(\langle \Sigma, \Phi \rangle)$.
- $\mathcal{T}$ is *flat complete* if $\mathcal{T}(\langle \Sigma, \Phi \rangle) = Cl_{\Sigma}(\Phi)$.

omitting generalisation to multi-argument **sbo**'s

Some trivia

- Monotone $\mathcal{T}$ is compositional, but not vice versa.
  - Compositionality admits rules with negative premises?
- Closed complete (stronger version) $\mathcal{T}$ is compositional and theory-oriented
- Sound theory-oriented $\mathcal{T}$ is flat complete iff it is non-absent-minded.
- Closed completeness for flat specifications, viewed as nullary specification-building operations, is the same as flat completeness.

Fact: *The standard property-oriented semantics is really good:*

$\mathcal{T}_0$ is theory-oriented, monotone, sound, closed complete, etc.

Closed completeness does not imply completeness

Key theorem

Fact: *Let $\mathcal{T}_s$ and $\mathcal{T}$ be property-oriented semantics for specifications in $Spec$, including all flat specifications. Let*

- *$\mathcal{T}_s$ be sound, monotone and closed complete, and*
- *$\mathcal{T}$ be sound, compositional, non-absent-minded and theory-oriented.*

Then $\mathcal{T}_s$ is at least as strong as $\mathcal{T}$: for every $SP \in Spec$,

$$\mathcal{T}(SP) \subseteq \mathcal{T}_s(SP)$$

Consequently:

$\mathcal{T}_0$ is stronger than any other sound, compositional, non-absent-minded and theory-oriented semantics for structured specifications built from flat specifications using union, translation and hiding.

Instead of conclusions

Exercise: *Check if the assumptions that $\mathcal{T}$ is non-absent-minded and that $\mathcal{T}$ is theory-oriented in the key theorem and its corollary are necessary.*

(We didn't know!)

Proof of the key theorem, by induction on the structure of SP:

$$\begin{aligned}
&\mathcal{T}(\mathbf{sbo}(SP)) \\
&\quad = \mathcal{T}(\mathbf{sbo}(\underline{\langle \Sigma, \mathcal{T}(SP)\rangle})) \\
&\quad \subseteq Th[\mathbf{sbo}(\langle \Sigma, \mathcal{T}(SP)\rangle)] \\
&\quad = \mathcal{T}_s(\mathbf{sbo}(\langle \Sigma, \mathcal{T}(SP)\rangle)) \\
&\quad \subseteq \mathcal{T}_s(\mathbf{sbo}(\langle \Sigma, \mathcal{T}_s(SP)\rangle)) \\
&\quad = \mathcal{T}_s(\mathbf{sbo}(SP))
\end{aligned}$$

For any SP we seem to need a specification $\mathrm{BS}_{\mathcal{T}(\mathrm{SP})}$ such that $\mathcal{T}(\mathrm{BS}_{\mathcal{T}(\mathrm{SP})}) = \mathcal{T}_s(\mathrm{BS}_{\mathcal{T}(\mathrm{SP})}) = \mathcal{T}(\mathrm{SP})$ and $\mathrm{Mod}[\mathrm{BS}_{\mathcal{T}(\mathrm{SP})}] = \mathrm{Mod}_{\,Sig[\mathrm{SP}]}[\mathcal{T}(\mathrm{SP})]$.

Indeed — see below!

$\mathcal{T}$ better be non-absent-minded: sketch of a counterexample

Consider signatures Σ, Σ' with $\sigma\colon \Sigma \to \Sigma'$. Let $\mathbf{Sen}(\Sigma) = \{\alpha\}$, $\mathbf{Sen}(\Sigma') = \{\alpha, \beta\}$, with σ-translation preserving α, and let $\mathbf{Mod}(\Sigma) = \mathbf{Mod}(\Sigma') = \{M_1, M_2, M_3\}$, with the identity σ-reduct. Put $M_1 \models \alpha$, $M_2 \not\models \alpha$, $M_3 \models \alpha$, $M_1 \models \beta$, $M_2 \not\models \beta$, $M_3 \not\models \beta$. Take $B^AD = \langle \Sigma', \{\beta\} \rangle|_\sigma$; then $Mod[B^AD] = \{M_1\}$.

