Integrating Hardware Description Languages and Proof Systems*

K. G. W. Goossens
Laboratory for Foundations of Computer Science
University of Edinburgh

April 1992

Hardware description languages have been used in industry since the 1960s to document and simulate hardware designs. Simulation is a very useful tool to find design faults without the need to manufacture the design. A well known drawback of simulation, however, is that the number of inputs combinations (or test vectors) increases exponentially. For modern designs, it would take years to fully simulate a design. In practice a limited number of test vectors are used to probe the circuit, possibly failing to uncover faults. A response to this situation has resulted in *formal verification* of hardware designs. This entails using a mathematical proof system to describe the design, followed by proving correctness with respect to its specification. Most proposed methodologies are not automated, and need considerable expertise to be used. Although formal verification methods remove the exponential explosion occurring for simulation, verification takes considerable time. A severe drawback is that many notations are employed, depending on the tools which are used. Industrial hardware description languages have not yet been used, alienating the hardware verification field from the industrial designers.

This work aims to address this problem. To be able to use a hardware description language in conjunction with a proof system it must have a firm mathematical basis. This work has provided *formal semantics* for a widely used industrial hardware description language called ELLA[1]. This semantics has been embedded in the LAMBDA[2] proof system. LAMBDA is a higher order logic proof system which allows specifications of designs to be stated in a natural and succinct form. Using the proof system, a number of results have been proved which confirm the correctness of the model used in the industrial simulator for ELLA. It is now possible for industrial users to describe designs in LAMBDA using a familiar ELLA notation. Designs written in this standard notation may be proven correct using standard formal verification techniques. Moreover, circuits may be simulated within the proof system, using the underlying formal definition of the hardware description language. In addition, powerful *symbolic simulation* techniques may be used, allowing a great reduction in the number of test vectors needed to fully simulate a design.

References

[1] Computer General Electronic Design, The New Church, Henry St, Bath BA1 1JR, England. *The ELLA Language Reference Manual*, issue 4.0, 1990.

[2] Mick Francis, Simon Finn, and Ellie Mayger. *Reference Manual for the Lambda System.* Abstract Hardware Limited, version 3.2, November 1990.

*This poster was presented at the IFIP 12th World Congress in Madrid, Spain, September 1992