

# Component Interfaces for System Synthesis

Sven Schewe and Bernd Finkbeiner

Universität des Saarlandes, 66123 Saarbrücken, Germany  
{schewe|finkbeiner}@cs.uni-sb.de

**Abstract.** Component-based design is widely considered the major time and cost effective approach to the development of distributed systems. A key concept in this approach is the notion of interface guarantees. The interfaces guarantees of a component are the properties the component can establish in every environment, that is, even in the case that the remainder of the system cooperates to violate them. In this setting, the behavior of the local environment of a component is hostile (rather than maximal). We present a sound and complete proof rule for the compositional construction of distributed systems that is based on interface guarantees. Our proof rule establishes a rigorous framework for the specification and analysis of interfaces that divides the design process into two natural phases. In the first phase, the specification is strengthened into a conjunction of interface guarantees for the individual processes. In the second phase, the processes are constructed to provide their respective interface guarantees. Strengthening the specification into a conjunction of interface guarantees is the only manual step, while (1) checking the correctness of the strengthening, (2) testing if the required interface guarantees are realizable by the individual components, and (3) constructing component implementation that provide the required interface guarantees can be automated. We show that the satisfiability and synthesis problem for branching-time specifications read as interface guarantees are exponentially harder than under the traditional assumption of maximal environments.