Let then $\mathcal{T}$ drop the axiom α in all flat specifications and $\mathcal{T}(B^AD) = \{\alpha\}$ and $\mathcal{T}(\sigma(B^AD)) = \{\alpha, \beta\}$. $\mathcal{T}$ may be given by:

$$\frac{SP' \vdash \beta}{SP' \vdash \alpha} \qquad \frac{\beta \in \Phi'}{\langle \Sigma', \Phi' \rangle \vdash \beta} \qquad \frac{SP' \vdash \alpha}{SP'|_\sigma \vdash \alpha} \qquad \frac{SP \vdash \alpha}{\sigma(SP) \vdash \beta}$$

Then $\mathcal{T}$ is sound, compositional and theory-oriented, but for $\sigma(B^AD)$ it is stronger than $\mathcal{T}_0$, which yields $\mathcal{T}_0(B^AD) = \{\alpha\}$ and $\mathcal{T}_0(\sigma(B^AD)) = \{\alpha\}$.

Ughhh!

$\mathcal{T}$ better be theory-oriented: sketch of a counterexample

Consider signatures Σ, Σ' with $\sigma\colon \Sigma \to \Sigma'$. Let $\mathbf{Sen}(\Sigma) = \{\alpha', \alpha\}$, $\mathbf{Sen}(\Sigma') = \{\alpha', \alpha, \beta\}$, with σ-translation preserving α amd α', and let $\mathbf{Mod}(\Sigma) = \mathbf{Mod}(\Sigma') = \{M_1, M_2, M_3, M_4\}$, with the identity σ-reduct. Put $M_1 \models \alpha$, $M_2 \not\models \alpha$, $M_3 \models \alpha$, $M_4 \not\models \alpha$, $M_1 \models \beta$, $M_2 \not\models \beta$, $M_3 \not\models \beta$, $M_4 \not\models \beta$, $M_1 \models \alpha'$, $M_2 \not\models \alpha'$, $M_3 \models \alpha'$, $M_4 \models \alpha'$. Take $B^AD = \langle \Sigma', \{\beta\}\rangle|_{\sigma}$.

Let then $\mathcal{T}$ omit the consequence α' of the axiom β in all flat specifications and $\mathcal{T}(B^AD) = \{\alpha\}$ and $\beta \in \mathcal{T}(\sigma(B^AD))$. $\mathcal{T}$ may be given by:

$$\frac{SP' \vdash \beta}{SP' \vdash \alpha} \qquad \frac{SP' \not\vdash \beta \quad SP' \vdash \alpha}{SP' \vdash \alpha'} \qquad \frac{\alpha \in \Phi}{\langle \Sigma, \Phi\rangle \vdash \alpha'} \qquad \cdots \qquad \frac{SP \vdash \alpha \quad SP \not\vdash \alpha'}{\sigma(SP) \vdash \beta}$$

Then $\mathcal{T}$ is sound, compositional and non-absent-minded, but for $\sigma(B^AD)$ it is stronger than $\mathcal{T}_0$.

Ughhh!

Key theorem'

Fact: *Let $\mathcal{T}_s$ and $\mathcal{T}$ be property-oriented semantics for specifications in $Spec$, including all flat specifications. Let*

- *$\mathcal{T}_s$ be sound, monotone and closed complete, and*
- *$\mathcal{T}$ be sound, monotone, and non-absent-minded (need not be theory-oriented).*

Then $\mathcal{T}_s$ is at least as strong as $\mathcal{T}$: for every $SP \in Spec$,

$$\mathcal{T}(SP) \subseteq \mathcal{T}_s(SP)$$

Consequently:

$\mathcal{T}_0$ is stronger than any other sound, monotone, and non-absent-minded semantics for structured specifications built from flat specifications using union, translation and hiding.

Entailment systems

Entailment system for $\mathbf{Sen}\colon \mathbf{Sign} \to \mathbf{Set}$:

$$\mathcal{E} = \langle \vdash_\Sigma \subseteq 2^{\mathbf{Sen}(\Sigma)} \times \mathbf{Sen}(\Sigma) \rangle_{\Sigma \in |\mathbf{Sign}|}$$

reflexivity: $\{\varphi\} \vdash_\Sigma \varphi$
weakening: if $\Phi \vdash_\Sigma \varphi$ then $\Phi \cup \Psi \vdash_\Sigma \varphi$
transitivity: if $\Phi \vdash_\Sigma \psi$ and $\Psi_\varphi \vdash_\Sigma \varphi$ for each $\varphi \in \Phi$ then $\bigcup_{\varphi \in \Phi} \Psi_\varphi \vdash_\Sigma \psi$
translation: if $\Phi \vdash_\Sigma \varphi$ then $\sigma(\Phi) \vdash_{\Sigma'} \sigma(\varphi)$ for $\sigma\colon \Sigma \to \Sigma'$

