Verification of a Translator for MDG's library in HOL

Haiyan Xiong, Paul Curzon, Sofiène Tahar and Ann Blandford

Presented by Haiyan Xiong, School of Computing Science, Middlesex University, h.xiong@mdx.ac.uk
Sofiène Tahar is at ECE Dept., Concordia University, Canada,
Paul Curzon, and Ann Blandford are at School of Computing Science, Middlesex University

In the 1990s, due to the efficiency breakthrough provided by Binary Decision Diagrams (BDDs), industry has successfully applied BDD-based tools in digital circuit synthesis and verification. Now, an important consideration is whether the verification systems are themselves correct. Ideally verification systems should themselves be formally verified using a verification system with a different architecture. Based on this consideration, we investigate the verification of aspects of the Multiway Decision Graphs (MDG) verification system using the higher order logic (HOL) theorem prover. In the MDG system, the specification language is MDG-HDL. It allows the use of abstract variables for representing data signals. Some MDG-HDL components are compiled directly into decision graphs. Others are compiled via a tabular representation into decision graphs. The aim of our work is to use the HOL system to prove properties of a formal specification of this compiler. In particular, we will demonstrate that this compiler specification preserves the correctness results produced by the MDG verification system. The compiler specification is split into two phases. The first phase compiles the MDG-HDL language into the TABLE language. The second phase compiles the TABLE language into decision graphs. In this paper, we discuss the verification of the first compilation stage.