Several compositional methods for the development of systems use the assumption commitment paradigm, by which a system (a process or a network of concurrent processes) is required to satisfy the commitment whenever it operates in an environment that respects the assumption. Compositional methods propose rules for deducing the correctness of concurrent process $P_1|P_2$ with respect to its specification from the correctness of the components $P_1$ and $P_2$ with respect to their specifications. It appears that the parallel rules for assumption-commitment specifications of state-based and message-based processes look remarkably different.

In order to relate them, in the first part of the paper, a semantic parallel rule is formulated which abstracts from the way of communication. In that semantic framework, we consider abstract computations as labeled sequences of elements, where both elements and labels are left unspecified. We denote by $\mathcal{M}(P)$ the set of computations of a process $P$ but omit the definition of the modeling function $\mathcal{M}$. Then, a process is said to be correct with respect to an assumption-commitment specification if all the computations of the process are contained in the set of sequences corresponding to the specification. This set is constructed out of the set of computations allowed by the safety assumptions, the set of computations allowed by the safety commitments, and the set of computations allowed by the general (safety and/or liveness) commitments. The set of computations of $P_1|P_2$ is denoted by $\mathcal{M}(P_1) \otimes \mathcal{M}(P_2)$ where the merging operator $\otimes$ is again left unspecified. This operator behaves as a parameter of the semantic rule. In the second part of the paper, this semantic rule is gradually transformed into specific (language-dependent) rules for assumption-commitment specifications of state-based and message-based processes by giving specific definitions for the unspecific notions used in the semantic framework. In each case, the transformation involves four steps. In the first step, we give the exact definition of a computation and the definition of $\mathcal{M}(P)$ for the considered process language. In the second step, we define the merging operator $\otimes$ and check that $\mathcal{M}(P_1|P_2)$ is equal to $\mathcal{M}(P_1) \otimes \mathcal{M}(P_2)$. In the third step, we define the sets of computations allowed by the assumption and the commitment parts of the specification. In the fourth step, we finally show that the premises of the semantic rule can be retrieved from the premises of the syntactic rules. Therefore, this paper shows that the syntactic parallel rules for assumption-commitment specifications for both state-based and message-based processes are just instances of the same semantic rule.

Reviewer: P. Collette (Manchester)


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.