Entailment for Structured Specifications

Citation for published version:

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.

\[
\begin{array}{ccc}
SP \vdash \varphi_1 & \ldots & SP \vdash \varphi_n \quad \{\varphi_1, \ldots, \varphi_n\} \vdash_{\text{Sig}(SP)} \varphi \\
SP \vdash \varphi \\
\langle \Sigma, \Phi \rangle \vdash \varphi \\
SP_1 \vdash \varphi & SP_2 \vdash \varphi \\
SP_1 \cup SP_2 \vdash \varphi \\
SP \vdash \varphi & SP \vdash \sigma(\varphi) \\
SP \text{ with } \sigma \vdash \sigma(\varphi) \\
\end{array}
\]

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

The judgement \( SP \vdash \varphi \) is meant to capture the property that \( \varphi \) 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 INS which is finitely exact, admits propositional operators, satisfies Craig interpolation, and has a complete entailment relation \( \langle \models \Sigma \rangle_{\Sigma \in \text{Sign}} \). [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.


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