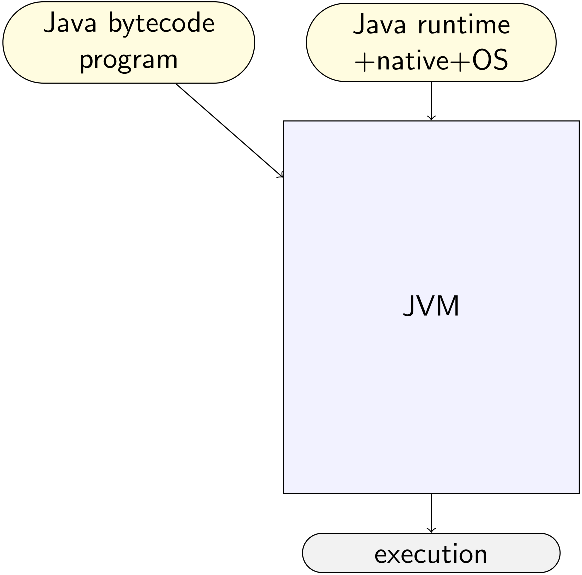
JBMC: A Bounded Model Checking Tool for Verifying Java Bytecode

Lucas Cordeiro
Daniel Kroening
Peter Schrammel

The University of Manchester
University of Oxford
University of Sussex
diffblue AI for Code

