



THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

Entailment for Structured Specifications

Citation for published version:

Hennicker, R, Sannella, D, Tarlecki, A & Wirsing, M 2017, Entailment for Structured Specifications. in B Woltzenlogel Paleo (ed.), *Towards an Encyclopaedia of Proof Systems*. College Publications, London, UK.

Link:

[Link to publication record in Edinburgh Research Explorer](#)

Document Version:

Peer reviewed version

Published In:

Towards an Encyclopaedia of Proof Systems

General rights

Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.



Entailment for Structured Specifications

(1988)

$$\begin{array}{c}
 \frac{SP \vdash \varphi_1 \quad \cdots \quad SP \vdash \varphi_n \quad \{\varphi_1, \dots, \varphi_n\} \vdash_{\text{Sig}[SP]} \varphi}{SP \vdash \varphi} \\
 \frac{}{\langle \Sigma, \Phi \rangle \vdash \varphi} \quad \varphi \in \Phi \\
 \frac{SP_1 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi} \quad \frac{SP_2 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi} \\
 \frac{SP \vdash \varphi}{SP \text{ with } \sigma \vdash \sigma(\varphi)} \quad \frac{SP \vdash \sigma(\varphi)}{SP \text{ hide via } \sigma \vdash \varphi}
 \end{array}$$

Clarifications: $\mathbf{INS} = \langle \mathbf{Sign}, \mathbf{Sen} : \mathbf{Sign} \rightarrow \mathbf{Set}, \mathbf{Mod} : \mathbf{Sign}^{op} \rightarrow \mathbf{Cat}, \langle \models_{\Sigma} \subseteq |\mathbf{Mod}(\Sigma)| \times \mathbf{Sen}(\Sigma) \rangle_{\Sigma \in \mathbf{Sign}} \rangle$ is an institution that defines the logical system used for specifications, SP , SP_1 and SP_2 are structured Σ -specifications over \mathbf{INS} , where Σ is a signature in the category \mathbf{Sign} , $\varphi, \varphi_1, \dots, \varphi_n$ are Σ -sentences, i.e. elements in $\mathbf{Sen}(\Sigma)$, Φ is a set of Σ -sentences, and $\sigma(\varphi)$ denotes $\mathbf{Sen}(\sigma)(\varphi)$, the translation of the sentence φ along $\sigma : \Sigma \rightarrow \Sigma'$. Structured specifications in \mathbf{INS} are built from basic specifications $\langle \Sigma, \Phi \rangle$, the union of Σ -specifications $SP_1 \cup SP_2$, the translation “ SP with σ ” of SP along a signature morphism $\sigma : \Sigma \rightarrow \Sigma'$, and hiding “ SP hide via σ ” for hiding the symbols in SP not occurring in the image of $\sigma : \Sigma' \rightarrow \Sigma$. $\text{Sig}[SP]$ is the signature of SP . Translations of Σ -sentences and Σ' -models along $\sigma : \Sigma \rightarrow \Sigma'$ are required to preserve satisfaction: for any $\varphi \in \mathbf{Sen}(\Sigma)$ and $M' \in |\mathbf{Mod}(\Sigma')|$, $M' \models_{\Sigma'} \mathbf{Sen}(\sigma)(\varphi) \Leftrightarrow \mathbf{Mod}(\sigma)(M') \models_{\Sigma} \varphi$. Finally, $\langle \vdash_{\Sigma} \subseteq \text{Pow}(\mathbf{Sen}(\Sigma)) \times \mathbf{Sen}(\Sigma) \rangle_{\Sigma \in \mathbf{Sign}}$ is a sound entailment relation for the satisfaction relation $\langle \models_{\Sigma} \rangle_{\Sigma \in \mathbf{Sign}}$.

The judgement $SP \vdash \varphi$ is meant to capture the property that φ is satisfied in all models of SP .

History: The first systems for proving entailment in structured specifications were given by Sannella and Burstall [1], Sannella and Tarlecki [2], and Wirsing [3]. The above presentation can be found in [6], Sect. 9.2.

Remarks: The system is sound; completeness is shown in [3] for the first-order logic instance and in [5, 6] for an institution \mathbf{INS} which is finitely exact, admits propositional operators, satisfies Craig interpolation, and has a complete entailment relation $\langle \vdash_{\Sigma} \rangle_{\Sigma \in \mathbf{Sign}}$. [7] shows that this is the most powerful sound proof system that is compositional in the structure of specifications. [4] provides additional rules for observability operators.

-
- [1] Donald Sannella and Rod M. Burstall. “Structured Theories in LCF”. In: *CAAP’83, Trees in Algebra and Programming, 8th Colloquium, Proc.* Vol. 159. LNCS. Springer, 1983, pp. 377–391.
 - [2] Donald Sannella and Andrzej Tarlecki. “Specifications in an Arbitrary Institution”. In: *Information and Computation* 76.2/3 (1988), pp. 165–210.
 - [3] Martin Wirsing. “Structured Specifications: Syntax, Semantics and Proof Calculus”. In: *Logic and Algebra of Specification, NATO Advanced Institute, 1991.* Vol. 94. Springer, 1993, pp. 411–442.
 - [4] Rolf Hennicker. *Structured Specifications with Behavioural Operators: Semantics, Proof Methods and Applications.* Habilitation thesis. LMU Munich, 1997.
 - [5] Tomasz Borzyszkowski. “Logical systems for structured specifications”. In: *Theoretical Computer Science* 286.2 (2002), pp. 197–245.
 - [6] Donald Sannella and Andrzej Tarlecki. *Foundations of Algebraic Specification and Formal Software Development.* Monographs in Theoretical Computer Science. An EATCS Series. Springer, 2012.
 - [7] Donald Sannella and Andrzej Tarlecki. “Property-oriented semantics of structured specifications”. In: *Mathematical Structures in Computer Science* 24.2 (2014), e240205.

Entry 22 by: Rolf Hennicker, Donald Sannella, Andrzej Tarlecki, Martin Wirsing