MUNI
FI

Symbiotic 10

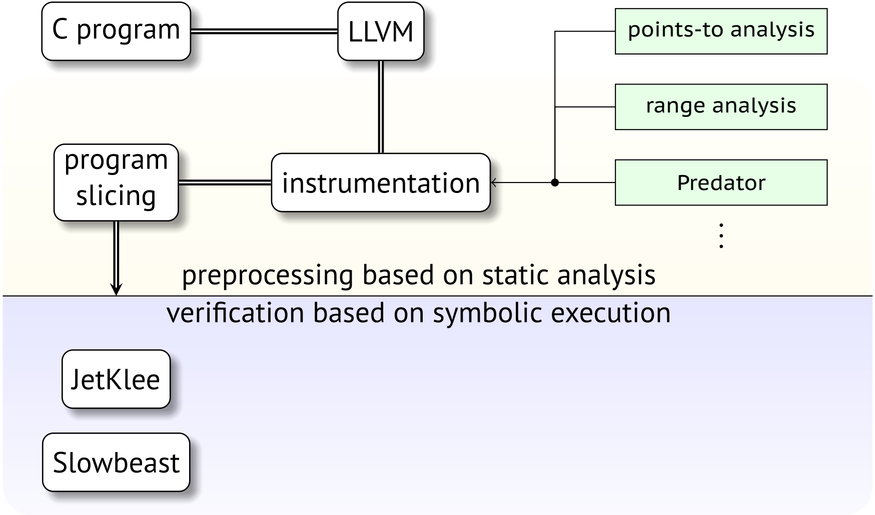
Lazy Memory Initialization and Compact Symbolic Execution

**Martin Jonáš, Kristián Kumor, Jakub Novák, Jindřich Sedláček,
Marek Trtík, Lukáš Zaoral, Paulína Ayaziová, and *Jan Strejček***

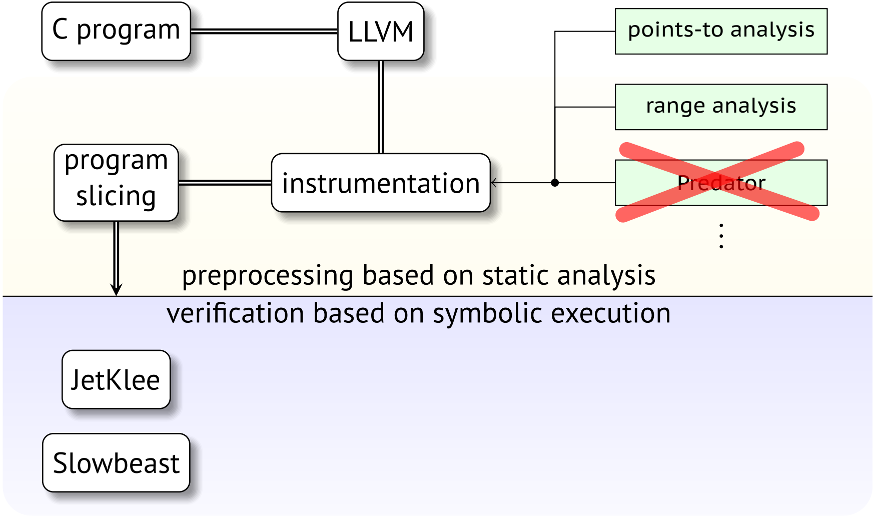
Faculty of Informatics, Masaryk University, Brno, Czechia