- $\mathcal{E}$ is *sound* for an institution $\mathbf{I} = \langle \mathbf{Sign}, \mathbf{Sen}, \mathbf{Mod}, \langle \models_\Sigma \rangle_{\Sigma \in |\mathbf{Sign}|} \rangle$

$$\Phi \models \varphi \textit{ whenever } \Phi \vdash_\Sigma \varphi$$

- $\mathcal{E}$ is *complete* for an institution $\mathbf{I} = \langle \mathbf{Sign}, \mathbf{Sen}, \mathbf{Mod}, \langle \models_\Sigma \rangle_{\Sigma \in |\mathbf{Sign}|} \rangle$

$$\Phi \vdash_\Sigma \varphi \textit{ whenever } \Phi \models \varphi$$

Fix an entailment system $\mathcal{E} = \langle \vdash_\Sigma \rangle_{\Sigma \in |\mathbf{Sign}|}$ for $\mathbf{Sen}\colon \mathbf{Sign} \to \mathbf{Set}$

Property-oriented semantics

$$\mathcal{T}\colon \mathit{Spec} \to \mathit{SenSets}$$

such that for $SP \in \mathit{Spec}$, if $\mathit{Sig}[SP] = \Sigma$ then $\mathcal{T}(SP) \subseteq \mathbf{Sen}(\Sigma)$.

$\mathcal{T}$ is $\mathcal{E}$-*theory oriented*, *compositional*, *monotone*, *non-absent-minded* — as before.

$\mathcal{T}$ is $\mathcal{E}$-*sound* if $\mathcal{T}(SP) = \mathit{Th}[SP]$ *in every institution for which* $\mathcal{E}$ *is sound*.

$\mathcal{T}$ is $\mathcal{E}$-*complete* if it is complete *in every institution for which* $\mathcal{E}$ *is sound and complete*.

The standard compositional property-oriented semantics

$$\mathcal{T}_{\mathcal{E}} \colon \mathit{Spec} \to \mathit{SenSets}$$

The standard property-oriented semantics in the framework of $\mathcal{E}$ assigns an $\mathcal{E}$-Σ-theory $\mathcal{T}_{\mathcal{E}}(SP)$ to any well-formed structured Σ-specification SP built from flat specifications using union, translation and hiding:

$$\mathcal{T}_{\mathcal{E}}(\langle \Sigma, \Phi \rangle) = Cl^{\mathcal{E}}_{\Sigma}(\Phi)$$
$$\mathcal{T}_{\mathcal{E}}(SP \cup SP') = Cl^{\mathcal{E}}_{Sig[SP]}(\mathcal{T}_{\mathcal{E}}(SP) \cup \mathcal{T}_{\mathcal{E}}(SP'))$$
$$\mathcal{T}_{\mathcal{E}}(\sigma(SP)) = Cl^{\mathcal{E}}_{\Sigma}(\sigma(\mathcal{T}_{\mathcal{E}}(SP)))$$
$$\mathcal{T}_{\mathcal{E}}(SP|_{\sigma}) = \sigma^{-1}(\mathcal{T}_{\mathcal{E}}(SP))$$

Fact: *The standard property-oriented semantics is quite good:*

$\mathcal{T}_{\mathcal{E}}$ *is $\mathcal{E}$-theory-oriented, monotone, $\mathcal{E}$-sound, etc.*

Proving semantic consequence

The standard compositional proof system

$$\frac{\varphi \in \Phi}{\langle \Sigma, \Phi \rangle \vdash \varphi} \qquad \frac{SP_1 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi} \qquad \frac{SP_2 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi}$$

$$\frac{SP \vdash \varphi}{\sigma(SP) \vdash \sigma(\varphi)} \qquad \frac{SP' \vdash \sigma(\varphi)}{SP'|_\sigma \vdash \varphi}$$

Plus a *structural rule*:

$$\frac{\text{for } i \in J, SP \vdash \varphi_i \qquad \{\varphi_i\}_{i \in J} \vdash_{Sig[SP]} \varphi}{SP \vdash \varphi}$$

Key theorems

$\mathcal{T}_{\mathcal{E}}$ is stronger than any other $\mathcal{E}$-sound, compositional, non-absent-minded and $\mathcal{E}$-theory-oriented semantics for structured specifications built from flat specifications using union, translation and hiding.

$\mathcal{T}_0$ is stronger than any other $\mathcal{E}$-sound, monotone, and non-absent-minded semantics for structured specifications built from flat specifications using union, translation and hiding.

Conclusion

The standard compositional property-oriented semantics is imperfect.

But it is the best one can give.

And we made this precise.