TACAS / SV-COMP 2023

JVM vs JBMC



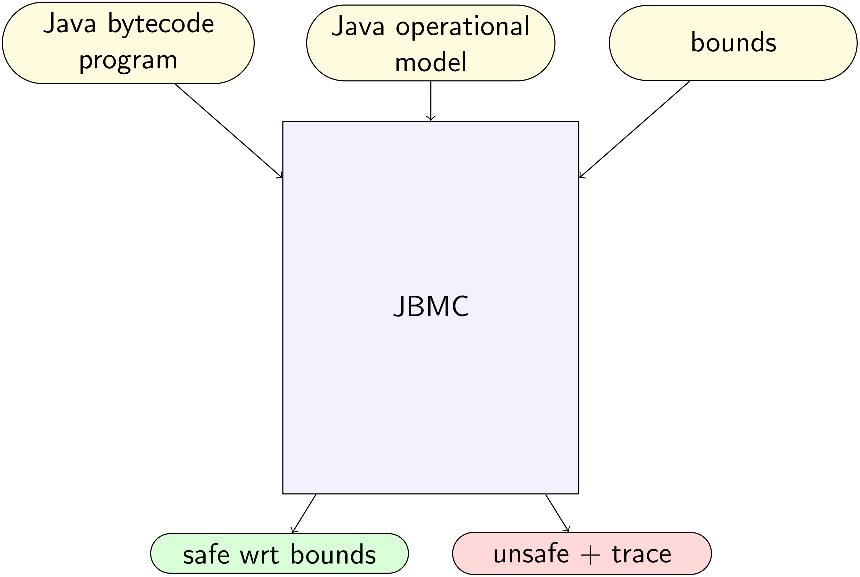
Java bytecode program

Java runtime +native+OS

JVM

execution

JVM vs JBMC



Java bytecode program

Java operational model

bounds

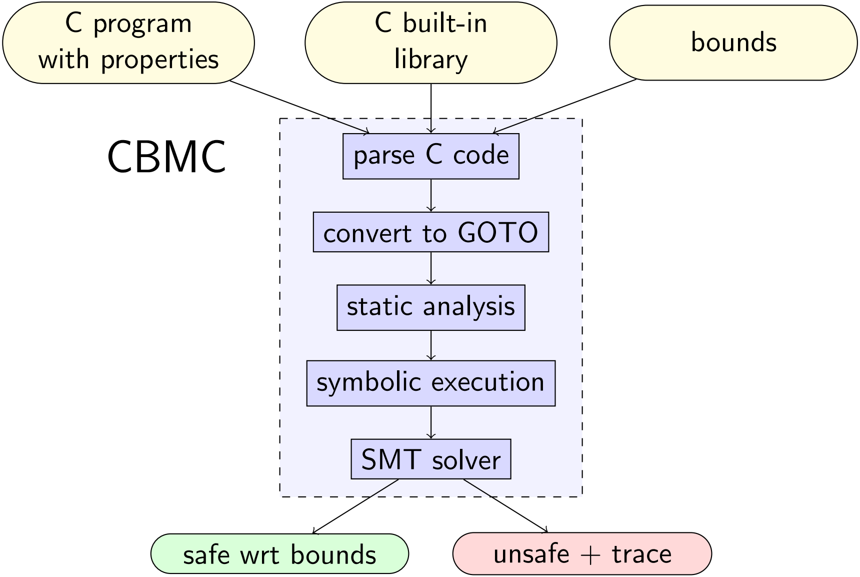
JBMC

safe wrt bounds

unsafe + trace

CBMC

Clarke, Kroening & Lerda, TACAS'04



C program with properties

C built-in library

bounds

CBMC

parse C code

convert to GOTO

static analysis

symbolic execution

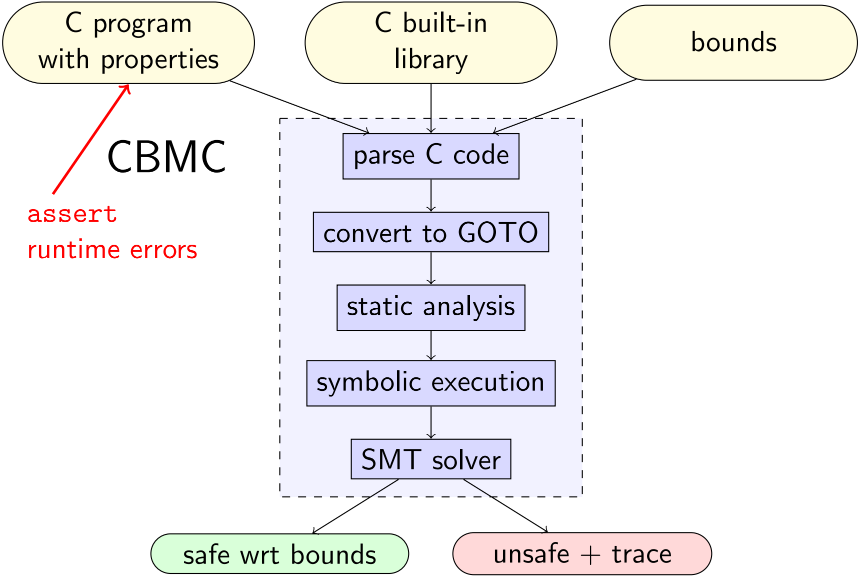
SMT solver

safe wrt bounds

unsafe + trace

CBMC

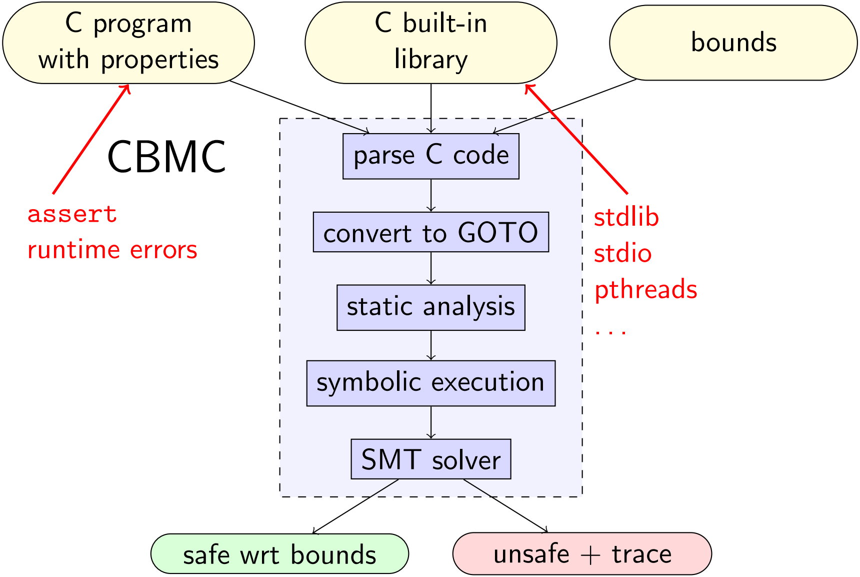
