# Refinement of Structured Specifications (1991)

$$\frac{\text{for all } \varphi \in \Phi, SP \vdash \varphi}{SP \vdash \langle Sig[SP], \Phi\rangle}$$

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

$$\frac{SP' \textbf{ hide via } \sigma \vdash SP}{SP' \vdash SP \textbf{ with } \sigma}$$

$$\frac{\widehat{SP} \vdash SP'}{SP \vdash SP' \textbf{ hide via } \sigma} \quad \sigma\colon SP \to \widehat{SP} \text{ admits model expansion}$$

**Clarifications: INS** = $\langle$**Sign**, **Sen**: **Sign** $\to$ **Set**, **Mod**: **Sign**$^{op}$ $\to$ **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, and $SP$, $SP_1$, $SP_2$, $SP'$ and $\widehat{SP}$ are structured specifications over **INS**. Structured specifications in **INS** are built from basic specifications $\langle \Sigma, \Phi\rangle$ where $\Sigma \in |\mathbf{Sign}|$ and $\Phi \subseteq \mathbf{Sen}(\Sigma)$, the union of $\Sigma$-specifications $SP_1 \cup SP_2$, the translation "$SP$ **with** $\sigma$" of $SP$ along a signature morphism $\sigma\colon \Sigma \to \Sigma'$, and hiding "$SP$ **hide via** $\sigma$" for hiding the symbols in $SP$ not occurring in the image of $\sigma\colon \Sigma' \to \Sigma$. $Sig[SP]$ is the signature of $SP$ and $Mod[SP] \subseteq |\mathbf{Mod}(Sig[SP])|$ is the class of models of $SP$. A signature morphism $\sigma\colon Sig[SP] \to Sig[SP']$ is a specification morphism $\sigma\colon SP \to SP'$ if for every $M' \in Mod[SP']$, $\mathbf{Mod}(\sigma)(M') \in Mod[SP]$. Then $\sigma$ admits model expansion if $\mathbf{Mod}(\sigma)\colon Mod[SP'] \to Mod[SP]$ is surjective. The judgement $SP \vdash \varphi$ is entailment for structured specifications which is required to be sound: $SP \vdash \varphi$ implies $M \models_{Sig[SP]} \varphi$ for every $M \in Mod[SP]$.

The judgement $SP \vdash SP'$ is meant to capture that $SP$ refines (or entails) $SP'$, that is, $Sig[SP] = Sig[SP']$ and $Mod[SP] \subseteq Mod[SP']$.

**History:** The first proof systems for refinement of structured specifications were given by Farrés-Casals [1] and Wirsing [2]. The above presentation can be found in [4], Sect. 9.3.

**Remarks:** The calculus is sound; it is complete if the underlying entailment system for structured specifications is complete [2, 4]. [3] provides additional rules for observability operators to support refinement by observational abstraction.


[1] Jordi Farrés-Casals. "Proving Correctness of Constructor Implementations". In: *Mathematical Foundations of Computer Science 1989, MFCS'89, Porabka-Kozubnik, Poland, August 28 - September 1, 1989, Proceedings*. Vol. 379. Lecture Notes in Computer Science. Springer, 1989, pp. 225–235.

[2] Martin Wirsing. "Structured Specifications: Syntax, Semantics and Proof Calculus". In: *Logic and Algebra of Specification, Proceedings of the NATO Advanced Institute, 1991*. Vol. 94. Springer, 1993.

[3] Rolf Hennicker. *Structured Specifications with Behavioural Operators: Semantics, Proof Methods and Applications*. Habilitation thesis. LMU Munich, 1997.

[4] Donald Sannella and Andrzej Tarlecki. *Foundations of Algebraic Specification and Formal Software Development*. Monographs in Theoretical Computer Science. An EATCS Series. Springer, 2012.



Entry 29 by: Rolf Hennicker, Donald Sannella , Andrzej Tarlecki , Martin Wirsing