The CBMC bounded model checker for C

Paul Jackson

School of Informatics
University of Edinburgh

Formal Verification
Spring 2017
Sources

CBMC: Bounded Model Checking for ANSI-C

*Introductory slides on CBMC from CProver website.*
*V1.0, 2010.*

The CProver Suite of Verification Tools.

*Martin Brain. 2016.*
*First part of a tutorial on CBMC and related tools given at the FM 2016 conference.*

References of form In and Tn refer respectively to slide n of these presentations.
Outline

- Recap on BMC. I16-I20.
- Encoding straight line code and conditionals. T16
- Loop unrolling. I29-I32.
- Inlining function calls
  - A standard compiler transformation
  - Recursive definitions handled in similar way to loops
- Slicing. T17
- Library calls
  - Assumed to have non-deterministic behaviour
- Handling the heap. I13
  - Uses EUF.
  - Can apply either SMT techniques or reduction to SAT.
- Bit-vectors. I34-40
Automatic property checks

Include

▶ **Buffer overflows**: For each array access, check whether the upper and lower bounds are violated.

▶ **Pointer safety**: Search for NULL-pointer dereferences or dereferences of other invalid pointers.

▶ **Division by zero**: Check whether there is a division by zero in the program.

▶ **Not-a-Number**: Check whether floating-point computation may result in NaNs.

▶ **Uninitialised local**: Check whether the program uses an uninitialised local variable.

▶ **Data race**: Check whether a concurrent program accesses a shared variable at the same time in two threads.
CProver Tool Suite

See T11