J Autom Reasoning (2012) 48:419–439
DOI 10.1007/s10817-010-9206-x

Proof Pearl: A Formal Proof of Dally and Seitz' Necessary and Sufficient Condition for Deadlock-Free Routing in Interconnection Networks

Freek Verbeek · Julien Schmaltz

Received: 19 August 2009 / Accepted: 7 September 2010 / Published online: 18 September 2010

Abstract Avoiding deadlock is crucial to interconnection networks. In '87, Dally and Seitz proposed a necessary and sufficient condition for deadlock-free routing. This condition states that a routing function is deadlock-free if and only if its channel dependency graph is acyclic. We formally define and prove a slightly different condition from which the original condition of Dally and Seitz can be derived. Dally and Seitz prove that a deadlock situation induces cyclic dependencies by *reductio ad absurdum*. In contrast we introduce the notion of a *waiting graph* from which we explicitly construct a cyclic dependency from a deadlock situation. Moreover, our proof is structured in such a way that it only depends on a small set of proof obligations associated to arbitrary routing functions and switching policies. Discharging these proof obligations is sufficient to instantiate our condition for deadlock-free routing on particular networks. Our condition and its proof have been formalized using the ACL2 theorem proving system.

Keywords Deadlock-free routing · Interactive theorem proving · ACL2

This research is supported by NWO/EW project Formal Validation of Deadlock Avoidance Mechanisms (FVDAM) under grant no. 612.064.811.

F. Verbeek · J. Schmaltz (✉)
Institute for Computing and Information Sciences, Radboud University Nijmegen,
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
e-mail: julien@cs.ru.nl

F. Verbeek
e-mail: f.verbeek@cs.ru.nl

F. Verbeek · J. Schmaltz
School of Computer Science, Open University of The Netherlands,
P.O. Box 2960, 6401 DL Heerlen, The Netherlands