Effective Bug Hunting with Spin and Modex

Gerard J. Holzmann[1] and Theo C. Ruys[2]

[1] NASA/JPL, Laboratory for Reliable Software.
http://spinroot.com/gerard/
[2] University of Twente, The Netherlands.
http://www.cs.utwente.nl/~ruys/

Abstract. This tutorial consists of two parts. In the first part we present an advanced overview of Spin [1, 4], and illustrate its practical application to logic model checking problems. In the second part of the tutorial we present an overview of a related tool called Modex [2, 3]. Modex can be used to extract Spin verification models directly from C source code. It supports the definition of user-defined abstractions, and cleverly exploits the capability in Spin version 4 to include embedded C code inside abstract verification models. We will show how to use Spin and Modex, separately and combined, in an effective way when searching for design errors in distributed software applications. Both Spin and Modex are written in ANSI-C and can freely be used on research projects.

The first part of this tutorial is meant for intermediate to advanced Spin users. The objective is to illustrate the effective application of both Promela and Spin, giving solutions to frequently encountered verification problems and discussing some useful recipes for the use of logic model checkers. We will also take a look 'under the hood' to briefly describe the architecture of Spin's verification engine, and then show how one can exploit this information in building Promela verification models that include embedded C code constructs.

The second part of the tutorial shows how Modex can be used to extract verification models from C code. This process relies on a user-definition of an abstraction table to guide the model extraction process. We will show how this methodology was first used for the exhaustive verification of a commercial telephone switch, developed at Bell Labs between 1998 and 2001. The verification procedure based on model extraction and model checking for multi-threaded code proved to be significantly more effective in its bug finding capabilities than the standard software testing process.

References

1. G. J. Holzmann. *The* Spin *Model Checker – Primer and Reference Manual.* Addison-Wesley, Boston, Massachusetts, USA, 2004.
2. G. J. Holzmann and M. H. Smith. An Automated Verification Method for Distributed Systems Software Based on Model Extraction. *IEEE Transactions on Software Engineering*, 28(4):364–377, April 2002.
3. Modex Homepage. URL: http://cm.bell-labs.com/cm/cs/what/modex/.
4. Spin Homepage. URL: http://spinroot.com/spin/.