JBMC: A Bounded Model Checking Tool for Verifying Java Bytecode

Lucas Cordeiro
Pascal Kesseli
Daniel Kroening
Peter Schrammel
Marek Trtik

Computer Aided Verification 2018

Why?

Java and JVM languages:

- Most widely used
- Established software development culture

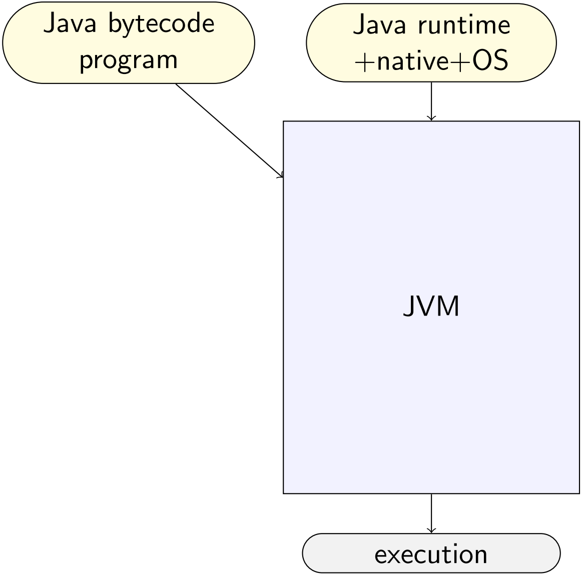
Only few model checking tools available:

- Symbolic JPF (Anand et al, TACAS'07)
- JayHorn (Kahsai et al, CAV'16)

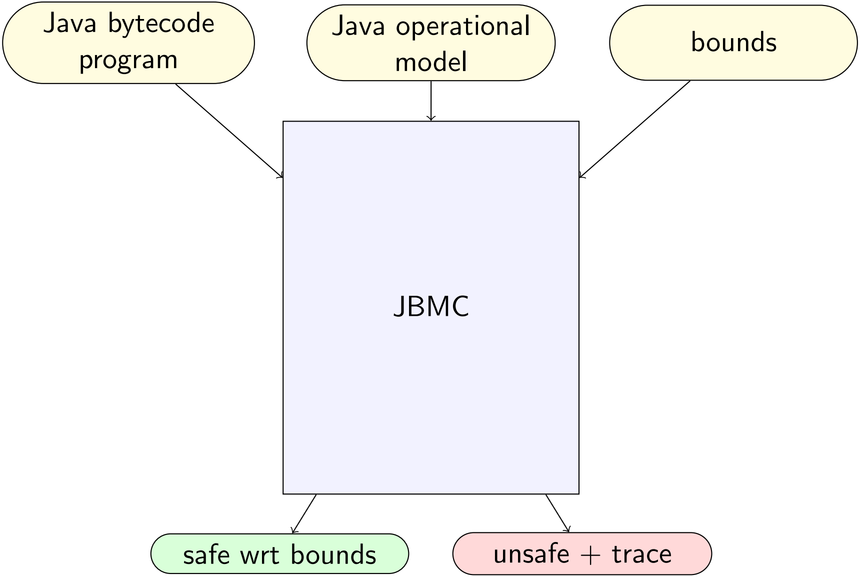
Many applications of BMC:

- Bug finding
- Program synthesis
- Test generation
- . . .

JVM vs JBMC

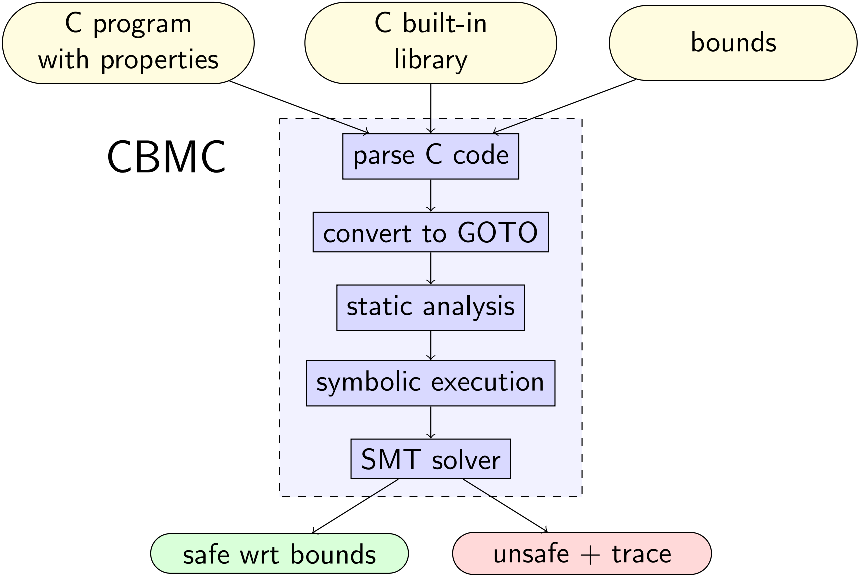

Java bytecode program
Java runtime +native+OS
JVM
execution

JVM vs JBMC


Java bytecode program
Java operational model
bounds
JBMC
safe wrt bounds
unsafe + trace

