# A Bounded Verification Tool for Java

Stefan Koppier

April 8, 2019

# Introduction

We present a tool that allows bounded model checking of Java source code. The tool works a layer over JBMC, a bounded verification tool for Java bytecode, developed by Lucas Cordeiro et al. [1]. Built on the CPROVER framework, which also drives the industrial strength bounded model checking tool CBMC.

We were inspired to develop this tool by CRUST [2]. CRUST is a bounded model checking tool to find memory problems in Rust source code, and we wanted a similar infrastructure to do further research on bounded model checking of Java source code.

The advantage of using this tool, over using JBMC itself is that we provide an interface for Java source code, instead of Java bytecode.

## Features

## Comparison between JBMC

## An overview of the tool

# Contents

# Chapter 1

# Lexing and Parsing

# Chapter 2

# Analysis

# Chapter 3

# Compilation

# Chapter 4

# Verification

# Chapter 5

# CProver

## 5.1 Properties

| | |
|---|---|
| array bounds | test |
| pointer | test |
| division by zero | test |
| arithmetic over- and underflow | test |
| shift greater than bit-width | test |
| floating-point for +/-Inf | test |
| floating-point for NaN | test |
| user assertions | test |

# Bibliography

[1] Lucas Cordeiro, Pascal Kesseli, Daniel Kroening, Peter Schrammel, and Marek Trtik. JBMC: A bounded model checking tool for verifying Java bytecode. volume 10981 of *LNCS*, pages 183–190. Springer, 2018.

[2] John Toman, Stuart Pernsteiner, and Emina Torlak. Crust: A bounded verifier for rust (n). In *Automated Software Engineering (ASE), 2015 30th IEEE/ACM International Conference on*, pages 75–80. IEEE, 2015.