Clarke, Kroening & Lerda, TACAS'04


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

CBMC

Clarke, Kroening & Lerda, TACAS'04



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

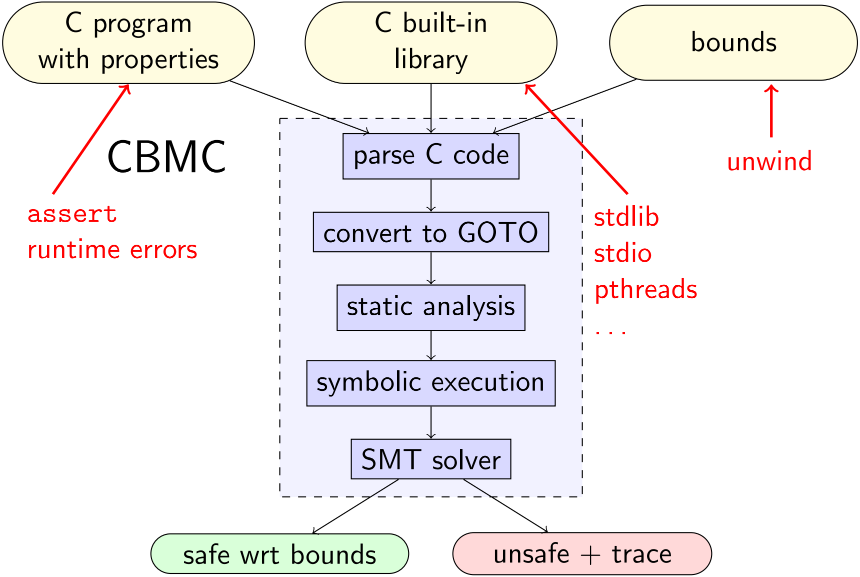
stdio

pthreads

...

CBMC

Clarke, Kroening & Lerda, TACAS'04



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

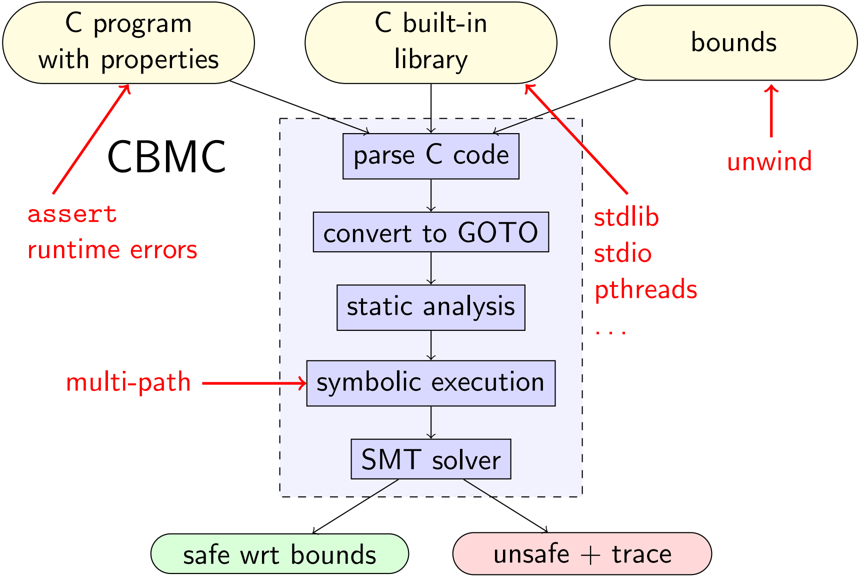
pthreads

...

unwind

CBMC

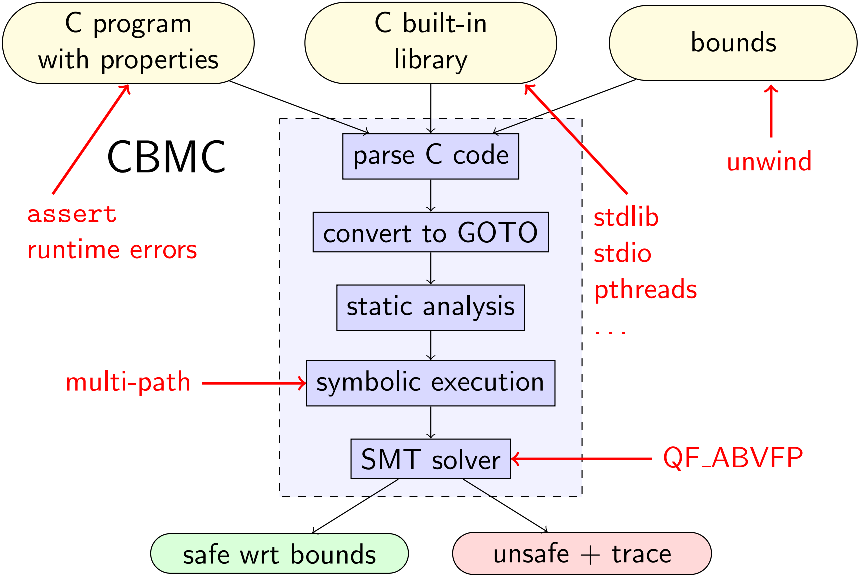
Clarke, Kroening & Lerda, TACAS'04



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
multi-path
stdlib
stdio
pthreads
. . .
unwind