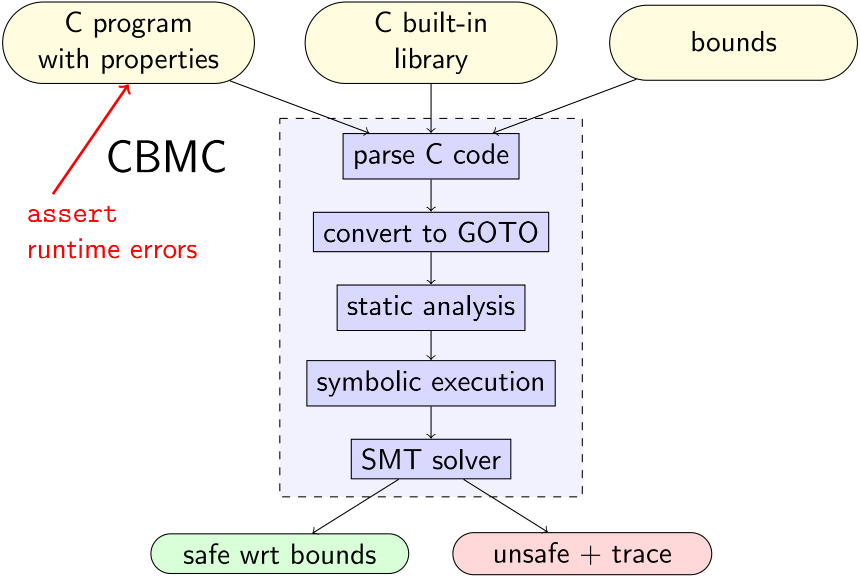
CBMC

Clarke, Kroening & Lerda, TACAS'04



CBMC

Clarke, Kroening & Lerda, TACAS'04



C program with properties

C built-in library

bounds

CBMC

assert

runtime errors

parse C code

convert to GOTO

static analysis

symbolic execution

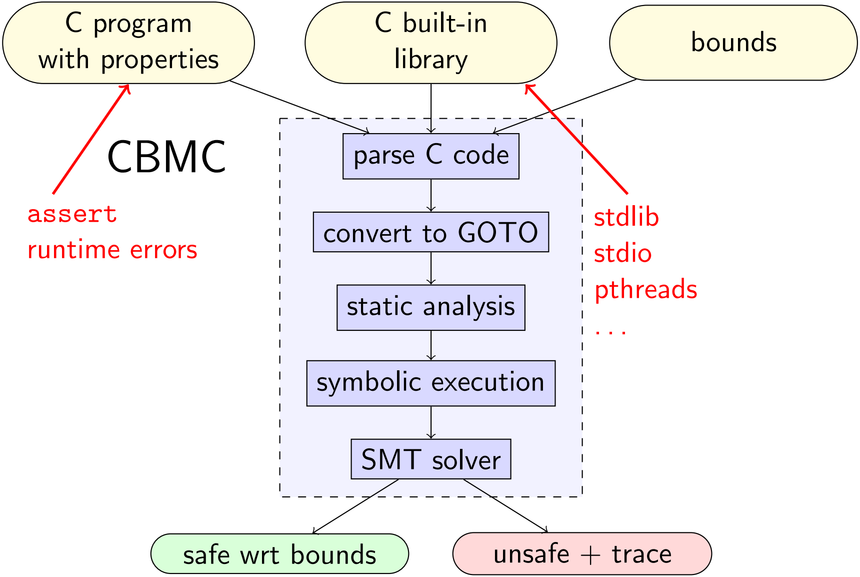
SMT solver

safe wrt bounds

unsafe + trace

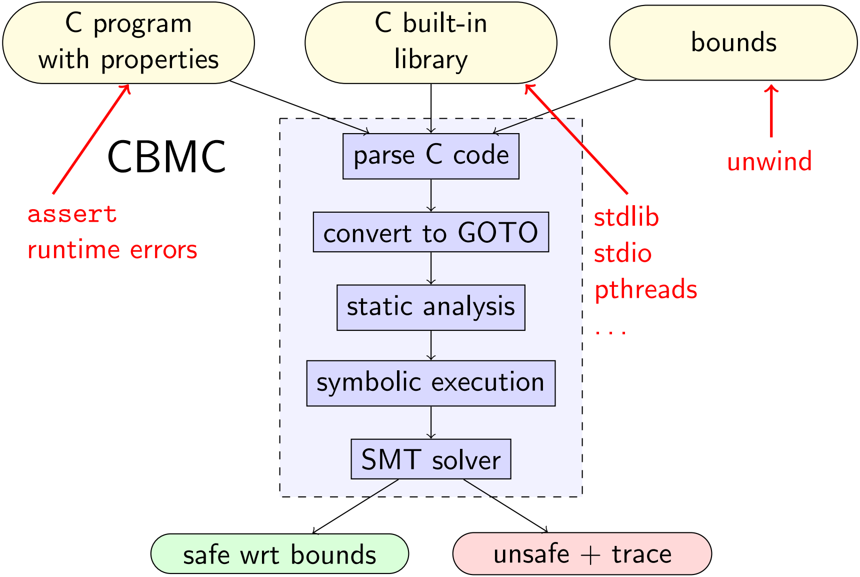
CBMC

