Journal of Applied Logic 9 (2011) 41–60

Contents lists available at ScienceDirect

Journal of Applied Logic

www.elsevier.com/locate/jal

Formal reliability analysis of combinational circuits using theorem proving

Osman Hasan [a,*], Jigar Patel [b], Sofiène Tahar [b]

[a] School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Sector H-12, Islamabad, Pakistan
[b] Department of Electrical and Computer Engineering, Concordia University, 1455 de Maisonneuve W., Montreal, Quebec, H3G 1M8, Canada

ARTICLE INFO

Article history:
Received 13 September 2010
Accepted 6 December 2010
Available online 12 January 2011

Keywords:
Formal verification
Higher-order logic
HOL
Probability theory
Reliability analysis
Theorem proving

ABSTRACT

Reliability analysis of combinational circuits has become imperative these days due to the extensive usage of nanotechnologies in their fabrication. Traditionally, reliability analysis of combinational circuits is done using simulation or paper-and-pencil proof methods. But, these techniques do not ensure accurate results and thus may lead to disastrous consequences when dealing with safety-critical applications. In this paper, we mainly tackle the accuracy problem of these traditional reliability analysis approaches by presenting a formal reliability analysis framework based on higher-order-logic theorem proving. We present the higher-order-logic formalization of the notions of fault and reliability for combinational circuits and formally verify the von-Neumann fault models for most of the commonly used logic gates, such as, AND, NOT, OR, etc. This formal infrastructure is then used along with a computer program, written in C++, to automatically reason about the reliability of any combinational circuit within a higher-order-logic theorem prover (HOL). For illustration purposes, we utilize the proposed framework to analyze the reliability of a few benchmark combinational circuits.

1. Introduction

Reliability analysis involves the usage of probabilistic techniques for the prediction of reliability related parameters, such as a system's resistance to failure and its ability to perform a required function under some given conditions. This information is in turn utilized to design more reliable and secure systems. The reliability analysis of combinational circuits has been conducted since their early introduction [20,22]. However, the ability to efficiently analyze the reliability of combinational circuits has become very challenging nowadays because of their growing sizes and complexity and the inherent variability in the nanoscale fabrication processes.

Traditionally, simulation has been the most commonly used computer based reliability analysis technique for combinational circuits, e.g., see [17,11,12]. Most simulation based reliability analysis software provide a programming environment for defining functions that approximate random variables for probability distributions. The sources of error and the input patterns in combinational circuits are random quantities and are thus modeled by these functions and the system is analyzed using computer simulation techniques [7], such as the Monte Carlo Method [19], where the main idea is to approximately answer a query on a probability distribution by analyzing a large number of samples. Statistical quantities, such as expectation and variance, may then be calculated, based on the data collected during the sampling process, using their mathematical relations in a computer. Due to the inherent nature of simulation coupled with the usage of computer arithmetic, the reliability analysis results attained by the simulation approach can never be termed as 100% accurate.

[*] Corresponding author.
E-mail addresses: osman.hasan@seecs.nust.edu.pk (O. Hasan), ji_p@ece.concordia.ca (J. Patel), tahar@ece.concordia.ca (S. Tahar).

1570-8683/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jal.2011.01.002

The accuracy of reliability analysis results has become imperative these days because of the extensive usage of hardware systems in safety critical areas, like medicine, military and transportation, where an erroneous analysis could even result in the loss of human lives. Formal methods are capable of conducting accurate system analysis and thus overcome the above mentioned limitations of simulation [10]. The main principle behind formal analysis of a system is to construct a computer based mathematical model of the given system and formally verify, within a computer, that this model meets rigorous specifications of intended behavior. Two of the most commonly used formal verification methods are model checking [2] and higher-order-logic theorem proving [8]. Model checking is an automatic verification approach for systems that can be expressed as a finite-state machine. Higher-order-logic theorem proving, on the other hand, is an interactive verification approach that allows us to mathematically reason about system properties by representing the behavior of a system in higher-order logic.