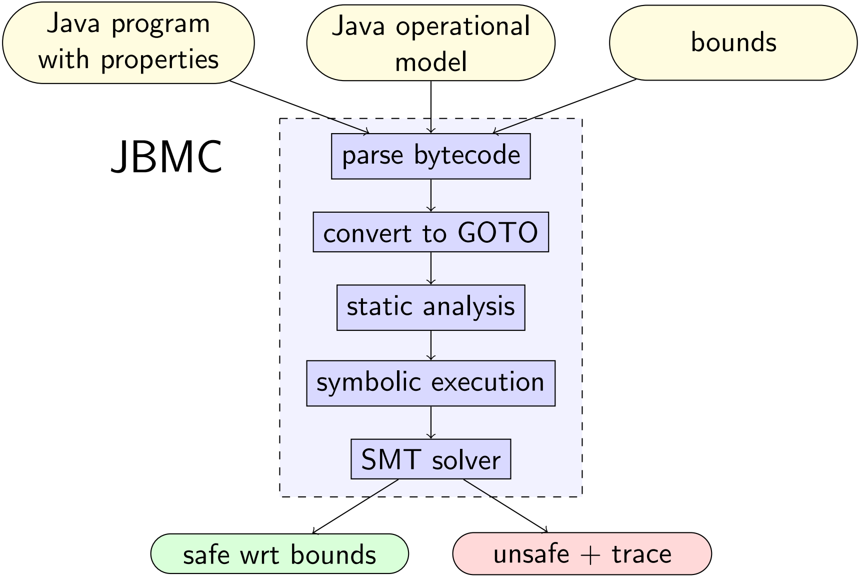
CBMC

Clarke, Kroening & Lerda, TACAS'04


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
...
unwind
multi-path
QF_ABVFP