Clarke, Kroening & Lerda, TACAS'04



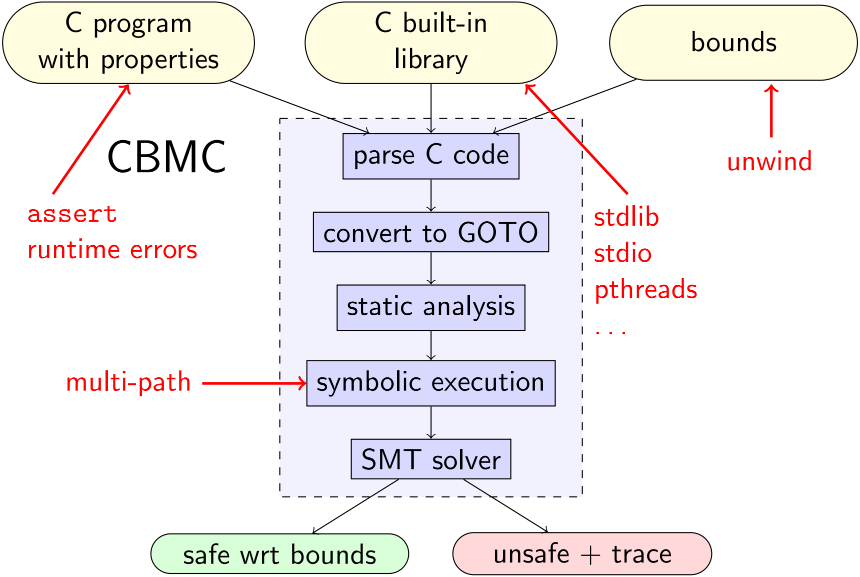
CBMC

Clarke, Kroening & Lerda, TACAS'04



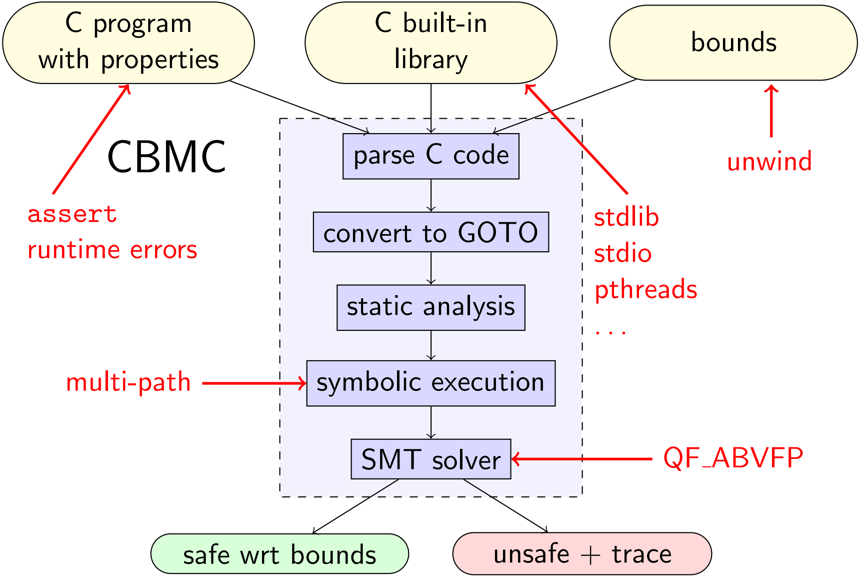
CBMC

Clarke, Kroening & Lerda, TACAS'04

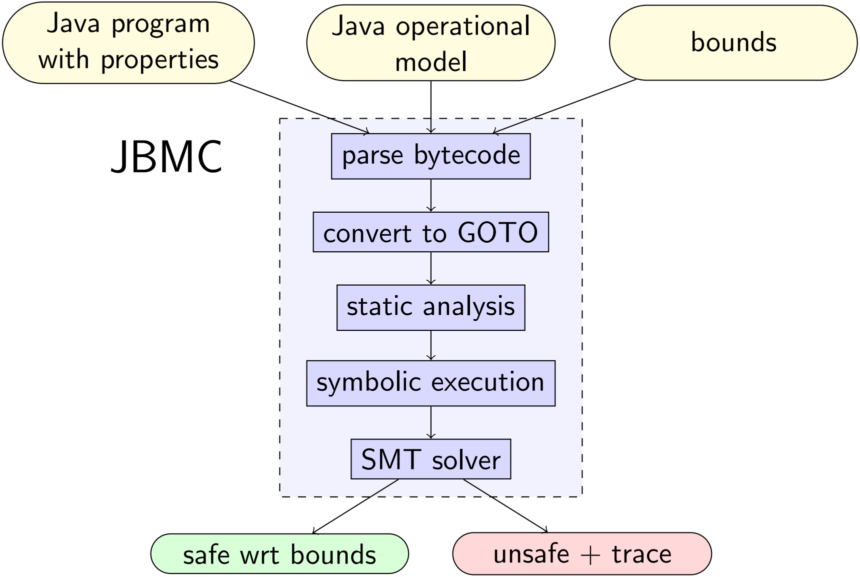


CBMC

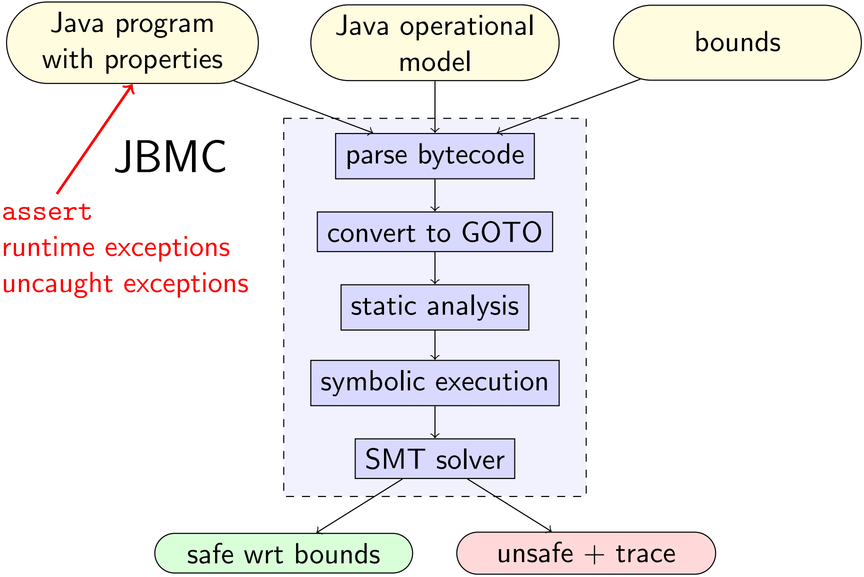
Clarke, Kroening & Lerda, TACAS'04



JBMC


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



Java program with properties

