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
Entailment for Structured Specifications (1988)

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

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