COMPOSITIONAL VERIFICATION OF COMPONENT-BASED HETEROGENEOUS SYSTEMS

Yan Jin

A THESIS SUBMITTED FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN THE SCHOOL OF COMPUTER SCIENCE

UNIVERSITY OF ADELAIDE

January 2004

Abstract

It is widely acknowledged that mathematically-based formal specification and verification methods can provide substantial help in revealing ambiguity and inconsistency of informal system descriptions, and increase confidence in the correctness of system designs. However, as their complexity rapidly grows, modern computer-based systems often consist of parts (or subsystems) with very different characteristics, *e.g.* data-centred vs. control-oriented. Traditional formal methods relying on a single specification language are no longer appropriate for coping with all aspects of such a system. A combination of languages to be used for system specification is required.

To meet this need, it is essential to devise sound principles and techniques for integrating various languages and for reasoning about the resultant component-based heterogeneous system. It is also essential to provide mechanical support for their formal verification. This thesis focuses on discrete-event systems and a class of specification languages, viz. graph-like visual languages. It takes a two-step approach to study these fundamental issues and seek practical, tool-supported solutions.

Firstly, an underlying methodological framework is proposed, which enables both the use of different languages (or formalisms) to describe different subsystems and the automatic verification of heterogeneous systems. This framework is built on a solid semantic base of interconnected discrete-event components. It uses a semantic interpretation approach to heterogeneous systems, specifying language-specific interpreters which enable heterogeneous components to be defined in terms of this semantic base. More specifically, the interpreters are parameterized with component models and execute on behalf of the components according to the semantics of the specification languages. They are also enhanced with facilities that allow analysis tools to access the state and transition information of the components and control their concurrent execution. As a

consequence, not only is the exhaustive analysis of heterogeneous systems supported, but also an open and extensible platform is provided, which allows various graph-like languages and formal verification techniques to be used for specifying and reasoning about heterogeneous systems.

Secondly, this thesis focuses on model checking, a robust and largely automatic approach to system formal verification. It proposes a compositional approach to combat the state space explosion problem, a well-known obstacle to model checking. This approach divides a verification problem of a system into sub-problems of its components and then addresses each sub-problem independently. The key is to specify abstract communication protocols for components using a lightweight formal language — *interface automata* [54], and then utilise these protocols as behavioural contracts for independent analysis of the components and their composition patterns. It is demonstrated that, adopting this divide-and-conquer approach, not only the basic properties of component-based systems, such as consistency and deadlock freedom, but also their safety properties can be proved. Furthermore, this compositional approach is implemented as automated tools in the context of the Moses tool suite [65], utilising the semantic interpretation approach proposed earlier. These tools are then applied to the verification of a non-trivial distributed embedded system — the Production Cell [138]. It is shown that a significant reduction in complexity of system verification is achieved.

Contents