Java operational model

bounds

JBMC

assert

runtime exceptions

uncaught exceptions

parse bytecode

convert to GOTO

static analysis

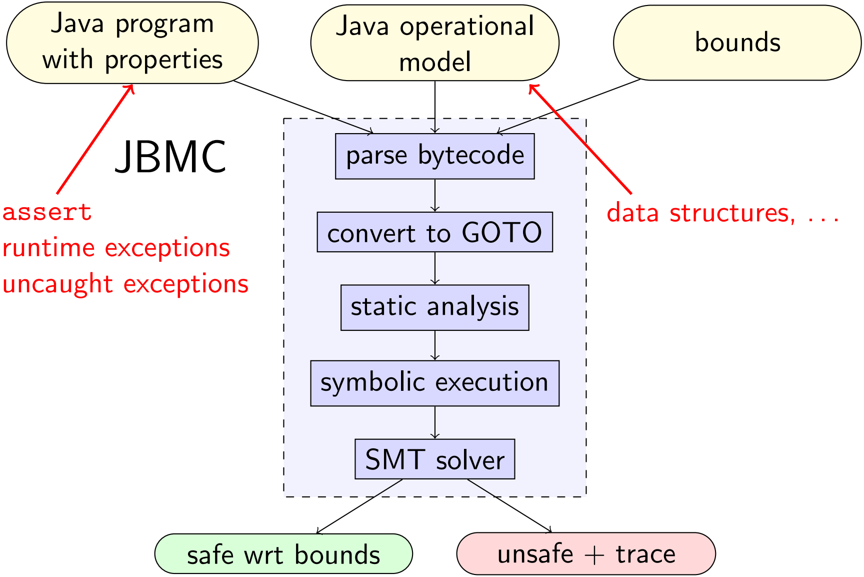
symbolic execution

SMT solver

safe wrt bounds

unsafe + trace

JBMC



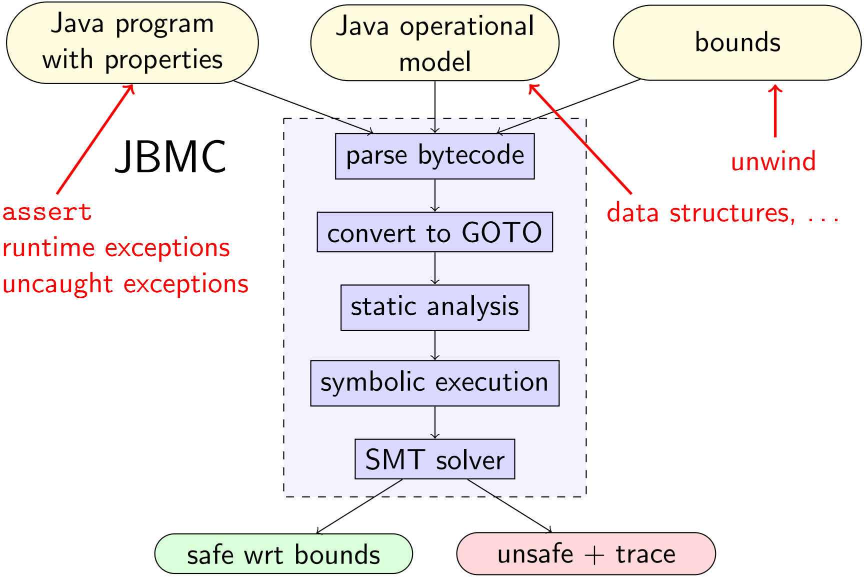
`assert`

runtime exceptions

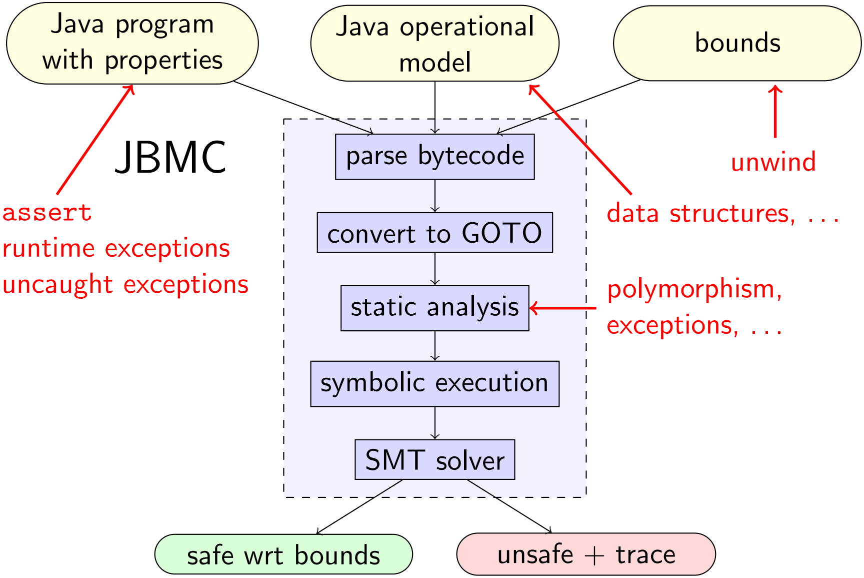
uncaught exceptions

data structures, . . .