JBMC

Cordeiro et al CAV'18



Java program with properties

Java operational model

bounds

JBMC

parse bytecode

convert to GOTO

static analysis

symbolic execution

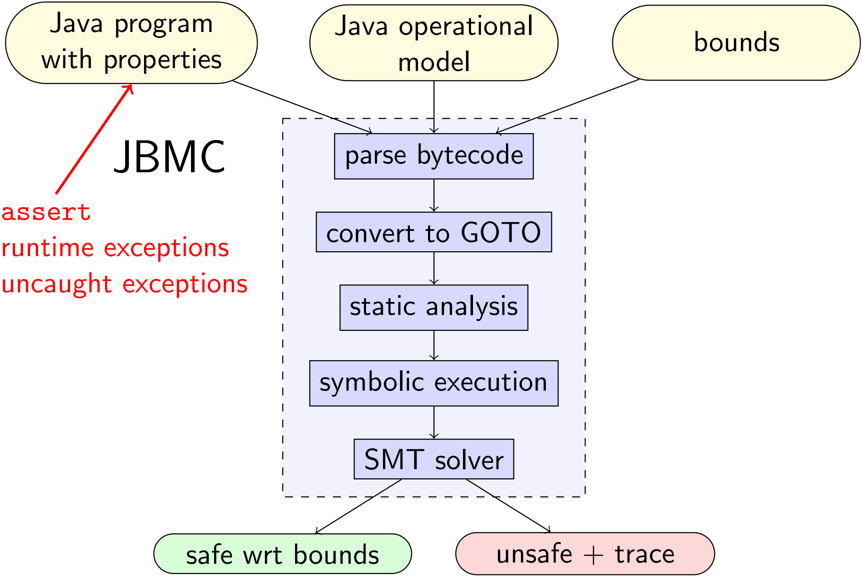
SMT solver

safe wrt bounds

unsafe + trace

JBMC

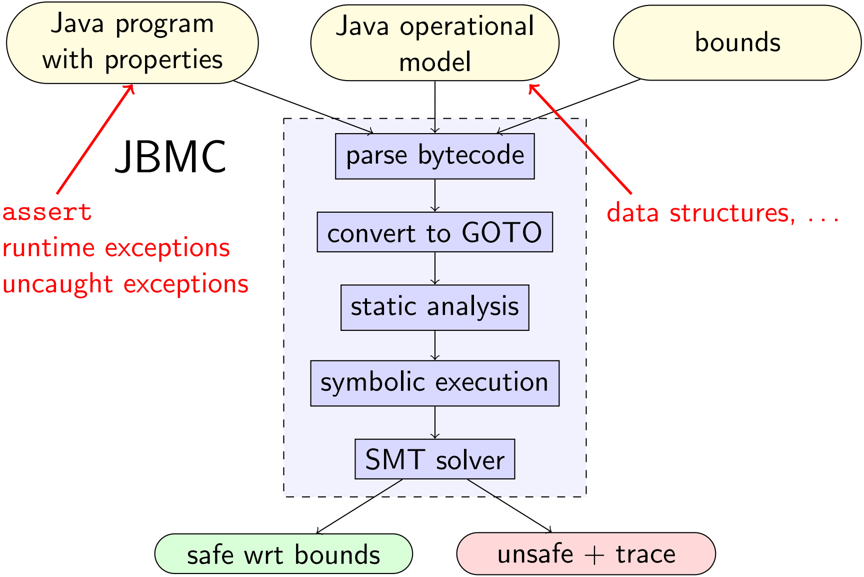
Cordeiro et al CAV'18


Java program with properties
Java operational model
bounds
JBMC
parse bytecode
convert to GOTO
static analysis
symbolic execution
SMT solver
safe wrt bounds
unsafe + trace

`assert`
runtime exceptions
uncaught exceptions

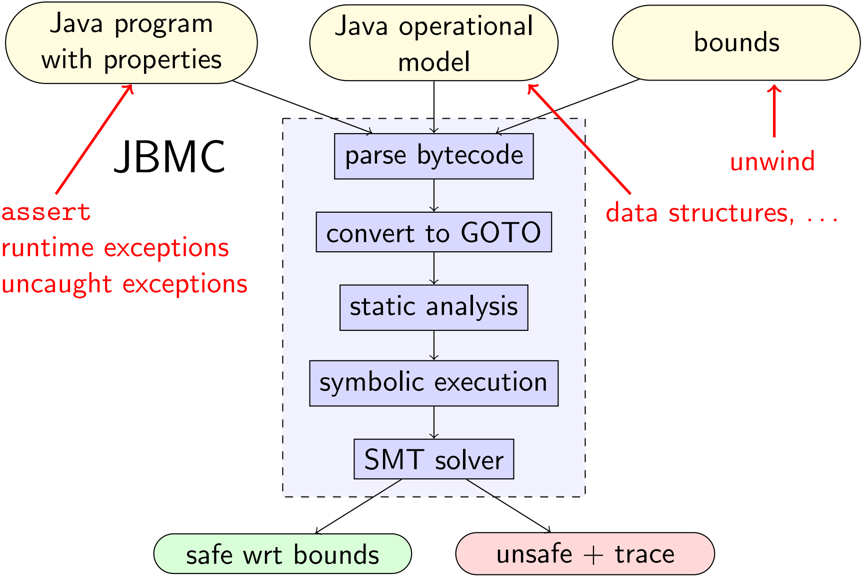
JBMC

Cordeiro et al CAV'18


Java program with properties
Java operational model
bounds
JBMC
parse bytecode
convert to GOTO
static analysis
symbolic execution
SMT solver
safe wrt bounds
unsafe + trace
`assert`
runtime exceptions
uncaught exceptions
data structures, ...

JBMC

Cordeiro et al CAV'18


Java program with properties
Java operational model
bounds
JBMC
parse bytecode
convert to GOTO
static analysis
symbolic execution
SMT solver
safe wrt bounds
unsafe + trace