TACAS 2024 – April 8, 2024

Symbiotic framework



Symbiotic framework: what is new in Symbiotic 10



C program

LLVM

points-to analysis

range analysis

~~Predator~~

program slicing

instrumentation

⋮

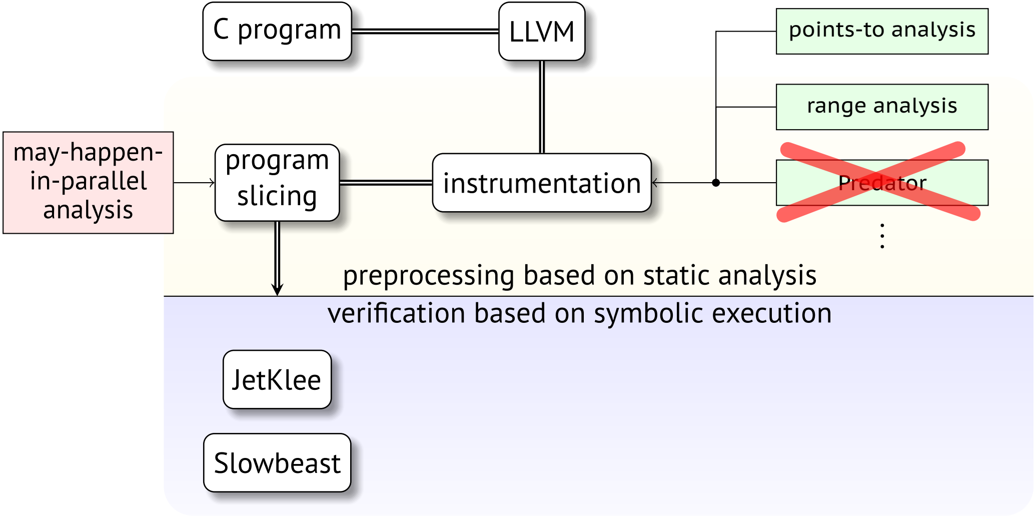
preprocessing based on static analysis

verification based on symbolic execution

JetKlee

Slowbeast

Symbiotic framework: what is new in Symbiotic 10



C program

LLVM

points-to analysis

range analysis

may-happen-in-parallel analysis

program slicing

instrumentation

~~Predator~~

⋮

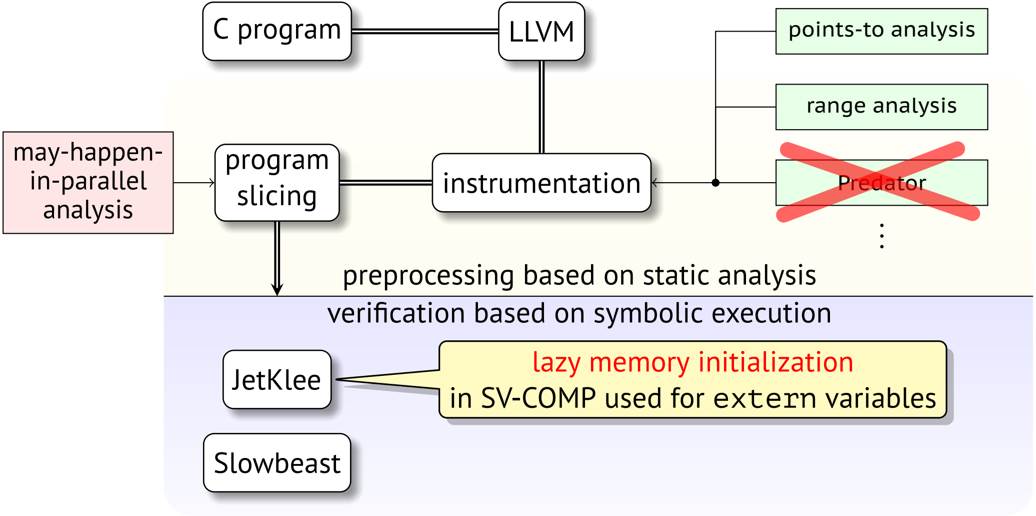
preprocessing based on static analysis

verification based on symbolic execution

JetKlee

Slowbeast

Symbiotic framework: what is new in Symbiotic 10



C program

LLVM

points-to analysis

range analysis

~~Predator~~

⋮

may-happen-in-parallel analysis

program slicing

instrumentation

preprocessing based on static analysis

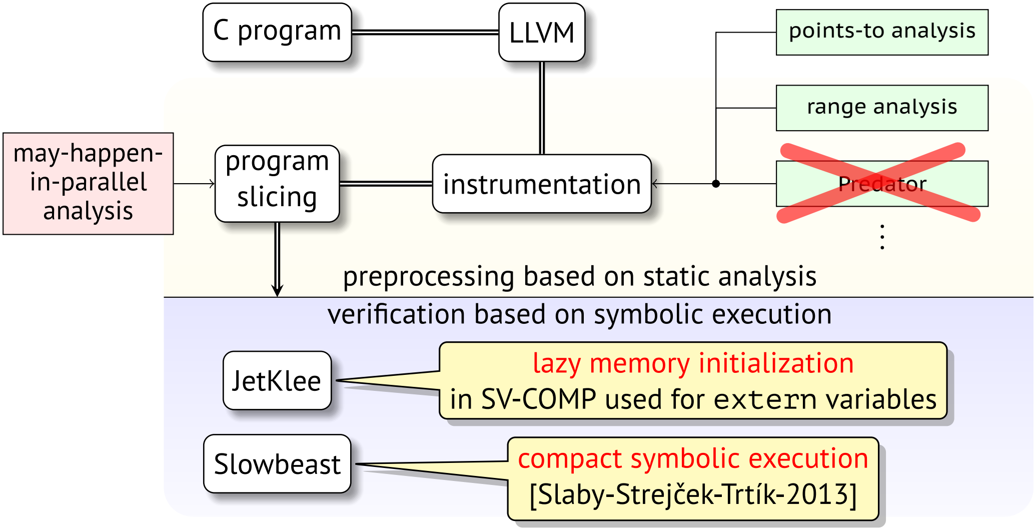
verification based on symbolic execution

JetKlee

Slowbeast

lazy memory initialization
in SV-COMP used for `extern` variables

Symbiotic framework: what is new in Symbiotic 10



C program

LLVM

points-to analysis

range analysis

~~Predator~~

⋮

may-happen-in-parallel analysis

program slicing

instrumentation

preprocessing based on static analysis

verification based on symbolic execution

JetKlee