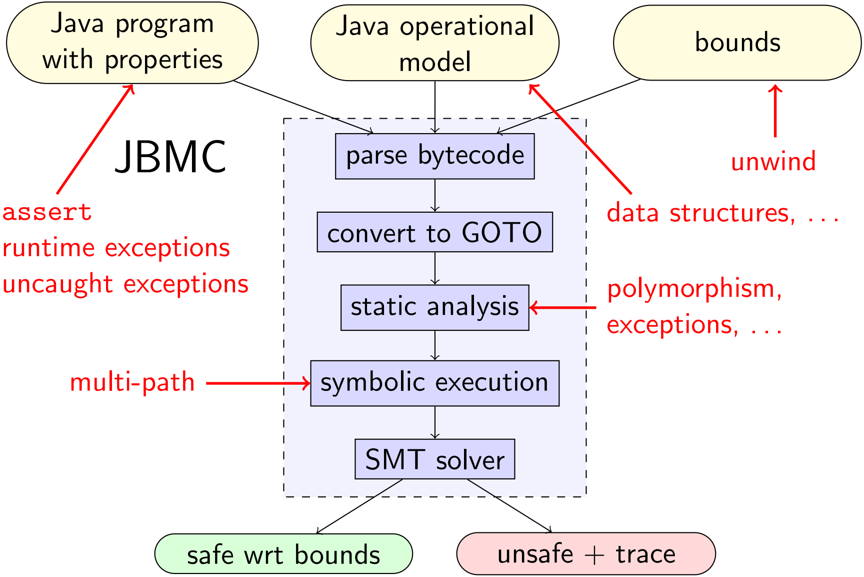
JBMC


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

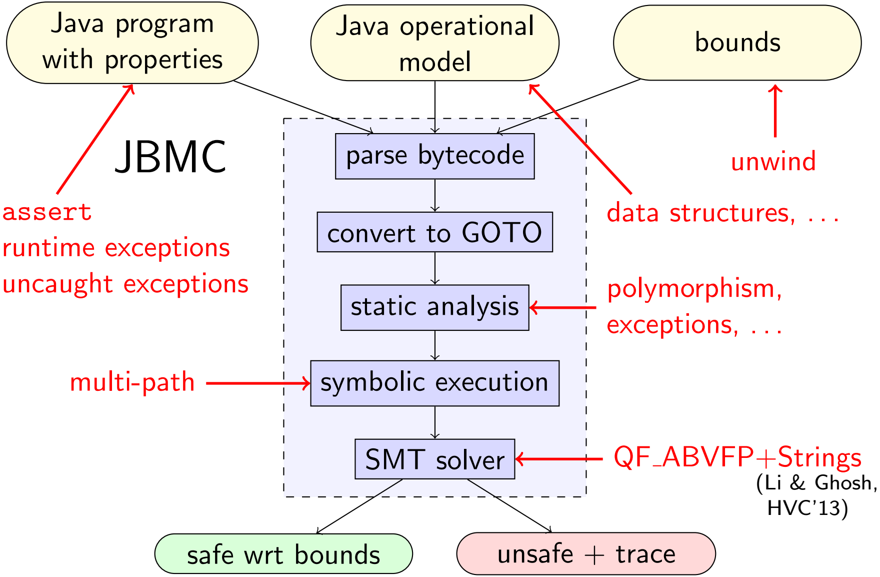
JBMC


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, . . .

JBMC

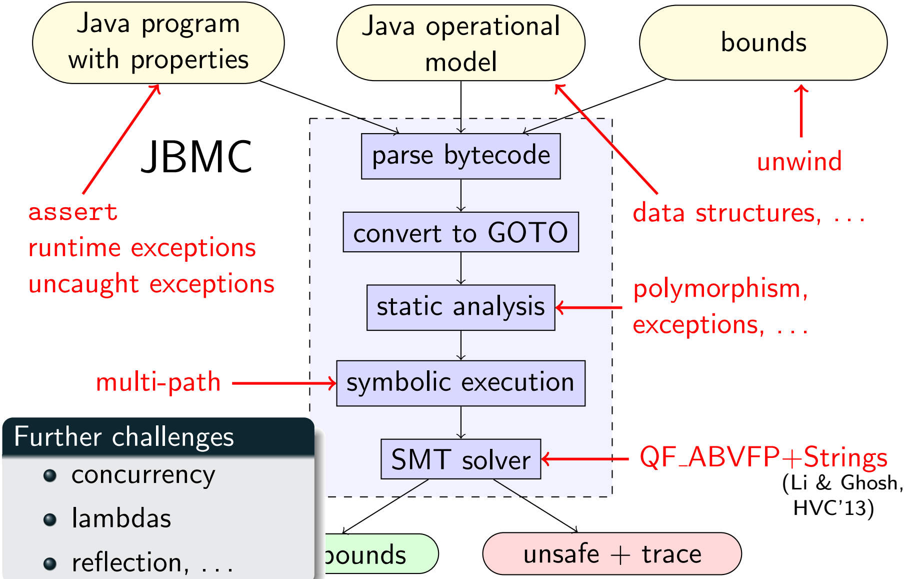

Java program with properties
Java operational model
bounds
JBMC
parse bytecode
convert to GOTO
static analysis
symbolic execution
SMT solver
safe wrt bounds
unsafe + trace
assert
runtime exceptions
uncaught exceptions
unwind
data structures, . . .
polymorphism,
exceptions, . . .
multi-path

JBMC



(Li & Ghosh, HVC'13)

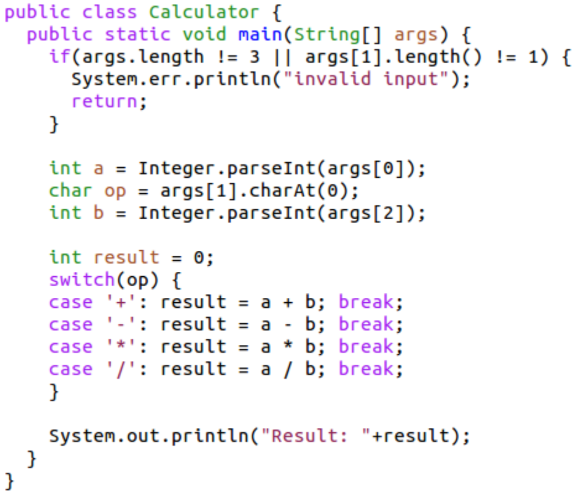
JBMC



Further challenges

- concurrency
- lambdas
- reflection, . . .