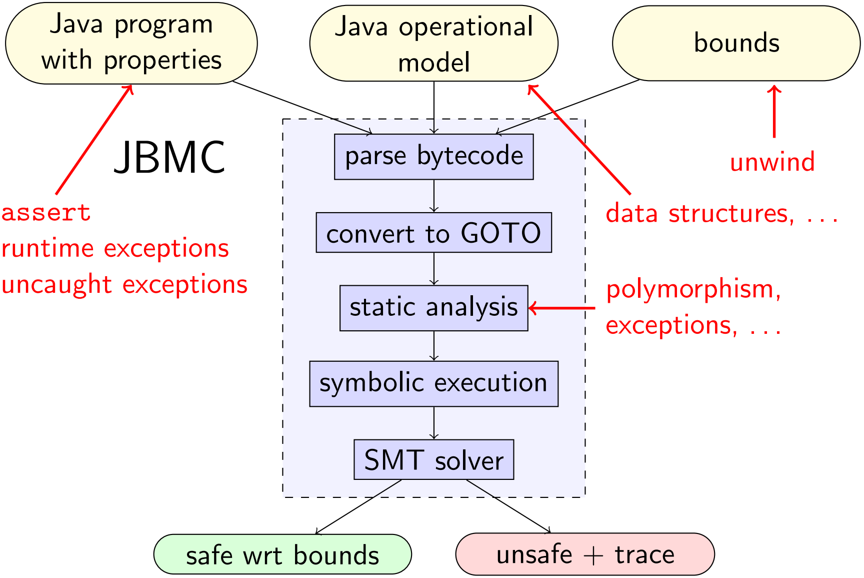
`assert`
runtime exceptions
uncaught exceptions

data structures, ...

unwind

JBMC

Cordeiro et al CAV'18


Java program with properties

Java operational model

bounds

JBMC

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

`assert`
runtime exceptions
uncaught exceptions

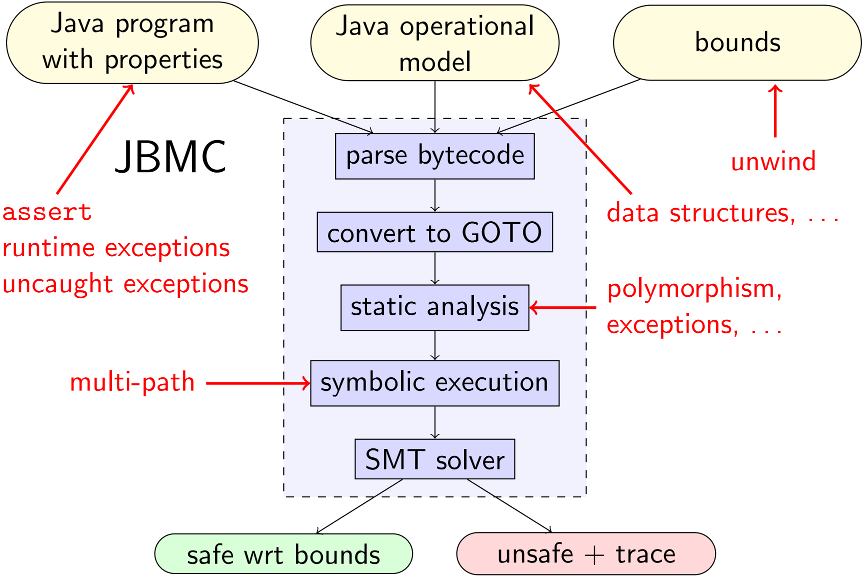
data structures, ...

unwind

polymorphism, exceptions, ...

JBMC

Cordeiro et al CAV'18



Java program with properties

Java operational model

bounds

JBMC

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

`assert`
runtime exceptions
uncaught exceptions

unwind

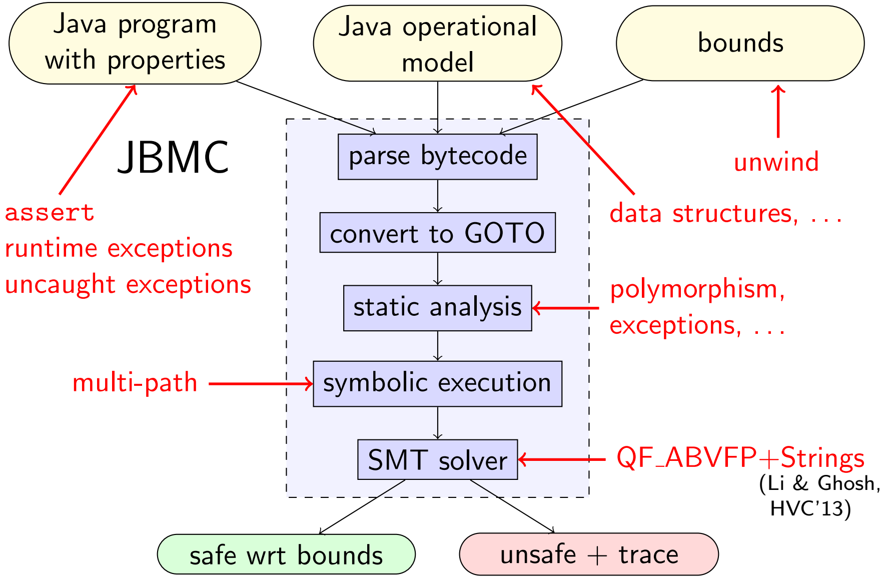
data structures, ...

