Ingeniería Investigación y Tecnología, volumen XV (número 4), octubre-diciembre 2014: 615-623
ISSN 1405-7743 FI-UNAM
(artículo arbitrado)

State of the Art in the Research of Formal Verification

Estado del arte de la investigación en verificación formal

Serna-M. Edgar
Corporación Universitaria Remington, Medellín, Colombia
E-mail: edgar.serna@remington.edu.co

Morales-V. David
Diversien S.A.S. Medellín, Colombia
E-mail: david.morales@diversien.com

Information on the article: received: May 2013, accepted: July 2013

Abstract

In recent years research in *formal verification* of hardware and software has reached important progresses in the development of methodologies and tools to meet the increasing complexity of systems. The explicit role of Formal Verification is to find errors and to improve the reliability on the accuracy of system design, which implies a challenge for *software engineering* of this century. The purpose of this research is to perform a systematic review of the literature to establish the state of the art of research in *formal verification* during the last 10 years and to identify the approaches, methods, techniques and methodologies used, as well as the intensity of those research activities. During the process it was found that research in this field has doubled since 2005, and that the mean value of researches conducted year after year remains the same and that prevail the application in control and interaction systems. Additionally it was found that, the case study is the most used method and that empirical research is the most applied type.

Keywords:

- formal verification
- formal methods
- software engineering
- engineering techniques
- research approaches

Resumen

En años recientes, la investigación en verificación formal de hardware y software ha logrado importantes progresos en el desarrollo de metodologías y herramientas para hacer frente a la creciente complejidad de los sistemas. La función explícita de la verificación formal es encontrar errores y mejorar la confianza en la exactitud del diseño del sistema, lo que supone un reto para la ingeniería de software de este siglo. El objetivo de esta investigación fue realizar una revisión sistemática a la literatura para determinar el estado del arte de la investigación en verificación formal en los últimos 10 años e identificar los enfoques, métodos, técnicas y metodologías empleadas, lo mismo que la intensidad de esa investigación. En el proceso se encontró que la investigación en esta área se duplicó a partir del año 2005, que hasta el momento mantiene un número promedio de investigaciones año tras año y que predomina la aplicación en sistemas de control e interacción. Además, que el estudio de caso es el método más utilizado y que la investigación empírica es la más aplicada.

Descriptores:

- *verificación formal*
- *métodos formales*
- *ingeniería de software*
- *técnicas de ingeniería*
- *enfoques de investigación*

Introduction

Functional verification has become the bottleneck for the design of complex systems. Simulating designs is money-demanding and time-demanding and performing a complete simulation is almost impossible. Currently, as a solution for these problems, designers have started using formal methods to perform *formal verification* on most of products. But there is still a wide gap for the verification of big designs, which can be built but cannot be verified completely because of the complexity of the problems they deal with (Sülflow *et al*., 2009). This has caused that in many countries, the academic world, industry and governments must face the challenge of reducing this technological gap and proposing new and ingenious solutions for specifying, designing, structuring and applying test cases by using *formal verification*.

Formal verification is a crucial element in the development of the current complex information systems. Moore's Law is still applied to determine the growth rate of the complexity of software and hardware products, but the complexity of verification becomes more complicated. In fact, theoretically, it augments exponentially with product's complexity and doubles in the same way with time. The community of computer sciences recognizes that functional verification is an important obstacle for a design methodology, and that it demands up to 70% of developing time and resources. But, despite the significant amount of efforts and resources applied in verification, functional faults continue as the cause of the significant number of errors of the final product. In extreme situations, the errors are artifacts of the simulation because they are not detected due to their non-exhaustive nature of the verification which is based in simulation. The real fact is that it does not matter how much time is applied in simulation or how exhaustive is the test plan, any attempt to validate a design by using simulation is by itself incomplete for any system.

Formal verification (FV) is a systematic process that uses mathematical reasoning to verify that design specification remains the same during implementation. With this verification is possible to overcome the challenges of simulation because all the possible input values can be explored algorithmically or exhaustively. In other words, to achieve a high degree of observation of the product it is not necessary to exaggerate the design or creating multiple scenarios.

One of the objectives of FV is to guarantee the complete coverage of the space of the states in the tested design, to achieve that it uses and applies techniques like model verification through the exploration of space of states and automated techniques to demonstrate the theorems. Currently, the most automated and most accepted FV technique is *Symbolic Model Verifier* or SMV and, despite its success as an important method for the *formal verification* of sequential commercial designs, is still limited in relation to the size of the verifiable designs (Copty *et al*., 2001). *Formal verification* requires that engineers think different. For instance, simulation is empirical, this means that using trial and error to test all of the possible combinations and try to discover errors can take significant time. For this reason, it does not fully achieve it. Besides, because engineers must define and create a high number of input scenarios, they focus their efforts on *breaking* the design but not on which design *must do*. *Formal verification*, on the contrary, is mathematical and exhaustive and allows engineers become focused exclusively in finding which one is the correct behavior of the design.

The aim of this research is to conduct a systematic review in the literature regarding research in *formal verification* during the last decade, to determine the approaches, methods, techniques and research methodologies used and the intensity of these research activities. To achieve that, the paradigm of evidence-based research was used. The possibility of using this paradigm is proposed in Kitchenham *et al*. (2004) and Dyba *et al*. (2005), and the goal is to identify a question that can be answered, which could provide information and which can lead to evidences for that answer and evaluate it (Brereton *et al*., 2007). Thus, a systematic review to the literature is the first stage to conduct evidence-based research. The guidelines to perform a systematic review to the literature are explained in detail in Brereton *et al*. (2007) and Kitchenham (2009).

In the next section, the methodology applied in this research is described; the third section shows and analyzes the results obtained; the following section shows possible threats and limitations for validation and the last section gives details on conclusions and future work proposals.

Methodological process

Performing a systematic review to literature can be divided in three main stages (Brereton *et al*., 2007): (1) planning, (2) execution and (3) documentation, which in turn divides in a combination of other simpler procedures, as shown in Table 1.

According to Kitchenham (2009) and Kitchenham *et al*. (2009), planning a systematic review involves six definitions: