Aalto University
School of Science

Artem Yushkovskiy (student number 663230)
Aalto University, School of Science

A step towards the mathematically verified future

Espoo, June 2018 – The portability analysis and verification tool Porthos developed in 2017 at Aalto University has evolved from a prototype to an alpha-release version. As a continuation of the research project led by Assoc. Prof. Keijo Heljanko, the MS student Artem Yushkovskiy redesigned the architecture of the tool in order to make it easily extensible for supporting different programming languages, reliable and maintainable. The new tool can be used not only for research purposes, but also for analysing the portability of existing concurrent programs between different hardware architectures.

Performance vs reliability

Nowadays the progress is mostly concerned about increasing the speed of life by constructing computers that can operate faster and faster. On the contrary, one of the main questions that we should ask ourselves is how we can rely on machines, predict their behaviour and be sure about the result of their work. These issues are becoming particularly relevant for safety-critical systems, where an error can entail serious injury to people or even death. Thus, there exist numerous software verification techniques that can provide mathematically proved guarantees. Nonetheless, the last year's research has opened a large flaw in the general mathematical model of concurrent software systems, which makes the analysis inaccurate for most modern processors (such as x86, Power, etc.). This finding has commenced a new research field aimed to construct mathematical *memory model* of a processor architecture and verify programs with respect to this model. However, most modern tools that perform memory model-aware analysis are aimed at research of memory models itself, while few of them examine existing programs with respect to the hardware memory model.

Portability analysis

One of such tools is *Porthos*, which was prototyped in April 2017 by a group of researchers from Aalto University (Finland), TU Kaiserslautern (Germany), TU Braunschweig (Germany) and Fortiss GmbH (Germany). This tool is the first tool that analyses the *portability* of a program between two processor architectures, although it is able to analyse only simple programs written in the highly restricted C-like language. Therefore, in order to be able to process real-world C programs, it needed to be extended in order to acquire features of a full-scale compiler. The Master's thesis project by Artem Yushkovskiy completed in June 2018 aimed to investigate the directions of such an extension, redesign the tool and transform it from a proof-of-concept instrument to a usable analysis tool. During the work, the author implemented a C language interpretation engine supported by a knowledge base of functions that can serve as an instrument for customising the interpretation process.

New features

The key feature of the new tool is strict separation of its functional modules so that the architecture became transparent, extensible and testable. In addition to that, the author made some changes in the algorithm of the tool, that could be applied due to the new processing scheme. Although most of the changes do not influence the quality of analysis, some of them increase the detalisation of the analysing program model and therefore lead to more thorough analysis.

As the tool was almost completely redesigned, it received a new name *PorthosC*. Although still it supports only very basic C programs, it is designed to be highly extensible, therefore the extension of the support of C language is one of the main directions of the future work.