JBMC in Action

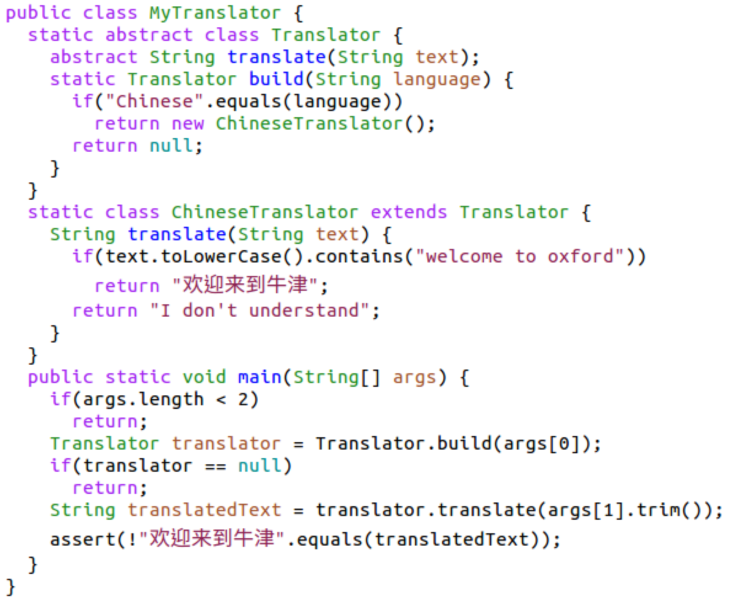


```
public class Calculator {
  public static void main(String[] args) {
    if(args.length != 3 || args[1].length() != 1) {
      System.err.println("invalid input");
      return;
    }

    int a = Integer.parseInt(args[0]);
    char op = args[1].charAt(0);
    int b = Integer.parseInt(args[2]);

    int result = 0;
    switch(op) {
    case '+': result = a + b; break;
    case '-': result = a - b; break;
    case '*': result = a * b; break;
    case '/': result = a / b; break;
    }

    System.out.println("Result: "+result);
  }
}
```

JBMC in Action

```
$ jbmc Calculator.class --classpath core-models.jar:. --trace
    --throw-runtime-exceptions

...
Runtime decision procedure: 0.980s
...
dynamic_object4={ ’-’, ’0’, ’4’ } // args[0].data
...
dynamic_object6={ ’/’ }           // args[1].data
...
dynamic_object8={ ’0’ }           // args[2].data
...
Calculator.java line 17 function Calculator.main
dynamic_object36={... .@class_identifier="java.lang.ArithmeticException" ...}
...
uncaught_exception=&dynamic_object36

Violated property:
  file Calculator.java line 3 function Calculator.main
  no uncaught exception
  uncaught_exception == null
```

JBMC in Action

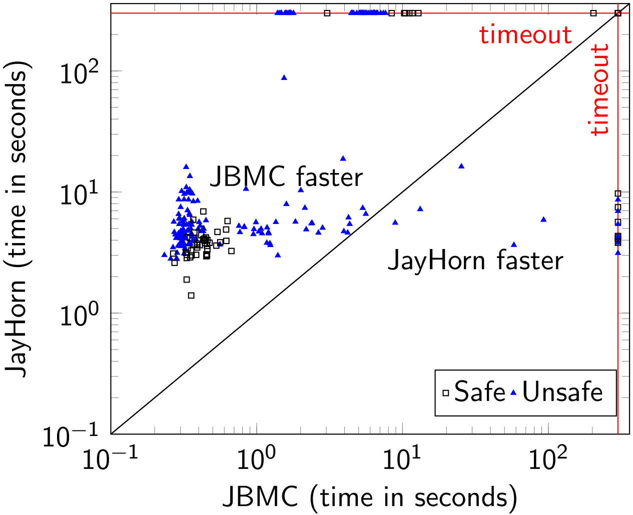


```java
public class MyTranslator {
  static abstract class Translator {
    abstract String translate(String text);
    static Translator build(String language) {
      if("Chinese".equals(language))
        return new ChineseTranslator();
      return null;
    }
  }
  static class ChineseTranslator extends Translator {
    String translate(String text) {
      if(text.toLowerCase().contains("welcome to oxford"))
        return "欢迎来到牛津";
      return "I don't understand";
    }
  }
  public static void main(String[] args) {
    if(args.length < 2)
      return;
    Translator translator = Translator.build(args[0]);
    if(translator == null)
      return;
    String translatedText = translator.translate(args[1].trim());
    assert(!"欢迎来到牛津".equals(translatedText));
  }
}
```

JBMC in Action

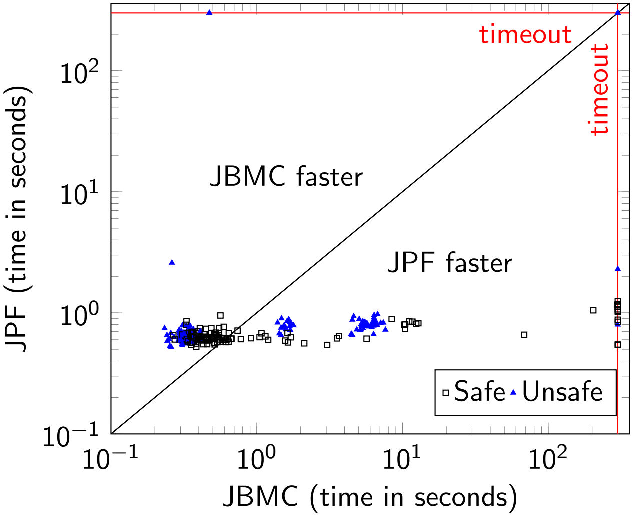
```
$ jbmc MyTranslator.class --classpath core-models.jar:. --trace
    --max-nondet-string-length 50

...
Runtime decision procedure: 0.786s
...
dynamic_object4={ ’C’, ’h’, ’i’, ’n’, ’e’, ’s’, ’e’ } // args[0].data
...
dynamic_object6={ ’\u0010’, ’\u0017’, ’w’, ’e’,
                  ’w’, ’E’, ’L’, ’C’, ’O’, ’M’, ’E’, ’ ’,
                  ’T’, ’o’, ’ ’,
                  ’o’, ’x’, ’f’, ’o’, ’r’, ’D’,
                  ’x’, ’x’, ’x’, ’x’, ’x’, ’x’, ’x’, ’x’, ’x’, ’x’, ’x’,
                  ’x’, ’ ’, ’ ’ }                     // args[1].data
...

Violated property:
  assertion at file MyTranslator.java line 31 function MyTranslator.main
```

