

Constructing Correct Circuits

Hardware Modelling with Dependent Types

Edwin Brady, James McKinna, and Kevin Hammond

School of Computer Science,
University of St Andrews, St Andrews, Scotland.

Abstract

Writing correct programs is difficult, particularly programs modelling low level hardware which work at the level of bits and logic gates. We describe a novel approach to constructing correct low level programs, by using dependent types to give an explicit and checkable link between the low level program and its high level meaning. Our approach closely links programming and theorem proving in that a type correct program is a constructive proof that the program meets its specification. We illustrate our approach by implementing a carry ripple adder for binary numbers.