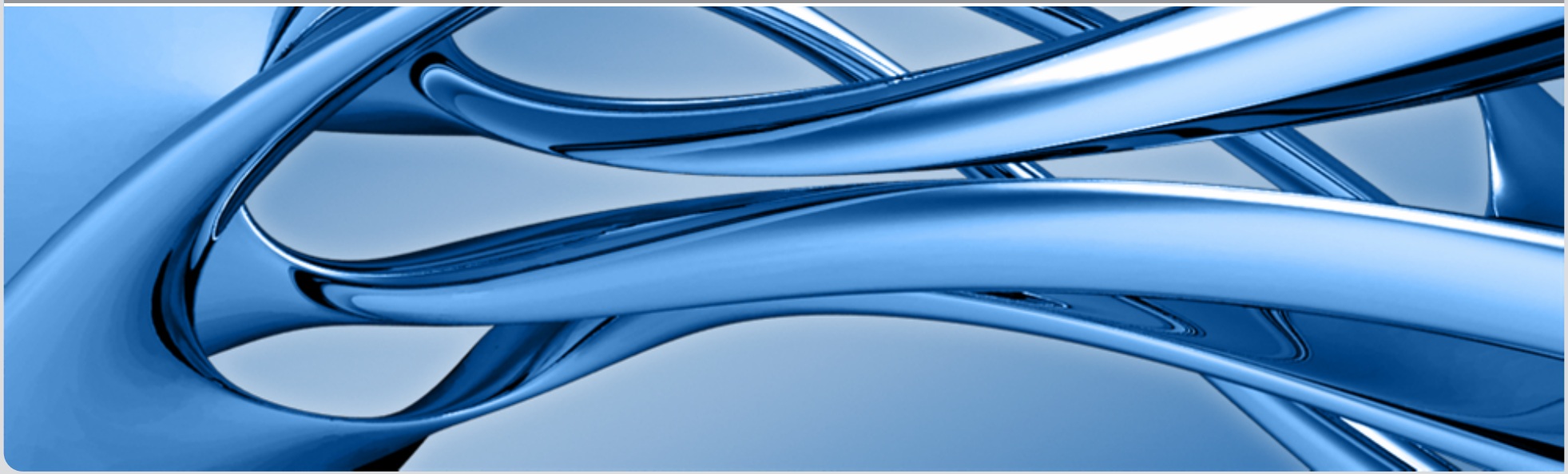
Karlsruhe Institute of Technology

Low-level Software Bounded Model Checking

Fully Automatic Software Verification

Authors: Florian Merz, Carsten Sinz, Stephan Falke

RESEARCH GROUP "VERIFICATION MEETS ALGORITHM ENGINEERING"



Introducing LLBMC

Karlsruhe Institute of Technology

- Software verification tool
- Fully automatic
- Bit-precise
- Low-level, embedded C-code
- Focus on bug finding
- Software Bounded Model Checking

Software Bounded Model Checking

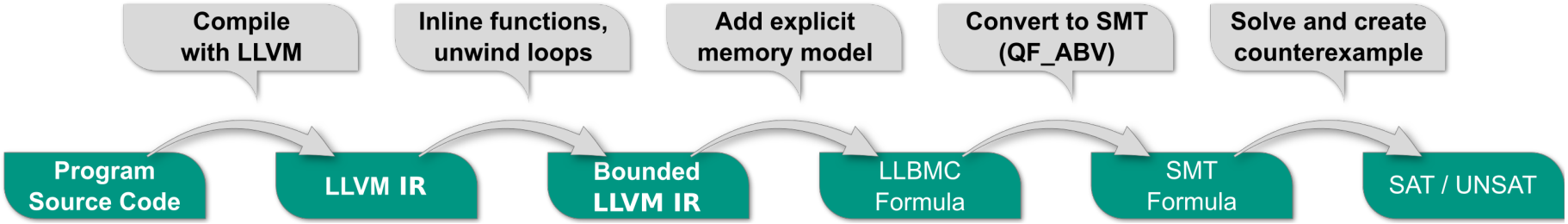
Karlsruhe Institute of Technology

- LLBMC does verification of bounded execution traces ...
- by using loop unwinding & function inlining ...
- ... to create a directed acyclic control flow graph, ...
- ... which is converted to an SMT formula ...
- ... using the Theory of Bit Vectors for ALU operations, and ...
- ... the Theory of Arrays for memory access operations.

What can it verify?

- Division by zero
- Arithmetic overflow
- Invalid `malloc`/`free`
- Invalid memory access operations (`load`/`store`)
- Custom preconditions/postconditions (`assert()`/`assume()`)

LLBMC architecture



Karlsruhe Institute of Technology

See you at the poster