Comparison with JayHorn 0.5.1



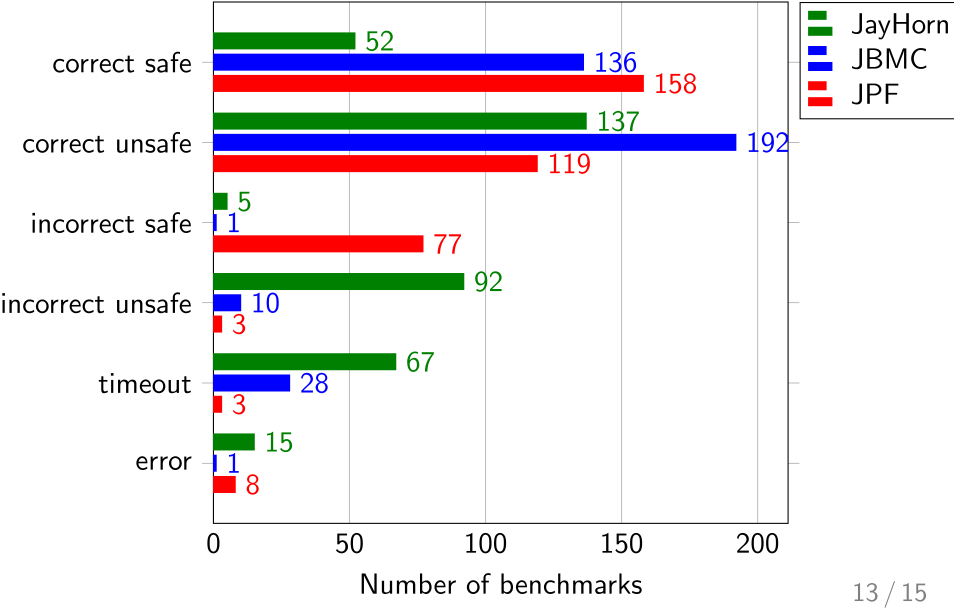
timeout 300s, 15GB

Comparison with JPF v32

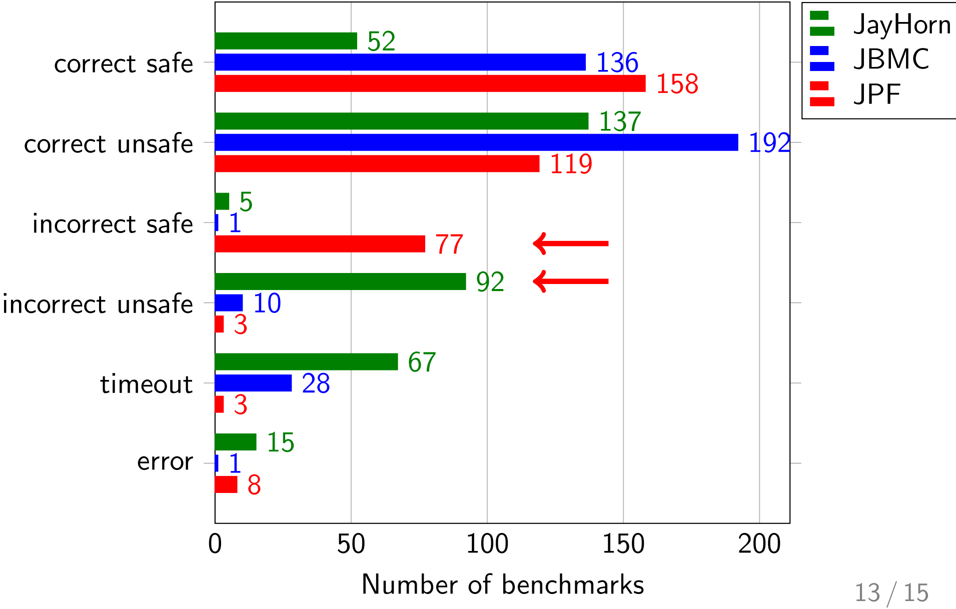


timeout 300s, 15GB

Comparison


JayHorn
JBMC
JPF
correct safe
52
136
158
correct unsafe
137
192
119
incorrect safe
5
1
77
incorrect unsafe
92
10
3
timeout
67
28
3
error
15
1
8
0
50
100
150
200
Number of benchmarks

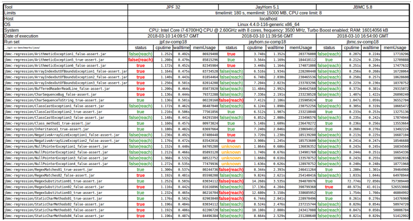
Comparison


correct safe
52
136
158
correct unsafe
137
192
119
incorrect safe
5
1
77
incorrect unsafe
92
10
3
timeout
67
28
3
error
15
1
8
0
50
100
150
200
Number of benchmarks
JayHorn
JBMC
JPF

Java @ TACAS SV-COMP 2019

Objectives:

- More languages in SV-COMP
- Standard benchmark set
- Comparability
- Reproducibility
- Re-use existing benchmarking infrastructure
  3 tools already integrated: JPF, Jayhorn, JBMC



