Another Old Story:
Compositional Property-oriented Semantics for Structured Specifications

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

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

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*:

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

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

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

Adopting the model-theoretic view of specifications

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

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

This yields the usual notions:

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

Standard structured specifications

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

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

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

captures basic properties

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

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

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

combines the constraints imposed

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

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

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

renames and introduces new components

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

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

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

hides auxiliary components

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

$$\boxed{SP \vdash \varphi \implies SP \models \varphi}$$

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

$$\boxed{SP \vdash \varphi \iff SP \models \varphi}$$

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

$$\boxed{\mathcal{T} : Spec \to Theories}$$

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

Functoriality not required!

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

Would be perfect, but is not compositional

The standard compositional property-oriented semantics

$$\boxed{\mathcal{T}_0 \colon \mathit{Spec} \to \mathit{Theories}}$$

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:

$$\boxed{\begin{aligned}
&\mathcal{T}_0(\langle \Sigma, \Phi \rangle) = Cl_\Sigma(\Phi)\\
&\mathcal{T}_0(SP \cup SP') = Cl_{Sig[SP]}(\mathcal{T}_0(SP) \cup \mathcal{T}_0(SP'))\\
&\mathcal{T}_0(\sigma(SP)) = Cl_\Sigma(\sigma(\mathcal{T}_0(SP)))\\
&\mathcal{T}_0(SP|_\sigma) = \sigma^{-1}(\mathcal{T}_0(SP))
\end{aligned}}$$

Getting there...

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

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

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*:

$$\mathbf{sbo}\colon \mathit{Spec}(\Sigma_1) \times \cdots \times \mathit{Spec}(\Sigma_n) \to \mathit{Spec}(\Sigma)$$

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

$$\mathcal{T} : Spec \rightarrow Theories$$

- $\mathcal{T}$ 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 complete* (for **sbo**) if $\mathcal{T}(\mathbf{sbo}(SP)) = Th[\mathbf{sbo}(SP)]$ when $Mod_{Sig[SP]}[\mathcal{T}(SP)] = Mod[SP]$.
- $\mathcal{T}$ is *non-absentminded* 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

- Monotonicity implies compositionality, but not vice versa.
  - Compositionality admits rules with negative premises?
- Flat completeness and non-absentmindedness are equivalent for sound $\mathcal{T}$.
- One-step completeness for flat specifications, viewed as nullary specification-building operations, is the same as flat completeness.

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

$\mathcal{T}_0$ *is monotone, sound, one-step complete, etc.*

One-step 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 one-step complete, and $\mathcal{T}$ be sound, compositional and non-absentminded. Then $\mathcal{T}_s$ is at least as strong as $\mathcal{T}$: for every $SP \in Spec$,*

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

Consequently:

> *$\mathcal{T}_0$ is stronger than any sound, compositional and non-absentminded property-oriented semantics for structured specifications built from flat specifications using union, translation and hiding.*

Instead of conclusions

Exercise: *Check if the assumption that $\mathcal{T}$ is non-absentminded in the key theorem and its corollary is necessary.*

(We don'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 $\mathrm{BS}_{\mathcal{T}(SP)}$ such that $\mathcal{T}(\mathrm{BS}_{\mathcal{T}(SP)}) = \mathcal{T}_s(\mathrm{BS}_{\mathcal{T}(SP)}) = \mathcal{T}(SP)$ and $\mathrm{Mod}[\mathrm{BS}_{\mathcal{T}(SP)}] = \mathrm{Mod}_{Sig[SP]}[\mathcal{T}(SP)]$.

Indeed — see below!

Sketch of a counterexample

to be (checked and) adjusted to the standard case

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 $M_1 \models \alpha$, $M_2 \not\models \alpha$, $M_3 \models \alpha$, $M_1 \models \beta$, $M_2 \not\models \beta$, $M_3 \not\models \beta$. Suppose we have a Σ-specification B^AD with $Mod[B^AD] = \{M_1\}$.

Let $\mathcal{T}$ be such that it drops 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 the structural rule plus:

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

Then $\mathcal{T}$ is sound and compositional, but for $\sigma(B^AD)$ it is stronger than the expected sound, monotone and one-step complete property-oriented semantics $\mathcal{T}_s$, which yields $\mathcal{T}_s(B^AD) = \{\alpha\}$ and $\mathcal{T}_s(\sigma(B^AD)) = \{\alpha\}$.

Ughhh!