polymorphism,
exceptions, ...

multi-path

JBMC

Cordeiro et al CAV'18



Java program with properties

Java operational model

bounds

JBMC

parse bytecode

convert to GOTO

static analysis

symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

`assert`

runtime exceptions

uncaught exceptions

unwind

data structures, ...

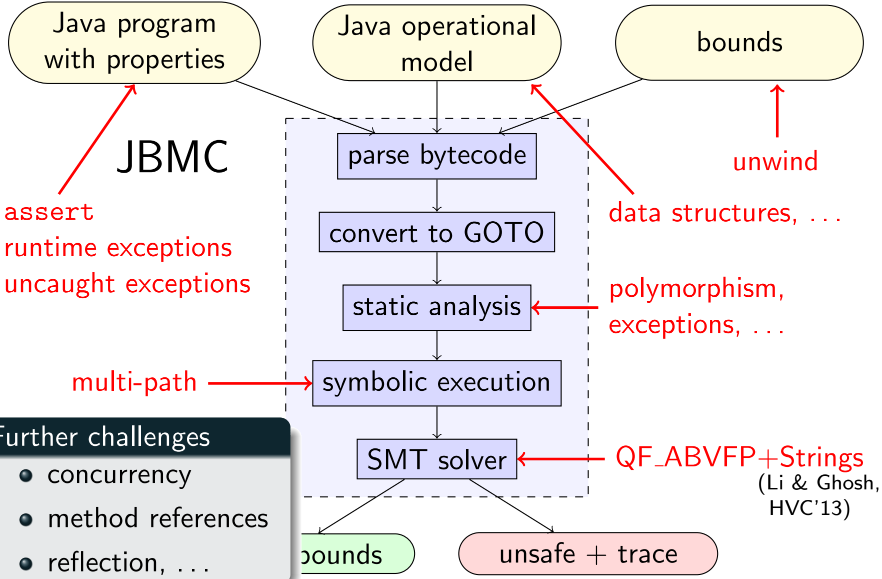
polymorphism, exceptions, ...

multi-path

QF_ABVFP+Strings (Li & Ghosh, HVC'13)

JBMC

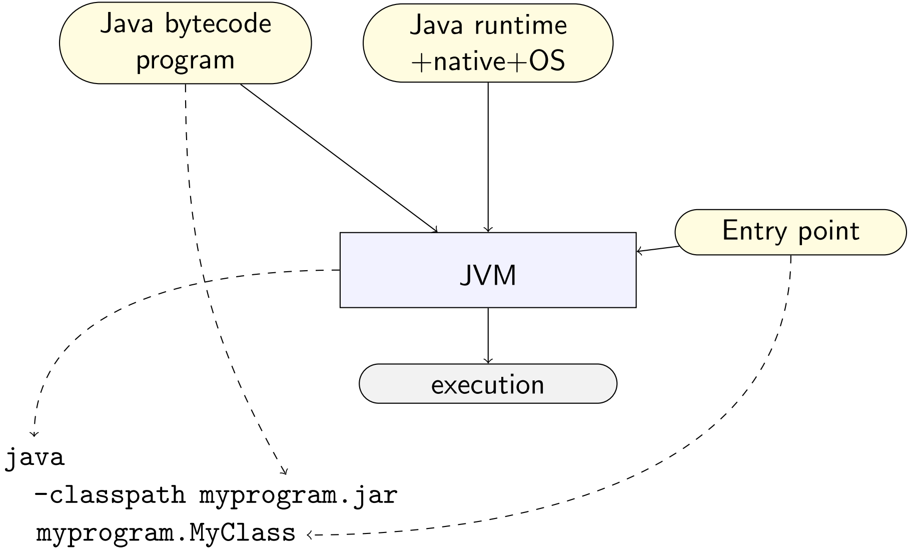
Cordeiro et al CAV'18


Java program with properties
Java operational model
bounds
JBMC
parse bytecode
convert to GOTO
static analysis
symbolic execution
SMT solver
ounds
unsafe + trace
assert
runtime exceptions
uncaught exceptions
data structures, . . .
unwind
polymorphism,
exceptions, . . .
multi-path
QF_ABVFP+Strings
(Li & Ghosh, HVC'13)

