State Space Explosion or: How To Fight An Uphill Battle

Markus A. Kuppe

Microsoft Research

Redmond

TLA$^+$ Community Meeting

Oxford Britain, 18 July 2018

Clarke - the father of model checking - lists scaling up model checking as one of the challenges that "*require major breakthroughs in order to become suciently practical for widespread use in industry*". While TLA$^+$ adoption rate has been increasing in recent years and several industrial success stories praise TLA$^+$ to be a useful addition to an engineer's tool-belt, it is still a niche on a global scale. And indeed it seems Clarke is right in that the absence of significant breakthroughs hinder large scale adoption. Engineers expect tools to be sufficiently powerful to check real-world models such as a consumer-producer problem with hundreds or thousands of processes. And engineers care very little about the Achilles heel of explicit state model checking: the state space explosion problem.

TLC - the TLA$^+$ explicit state model checker - is still far from and might never be able to check a consumer-producer problem for more than just a handful of processes. However, this appears to be an acceptable restriction if the model checker is capable of handling models large enough to exhibit interesting errors in a reasonable time.

In this tutorial we will explore the tricks and techniques available in TLA$^+$, TLC and the TLA Toolbox to squeeze out more performance to check models of interesting sizes despite the state space explosion problem. The tutorial will also shed light on what has been done under the hood so far to scale TLC to modern day hardware and what we are up to next to tackle Clarke's challenge.

This tutorials assumes previous knowledge of TLA$^+$, TLC and the TLA Toolbox. Participants are strongly encouraged to start and join a group discussion about the future roadmap of the TLC and TLA Toolbox development at the end of the tutorial.

References

[1] Edmund M. Clarke. The Birth of Model Checking. In Orna Grumberg and Helmut Veith, editors, *25 Years of Model Checking*, volume 5000, pages 1–26. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008. ISBN 978-3-540-69849-4 978-3-540-69850-0. URL `http://link.springer.com/10.1007/978-3-540-69850-0_1`. (document)