We believe that due to the recent developments in the formalization of probability theory concepts in higher-order-logic [18,14], we are now at the stage where we can handle the reliability analysis of a variety of combinational circuits in a higher-order-logic theorem prover with reasonable amount of modeling and verification efforts. The main motivation of using a higher-order-logic theorem prover for this purpose is the ability to formally analyze a broader range of combinational circuits and reliability properties by leveraging upon the high expressiveness of the underlying logic. But, this option involves two main challenges. The first one is that we need a foundational infrastructure to be able to formally specify and reason about the reliability of erroneous behavior of logical gates, which is unpredictable in nature, in logical terms. Whereas, the second one is related to the inherent nature of the higher-order-logic theorem proving, i.e., the tedious user efforts involved in interactively reasoning about the reliability properties of the system in hand. The second point mentioned here is one of the major limitations associated with the theorem proving approach and is the biggest reason why theorem proving has not been widely accepted as a verification tool in the industry.

This paper tackles both of the above mentioned challenges and, to the best of our knowledge, presents the first automatic theorem proving based approach for the reliability analysis of combinational circuits. The proposed approach is primarily inspired by the probabilistic gate models (PGM) method [11,12,25]. The main idea behind this approach is to formally represent the erroneous behavior of all the basic logical gates (AND, OR, NOT, etc.) in terms of the probabilities of obtaining *True* or a logical 1 at their inputs. These expressions, also referred to as the von-Neumann error models for combinational gates, can then be used to evaluate the reliability of a combinational circuit that is essentially a structure composed of the basic logical gates. We have also developed a C++ program that translates a combinational circuit, expressed in the hardware description language VHDL, to its corresponding logical description, writes the reliability theorem and generates its proof script, based on a rich library of formally verified theorems corresponding to the PGMs, that we have developed in this work. This kind of a setting makes the approach automatic, which is an attractive feature for the microelectronic design engineers, who are usually not comfortable in working with pure formal verification based approaches or logical reasoning.

The definitions and theorems, related to the von-Neumann error models for the basic gates and the generic reliability expression of a combinational circuit, exhibit random and probabilistic behaviors, due to the random nature of gate-faults. Therefore, they have been formally defined by building upon the methodology for higher-order-logic formalization of probabilistic algorithms given in [18]. Since this formalization has been done using the HOL theorem prover [9], the proposed work has also been done using HOL.

To illustrate the practical effectiveness and demonstrate the utilization of the proposed framework, we use it to assess the reliabilities of a comparator, a full adder and five benchmarks, i.e., LGSynth'91-C17, LGSynth'91-Majority, LGSynth'91-Parity, ISCAS-85-74283 (4-bit adder) and ISCAS-85-C6288 (16 × 16 multiplier). The comparator is a simple combinational circuit and is used to illustrate the working of the proposed automated framework. The simulation based PGM approach [12] was used to assess the reliability of the full adder circuit and therefore we assess its reliability using the proposed approach to highlight the accuracy of our results. The four benchmarks LGSynth'91-C17, LGSynth'91-Majority, LGSynth'91-Parity, and ISCAS-85-74283 have been analyzed to demonstrate the applicability of the approach to analyze real-world problems. We report some statistics, like the size of the circuit and the analysis time, for these benchmarks. Finally, the ISCAS-85-C6288 benchmark has been picked up due to its comparatively larger size, i.e., approximately 2400 gates. Instead of modeling this circuit at the gate level, we illustrate how the proposed approach can be used to model the given circuit using full adder cells, which significantly reduces the size of the model and thus demonstrates the scalability of the proposed approach towards hierarchical designs.

We have already presented some of the ideas and formalization related to the formalization of von-Neumann error models for the basic gates in a workshop [15]. The current paper is an extension to that work as we present further formalization details. Likewise, the idea of automatically reasoning about the reliability of combinational circuits is novel. The extensive case studies, presented in the current paper, is also one of the major extensions to our first paper [15] in the area.

The rest of the paper is organized as follows. Section 2 provides a review of the related work. In Section 3, we present a brief overview of the HOL theorem prover and the theorem proving based probabilistic analysis. Sections 4 and 5 present the description of the core formalizations of this paper that allow us to automatically conduct the reliability analysis of combinational circuits, i.e., the formalization of von-Neumann models for the basic logical gates and the generic reliability expression, respectively. Then, we illustrate the proposed framework using the comparator circuit example in Section 6. The case studies are given in Section 7. Finally, Section 8 concludes the paper.