Further challenges

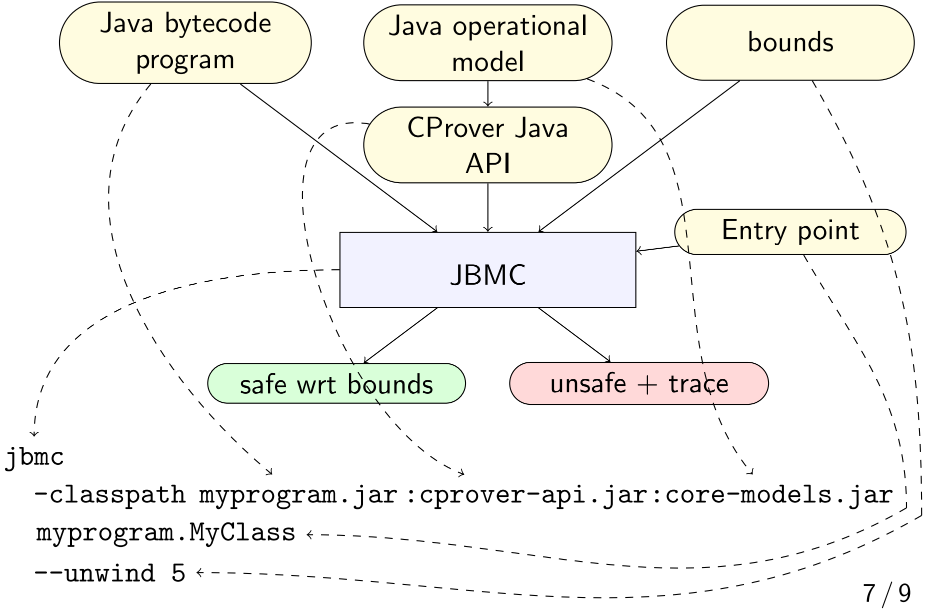
- concurrency
- method references
- reflection, . . .

Usage


Java bytecode program
Java runtime +native+OS
Entry point
JVM
execution

```
java
  -classpath myprogram.jar
  myprogram.MyClass
```

Usage



Java bytecode program

Java operational model

bounds

CProver Java API

Entry point

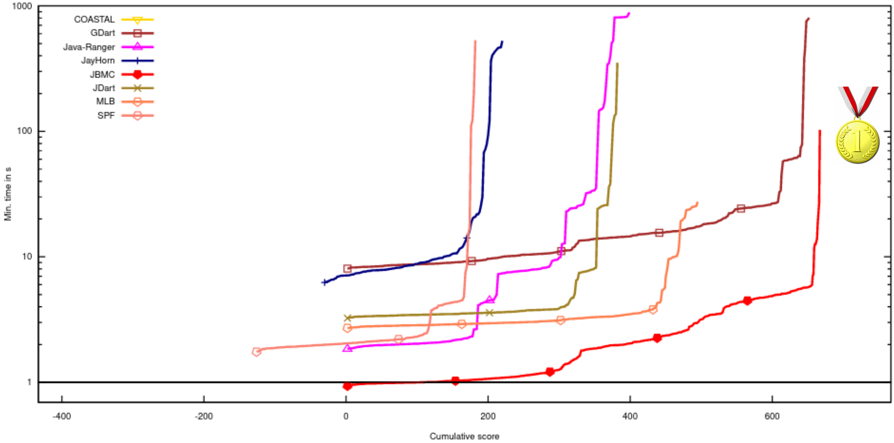
JBMC

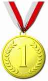
safe wrt bounds

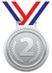
unsafe + trace

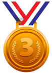
```
jbmc
  -classpath myprogram.jar:cprover-api.jar:core-models.jar
  myprogram.MyClass
  --unwind 5
```

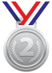
SV-COMP 2023 Results

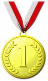


2019 

2020 

2021 

2022 

2023 

What's next

JBMC:

- Improved dynamic analysis
- Improved witness output

SV-COMP Java track:

- More and better benchmarks
- RuntimeException category
- Correctness witness checking

`https://github.com/diffblue/cbmc/tree/develop/jbmc`