JBMC: A Bounded Model Checking Tool for Verifying Java Bytecode

Lucas Cordeiro
Daniel Kroening
Peter Schrammel
JVM vs JBMC

Java bytecode program

Java runtime +native+OS

JVM

execution
**JVM vs JBMC**

- **Java bytecode program**
- **Java operational model**
- **bounds**

- safe wrt bounds
- unsafe + trace
How does it work?

Strengths and Weaknesses

What's next

CBMC

C program with properties

C built-in library

bounds

parse C code

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

Clarke, Kroening & Lerda, TACAS'04

C program with properties

C built-in library

bounds

parse C code

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

Clarke, Kroening & Lerda, TACAS'04
How does it work?

- **C program with properties**
- **C built-in library**
- **bounds**

**CBMC**

1. **parse C code**
2. **convert to GOTO**
3. **static analysis**
4. **symbolic execution**
5. **SMT solver**

- **safe wrt bounds**
- **unsafe + trace**

**Strengths and Weaknesses**

- **assert runtime errors**

**What's next**

- Clarke, Kroening & Lerda, TACAS’04
How does it work? Strengths and Weaknesses What's next

**CBMC**

- C program with properties
- C built-in library
- bounds

**CBMC**

- parse C code
  - convert to GOTO
    - static analysis
      - symbolic execution
        - SMT solver
          - safe wrt bounds
          - unsafe + trace

- assert runtime errors
- stdlib stdio pthreads ...
CBMC

C program with properties

parse C code

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

C built-in library

bounds

assert runtime errors

unwind

stdlib stdio pthreads ...

How does it work?

Strengths and Weaknesses

What's next

CBMC

C program with properties

parse C code

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

C built-in library

bounds

assert runtime errors

unwind

stdlib stdio pthreads ...

CBMC

Clarke, Kroening & Lerda, TACAS’04
**CBMC**

**How does it work?**

- C program with properties
- C built-in library
- bounds

**Strengths and Weaknesses**

- parse C code
- convert to GOTO
- static analysis
- symbolic execution
- SMT solver

**What's next**

- safe wrt bounds
- unsafe + trace
CBMC

How does it work?

- C program with properties
- C built-in library
- bounds

CBMC

assert runtime errors

multi-path

parse C code

convert to GOTO

static analysis

symbolic execution

SMT solver

SAFE wrt bounds

unsafe + trace

unwind

stdlib
stdio
pthreads ...

QF_ABVFP

Clark, Kroening & Lerda, TACAS’04
How does it work?

Strengths and Weaknesses

What's next

JBMC

Java program with properties → Java operational model → bounds

parse bytecode → convert to GOTO → static analysis → symbolic execution → SMT solver

safe wrt bounds

unsafe + trace

JBMC

Cordeiro et al CAV’18
How does it work?

Strengths and Weaknesses

What's next

JBMC

Java program with properties

Java operational model

bounds

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

assert runtime exceptions uncaught exceptions

JBMC

Cordeiro et al CAV’18
How does it work?

Strengths and Weaknesses

What's next

JBMC

Java program with properties

Java operational model

bounds

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

assert runtime exceptions uncaught exceptions

data structures, ...
**How does it work?**

1. **Java program with properties**
2. **Java operational model**
3. **bounds**

**Steps:**

- **parse bytecode**
- **convert to GOTO**
- **static analysis**
- **symbolic execution**
- **SMT solver**

**Results:**

- **safe wrt bounds**
- **unsafe + trace**

**Further challenges:**

- concurrency
- lambdas
- reflection, . . .
- polymorphism,
- exceptions, . . .
- multi-path

**Advantages:**

- assert
- runtime exceptions
- uncaught exceptions

**References:**

- JBMC
- Cordeiro et al CAV'18

**Other techniques:**

- QF ABVFP+Strings (Li & Ghosh, HVC'13)
How does it work?

JBMC

Java program with properties

Java operational model

bounds

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

assert

runtime exceptions

uncaught exceptions

unwind

data structures, ...

polymorphism, exceptions, ...

Cordeiro et al CAV’18

Further challenges

concurrency

lambdas

reflection, ...

Strengths and Weaknesses

What's next
How does it work? Strengths and Weaknesses What's next

Java program with properties → parse bytecode → convert to GOTO → static analysis → symbolic execution → SMT solver → safe wrt bounds

Java operational model

bounds

assert
runtime exceptions
uncaught exceptions

multi-path

unwind

data structures, ...
polymorphism, exceptions, ...

JBMC

JBMC Cordeiro et al CAV’18

QF ABVFP+Strings (Li & Ghosh, HVC’13)

Further challenges concurrency lambdas reflection, ...
How does it work?

**JBMC**

- **Java program with properties**
- **Java operational model**
- **bounds**

**How it works**

1. **parse bytecode**
2. **convert to GOTO**
3. **static analysis**
4. **symbolic execution**
5. **SMT solver**
   - **safe wrt bounds**
   - **unsafe + trace**

**Further challenges**

- concurrency
- lambdas
- reflection, . . .

**Strengths and Weaknesses**

- **assert**
- runtime exceptions
- uncaught exceptions

- **multi-path**

**What's next**

**Cordeiro et al CAV’18**

- **unwind**
  - data structures, . . .
  - polymorphism, exceptions, . . .

**QF_ABVFP+Strings**

(Li & Ghosh, HVC’13)
How does it work?

Strengths and Weaknesses

Cordeiro et al CAV’18

JBMC

Java program with properties

Java operational model

bounds

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

Further challenges

- concurrency
- lambdas
- reflection, ...

JBMC

assert

runtime exceptions

uncaught exceptions

unwind

data structures, ...

polymorphism, exceptions, ...

multi-path

QF_ABVFP+Strings

(Li & Ghosh, HVC’13)

unsafe + trace

What's next
SV-COMP 2019 Results
What’s next

JBMC:
- Concurrency support
- Witness output

SV-COMP 2020:
- Witness checker
- More and better benchmarks

www.cprover.org/jbmc