Newcastle University
School of Computing Science

CSC3304 : Software Verification Technology
Coursework 2011

Model Checking Research Report : IBM AS/400 Compression Cache

Nicolas Desfeux

Newcastle Upon Tyne, December 2, 2011

Contents

Introduction

Nowadays, the need for confidence in hardware and software is higher than ever. That's why companies need to proof the exactitude of the product or service they want to provide. Whether we speak of hardware or software, verification goals is to assure that it satisfies all the specifications expected. Model Checking is a verification method based algorithmic check of systems, or abstraction of the system. This discipline, in constant evolution, is a good way to provide insurance that a system respect design and development specifications.

The purpose of this document is to present an application of model checking in a real world company. We decided to focus on an IBM[1] device : the IBM AS/400 server[2][10]. We'll start by shortly introduce IBM and the AS/400 server, then we'll spend more time on why and how verification was used by IBM on this device.

1 IBM AS/400 Server

1.1 IBM

International Business Machines, also known as IBM [6][9], is a major company in all computers' domain. They develop hardware and software solutions for professional and private users.They also provide services in a lot of subjects related to computers (like services in security and confidentiality). IBM is a well known supplier for hardware companies as Intel for example.

IBM has a subdivision dedicated to hardware and materials. It carries on an entire life cycle for each products. It goes from the development to recycling, including integration and on site installation. It's in that division that are design and developed IBM's AS/400.
IBM also have a subdivision called IBM Research[5] , which develop and implement most of the verification tools and method use by IBM. IBM Research does study about a lot of subject, from chemistry to computing sciences. That's a big part of IBM company.

[1] International Business Machines

1.2 AS/400 Server

AS/400 Server is an IBM server dedicate to business.He was commercialize first in 1988. This device is based on 5 principles :

- Technology Independence : Isolation between hardware and software. Software don't have to care about which hardware is used.
- Object-Based Design : All the AS 400 architecture is Object-Based. That's a plus for the security [1]
- Hardware Integration : Focus on simple operation on huge data volume.
- Software Integration : Every component needed is included and tested by IBM.
- Single-Level Store : Virtual memory principles applies on AS/400.

Nowadays AS/400 server is regroup with other servers under the name of POWER System[4] . POWER provide an entire computing system, form hardware to software.

2 Model checking of IBM AS/400 Server

IBM have dedicated research laboratory working on verification. For example, IBM Haifa Research Laboratory works a lot on Formal Verification and Testing Technologies [3]. Verification have been used on both hardware and software part of AS/400.

2.1 Model checking in IBM

Verification is an entire part of the life cycle of IBM's hardware products. That's important for hardware development. It also make them save money, by avoiding work again on a products that didn't respect specification. IBM have an entire Verification and Analytics department, which keep IBM up to date on verification.

Having laboratory working on Verification allows IBM to create it own verification tools, and especially a model checker : Rulebase[7]. This tools is provided for verification engineers and designers. It's more dedicate to hardware formal verification.

It implements several model checking algorithms, and works as a classic model checker : state space reduction, generation of counter examples,...
The purpose of this tools is to make the verification process easier and faster. To use RuleBase, engineer used PSL/Sugar language. It's used to design the functional properties of design. This language have been develop by IBM (Sugar), and become a standard for Property Specification Language (under the name of PSL).

Late detection of bugs is expensive. IBM decided to spend money on verification (creating it own tools and language, spend time on model checking...), in order to save money on bug correction.

2.2 Using model checking on the AS/400 Server

Model checking was used on AS/400. We will focus on the use of model checking on the Compression cache. Previously compressed responses are stored in the compression cache, allowing for quicker response times. It needs to be verify, especially because it's tools that handle with data transfer. When AS/400 was designed, designers created the Compression Cache model, so they have no idea if it was going to work. Perform a model checking on this new architecture was a way to validate choices made by designers.

2.2.1 Properties that needs to be verify

In the AS/400 Server, a coherence is needed between data from the compression cache and data you found in other system cache. That's a property that model checking can handle, as it consist on checking good data transfer, and equality between caches data.
Data can also travel from the cache to the processors. For the good work of the AS/400, IBM has to be sure of the correctness data delivered to processors. Those are here safety and liveness properties that IBM had to check, and model checking is a very good way to check it.

2.2.2 Verification Process

Verification engineers didn't wait the end of development to start verification. They build an abstract model, and model checked it . This need a good communication between designers and verifiers, who have to work together. This model have been update each time design and architecture of the AS/400 architecture changed. The abstract model was created by formal Verification specialists, who know enough about model checking. They had to choose the good abstraction to deal the space and time problems include with model checking.

2.2.3 Verification Result

The use of RuleBase with those properties leads to the discover of several errors. Those errors where about architecture of the Compression cache. They could have lead to some coherence trouble. As an example, here is one of the error found : the bus protocol defines a time lag between receiving a request and responding to it [11]. This have leads to an update of the system architecture. Thanks to the model checking, those errors have been corrected before it becomes to hard to correct them. It also provide a confirmation that the new system design by IBM (Compression Cache) works as they expected.

Conclusion

IBM uses his own tools for model checking, but the purpose is always the same : being able to provide products that respect precise specifications. Thanks to those tools, they achieve to solve some difficult verifications problems. The AS/400 Server Compression cache may not be verify without those tools. Model checking on IBM's AS/400 Server Compression Cache helps engineers to define new properties and environments for their new servers (Power systems). For IBM, model checking allows verification of specifications, but also hardware improvements. It also confirmed and validated improvements made by engineers on the system itself.

References

[1] Google. Object-oriented security. http://www.object-oriented-security.org/. Access 02/12/2011.

[2] IBM. As 400 series. http://www-03.ibm.com/systems/i/. Access 28/11/2011.

[3] IBM. Formal verification and testing technologies. https://www.research.ibm.com/haifa/projects/verification/Formal_Methods-Home/index.html. Access 28/11/2011.

[4] IBM. Ibm power. http://en.wikipedia.org/wiki/IBM_POWER. Access 28/11/2011.

[5] IBM. Ibm research. http://www.research.ibm.com/about/. Access 28/11/2011.

[6] IBM. International business machines corporation. www.ibm.com/uk/en/. Access 28/11/2011.

[7] IBM. Rulebase. https://www.research.ibm.com/haifa/projects/verification/RB_Homepage/. Access 28/11/2011.

[8] Daniel GEIST Shoham BEN-DAVID, Cindy EISNER and Yaron WOLFSTHAL. Model checking at ibm. http://www.cs.uwaterloo.ca/~s3bendav/Special-issue.pdf. Access 18/11/2011.

[9] Wikipedia. Ibm. http://en.wikipedia.org/wiki/IBM. Access 28/11/2011.

[10] Wikipedia. Ibm system i. en.wikipedia.org/wiki/IBM_System_i. Access 20/11/2011.

[11] Ilan Beer Cindy Eisner Daniel Geist Tamir Heyman Iris Reuveni Eran Rippel Irit Shitsevalov YaronWolfsthal Tali Yatzkar-Haham Yael Abarbanel-Vinov, Neta Aizenbud-Reshef. On the effective deployment of functional formal verification. http://www.cs.rice.edu/~vardi/comp607/verification.pdf. Access 22/11/2011.