lazy memory initialization
in SV-COMP used for `extern` variables

Slowbeast

compact symbolic execution
[Slaby-Strejček-Trtík-2013]

Other improvements in Symbiotic

workflow of *symbolic execution (SE)* engines in *unreach-call*

1. forward SE in JetKlee (for 333s)
2. compact SE in Slowbeast (for 60s)
3. backward SE with loop folding (BSELF) in Slowbeast (no limit)
4. forward SE in Slowbeast (no limit)

Other improvements in Symbiotic

workflow of *symbolic execution (SE)* engines in *unreach-call*

1. forward SE in JetKlee (for 333s)
2. compact SE in Slowbeast (for 60s)
3. backward SE with loop folding (BSELF) in Slowbeast (no limit)
4. forward SE in Slowbeast (no limit)

other changes

- JetKlee can generate violation witnesses in format 2.0
- 300+ commits from Klee upstream merged to JetKlee
- all components run on LLVM 14
- many fixes (now we support Juliet benchmarks)

Results in SV-COMP 2024

- 2nd in MemSafety
- 2nd in FalsificationOverall
- 4th in SoftwareSystems

Results in SV-COMP 2024

- 2nd in MemSafety
- 2nd in FalsificationOverall
- 4th in SoftwareSystems

results in **MemSafety**	*PredatorHP*	*Symbiotic 10*
correct true	1630	**1643**
correct false	193	**212**
correct-unconfirmed true	0	0
correct-unconfirmed false	**3**	0
incorrect true	0	**5**[*]
incorrect false	**3**	0

[*] bugs caused mostly by imprecise modeling of `setlocale` and `getopt_long`