Entailment for Structured Specifications (1988)

$$\frac{SP \vdash \varphi_1 \quad \cdots \quad SP \vdash \varphi_n \qquad \{\varphi_1,\ldots,\varphi_n\} \vdash_{Sig[SP]} \varphi}{SP \vdash \varphi}$$

$$\frac{}{\langle \Sigma, \Phi\rangle \vdash \varphi}\ \varphi \in \Phi$$

$$\frac{SP_1 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi} \qquad \frac{SP_2 \vdash \varphi}{SP_1 \cup SP_2 \vdash \varphi}$$

$$\frac{SP \vdash \varphi}{SP\ \textbf{with}\ \sigma \vdash \sigma(\varphi)} \qquad \frac{SP \vdash \sigma(\varphi)}{SP\ \textbf{hide via}\ \sigma \vdash \varphi}$$

Clarifications: $\mathbf{INS} = \langle \mathbf{Sign}, \mathbf{Sen}\colon \mathbf{Sign} \to \mathbf{Set}, \mathbf{Mod}\colon \mathbf{Sign}^{op} \to \mathbf{Cat}, \langle \models_\Sigma \subseteq |\mathbf{Mod}(\Sigma)| \times \mathbf{Sen}(\Sigma)\rangle_{\Sigma \in |\mathbf{Sign}|}\rangle$ is an institution that defines the logical system used for specifications, SP, SP_1 and SP_2 are structured Σ-specifications over **INS**, where Σ is a signature in the category **Sign**, $\varphi, \varphi_1, \ldots, \varphi_n$ 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 $\sigma\colon \Sigma \to \Sigma'$. Structured specifications in **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 $\sigma\colon \Sigma \to \Sigma'$, and hiding "$SP$ **hide via** σ" for hiding the symbols in SP not occurring in the image of $\sigma\colon \Sigma' \to \Sigma$. $Sig[SP]$ is the signature of SP. Translations of Σ-sentences and Σ'-models along $\sigma\colon \Sigma \to \Sigma'$ 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, $\langle \vdash_\Sigma \subseteq Pow(\mathbf{Sen}(\Sigma)) \times \mathbf{Sen}(\Sigma)\rangle_{\Sigma \in |\mathbf{Sign}|}$ 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 **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