CPV: A Circuit-Based Program Verifier

Po-Chun Chien and Nian-Ze Lee
Motivation

**Motivation**

- Btor2 circuit [16]
  (HWMCC [6])

- C program
  (SV-COMP [1])

**Hardware model checkers**
ABC [8], AVR [12], ...

**Software verifiers**
CPAchecker [4], Esbmc [10], ...

Could circuits serve as IR for program verification?
Motivation

Could circuits serve as IR for program verification?

Hardware model checkers:
- ABC [8], AVR [12], ...

Software verifiers:
- CPAchecker [4], Esbmc [10], ...

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])
Motivation

Can circuits serve as IR for program verification?

Hardware model checkers
- ABC [8], AVR [12], ...

Software verifiers
- CPAchecker [4], ESBMC [10], ...

TRANSLATE

BTOR2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

SoSy-Lab, LMU Munich
Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Hardware model checkers

**B**tor2 circuit [16]

(HWMCC [6])

Software verifiers

C program

(SV-COMP [1])

**A**BC [8], **A**VR [12], ...

**C**P**A**checker [4], **E**sbmc [10], ...
Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?

Translate

Applicable?

Btor2 circuit [16]
(HWMCC [6])

C program
(SV-COMP [1])

Hardware model checkers

ABC [8], AVR [12], ...

Software verifiers

CPAchecker [4], ESBMC [10], ...

Motivation

Could circuits serve as IR for program verification?
1. Instrument the input program
2. Translate the program to a circuit
3. Verify the translated circuit with hardware model checkers
System Architecture

4. Translate the BTOR2 witness back to software domain
A sequential portfolio consisting of:

- Circuit
- AVR KI [17]
- AVR PDR [11]
- ABC IMC [14]
- ABC PDR [9]
- AVR BMC [7]

If Btor2-to-Aiger translation succeeds
Results in SV-COMP

6th place in ReachSafety
Results in SV-COMP

3rd place in ReachSafety-ECA
Results in SV-COMP

2nd place in ReachSafety-Hardware
Conclusion

- Our new tool CPV uses
  - circuits as IR and
  - hardware verifiers as backend.
- Good performance as a 1st time participant in SV-COMP!


