Bounded Model Checking of C++ Programs Based on the Qt Cross-Platform Framework (Journal-First Abstract)

Felipe R. Monteiro∗
Federal University of Amazonas
Manaus, Amazonas, Brazil

Lucas C. Cordeiro
University of Manchester
United Kingdom

Mário A. P. Garcia
Federal University of Amazonas
Manaus, Amazonas, Brazil

Eddie B. de Lima Filho
TPV Technology Ltd.
Manaus, Amazonas, Brazil

ABSTRACT
This work proposes an abstraction of the Qt framework, named as Qt Operational Model (QtOM), which is integrated into two different verification approaches: explicit-state model checking and symbolic (bounded) model checking. The proposed methodology is the first one to formally verify Qt-based applications, which has the potential to devise new directions for software verification of portable code. The full version of this paper is published in Software Testing, Verification and Reliability, on 02 March 2017 and it is available at https://doi.org/10.1002/stvr.1632.

CCS CONCEPTS
• General and reference → Verification; • Software and its engineering → Model checking; Software verification; Formal software verification;

KEYWORDS
Software Engineering, Qt Framework, Model Checking, Formal Verification, Verification in Industrial Practice

1 OVERVIEW
Technology companies, such as AMD, Intel and Amazon, increasingly invest effort and time to develop fast and cheap verification alternatives, in order to check for correctness in their systems and then reduce product recall rates. Among such alternatives, one of the most promising is the model checking approach; however, despite its advantages, there are many systems that could not be automatically verified, due to the restricted support of formal verifiers.

To tackle this problem, Monteiro et al. [4] propose a simplified version of the Qt framework, which is integrated into a model checker based on satisfiability modulo theories (SMT), known as the Efficient SMT-based Context-Bounded Model Checker (ESBMC) [2, 5], in order to verify actual Qt-based applications. Importantly, such an approach resulted in a success rate of 89% based on the developed benchmark test suite. Furthermore, the simplified version of the Qt framework, named as Qt Operational Model (QtOM), was also evaluated using other state-of-the-art verifiers for C++ programs. In fact, QtOM was combined with two different verification approaches during the experimental evaluation, i.e., explicit-state model checking and symbolic (bounded) model checking, which highlights its flexibility.

Contributions. Monteiro et al. [4] extend a previous published work by Garcia et al. [1] and Monteiro et al. [3]. QtOM was expanded, in order to include new features from the main Qt modules: QTCGI and QTCore. Indeed, the main contributions here are (i) the support for sequential and associative template-based containers, (ii) the integration of QtOM into the verification process of the state-of-the-art C++ verifiers DIVINE and LLBMC, and (iii) the verification of two Qt-based applications known as Locomaps and GeoMessage. Furthermore, the employed benchmark suite was extensively revised and expanded, now 13 times bigger than the previous work, and the performance of three SMT solvers (i.e., Z3, Yices, and Boolector) was evaluated, along with the proposed approach.

Availability of Data and Tools. The performed experiments are based on a set of publicly available benchmarks. All benchmarks, tools, and results, associated with the current evaluation, are available at http://esbmc.org/qtom.

REFERENCES

∗Corresponding author felipemonteiro@ufam.edu.br
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

AISE ’18, September 3–7, 2018, Montpellier, France
© 2018 Copyright held by the owner/author(s).
https://doi.org/10.1145/3238147.3241981