Tool	JPF 32				JayHorn 5.1				JBMC 5.8			
Limits	timelimit: 180 s, memlimit: 15000 MB, CPU core limit: 8											
Host	localhost											
OS	Linux 4.4.0-116-generic x86_64											
System	CPU: Intel Core i7-6700HQ CPU @ 2.60GHz with 8 cores, frequency: 3500 MHz, Turbo Boost enabled; RAM: 16014056 kB											
Date of execution	2018-03-10 14:09:57 GMT				2018-03-10 11:39:56 GMT				2018-03-10 16:54:00 GMT			
Run set	jpf.sv-comp18				jayhorn.sv-comp18				jbmc.sv-comp18			
../git-sv-benchmarks/java/	status	cputime	walltime	memUsage	status	cputime	walltime	memUsage	status	cputime	walltime	memUsage
jbmc-regression/ArithmeticException1_false-assert.jar	false(reach)	1.252s	0.492s	86929408	true	3.748s	1.352s	203776000	false(reach)	0.207s	0.224s	17719296
jbmc-regression/ArithmeticException5_true-assert.jar	false(reach)	1.208s	0.479s	85815296	true	3.564s	1.169s	184410112	true	0.212s	0.226s	12709888
jbmc-regression/ArithmeticException6_false-assert.jar	true	1.172s	0.452s	82345984	true	3.448s	1.164s	174071808	false(reach)	0.251s	0.264s	17477632
jbmc-regression/ArrayIndexOutOfBoundsException1_false-assert.jar	true	1.164s	0.475s	83734528	false(reach)	6.516s	1.934s	228200448	false(reach)	0.256s	0.268s	16728064
jbmc-regression/ArrayIndexOutOfBoundsException2_false-assert.jar	true	1.140s	0.443s	81854464	false(reach)	6.748s	2.030s	230465536	false(reach)	0.250s	0.257s	18628608
jbmc-regression/ArrayIndexOutOfBoundsException3_false-assert.jar	true	1.256s	0.501s	82014208	false(reach)	7.204s	2.023s	233783296	false(reach)	0.223s	0.236s	18378752
jbmc-regression/BufferedReaderReadLine_false-assert.jar	true	1.200s	0.464s	85073920	false(reach)	11.484s	2.992s	264642560	false(reach)	0.373s	0.381s	29315072
jbmc-regression/CharSequenceBug_false-assert.jar	true	1.136s	0.444s	79372288	false(reach)	7.336s	2.191s	233238528	false(reach)	1.407s	1.422s	26890240
jbmc-regression/CharSequenceToString_true-assert.jar	true	1.136s	0.501s	80220160	false(reach)	7.412s	2.186s	235905024	true	1.047s	1.059s	36552704
jbmc-regression/ClassCastException1_false-assert.jar	false(reach)	1.172s	0.462s	86487040	false(reach)	6.124s	1.898s	230752256	false(reach)	0.305s	0.319s	18665472
jbmc-regression/ClassCastException2_true-assert.jar	true	1.216s	0.506s	77561856	true	6.512s	1.907s	233218048	true	0.233s	0.253s	13275136
jbmc-regression/ClassCastException3_false-assert.jar	false(reach)	1.148s	0.441s	84291584	false(reach)	6.852s	2.080s	233496576	false(reach)	0.235s	0.242s	17874944
jbmc-regression/Class_method1_true-assert.jar	true	1.160s	0.457s	80973824	true	5.148s	1.609s	236470272	true	0.236s	0.256s	13553664
jbmc-regression/Inheritance1_true-assert.jar	true	1.180s	0.482s	83697664	true	7.240s	2.046s	230694912	true	0.260s	0.276s	13492224
jbmc-regression/NegativeArraySizeException1_false-assert.jar	false(reach)	1.236s	0.492s	87400448	true	3.720s	1.230s	185139200	false(reach)	0.213s	0.225s	16687104
jbmc-regression/NegativeArraySizeException2_false-assert.jar	false(reach)	1.176s	0.472s	83542016	true	3.908s	1.245s	185753600	false(reach)	0.241s	0.247s	18546688
jbmc-regression/NullPointerException1_false-assert.jar	false(reach)	1.152s	0.440s	84705280	unknown	1.864s	0.686s	136036352	false(reach)	0.243s	0.245s	16834560
jbmc-regression/NullPointerException2_false-assert.jar	false(reach)	1.212s	0.466s	85893120	unknown	1.740s	0.676s	134901760	false(reach)	0.244s	0.251s	16654336
jbmc-regression/NullPointerException3_false-assert.jar	false(reach)	1.368s	0.532s	88522752	unknown	1.668s	0.616s	133578752	false(reach)	0.243s	0.255s	16982016
jbmc-regression/NullPointerException4_false-assert.jar	false(reach)	1.272s	0.535s	77479936	unknown	1.636s	0.626s	128970752	false(reach)	0.240s	0.248s	18771968
jbmc-regression/RegexMatches01_true-assert.jar	true	1.300s	0.537s	80244736	false(reach)	8.344s	2.393s	246411264	true	1.280s	1.301s	39464960
jbmc-regression/RegexMatches02_false-assert.jar	true	1.192s	0.481s	85598208	false(reach)	9.824s	2.621s	254140416	false(reach)	1.033s	1.044s	64978944
jbmc-regression/RegexSubstitution01_true-assert.jar	true	1.252s	0.503s	83034112	false(reach)	14.268s	3.535s	394878976	true	72.774s	72.850s	757309440
jbmc-regression/RegexSubstitution02_false-assert.jar	true	1.116s	0.442s	81616896	false(reach)	17.136s	4.284s	390799360	true	40.973s	41.011s	526553088
jbmc-regression/RegexSubstitution03_true-assert.jar	true	1.232s	0.465s	86216704	false(reach)	12.680s	3.158s	338685952	true	1.754s	1.766s	46804992
jbmc-regression/StaticCharMethods01_true-assert.jar	true	1.176s	0.502s	82903040	false(reach)	6.744s	2.041s	228970496	true	0.261s	0.276s	14376960
jbmc-regression/StaticCharMethods02_false-assert.jar	true	1.196s	0.484s	83034112	false(reach)	8.524s	2.476s	237215744	false(reach)	0.829s	0.854s	50974720
jbmc-regression/StaticCharMethods03_false-assert.jar	true	1.192s	0.486s	82206720	false(reach)	10.188s	2.888s	243417088	false(reach)	0.847s	0.858s	50806784
jbmc-regression/StaticCharMethods04_false-assert.jar	true	1.196s	0.487s	84496384	false(reach)	8.664s	2.529s	231280640	false(reach)	0.821s	0.829s	51412992

Timeline:

- September 2018: Contribution of benchmarks
- October 2018: Tool submission

Watch out on `sv-comp.sosy-lab.org`
Subscribe to `sv-comp@googlegroups.com`

Download JBMC and contribute!

`www.cprover.org/jbmc`

Java @ TACAS SV-COMP 2019

- Contribute and participate!
- `sv-comp.sosy-lab.org`

`www.diffblue.com`

- Jobs in program analysis, verification and machine learning!

diffblue
AI for Code