

Prograss Report 3

Xie Li

September 14, 2020

Overview of the Progress

- ▶ Introduction to KLEE and static analyzer of ABSINT
- ▶ A summary of the tools: capabilities and algorithms.
- ▶

Tool Survey: KLEE

Usage:

```
llvm-gcc --emit-llvm -c code.c -o code.bc  
klee --max-time 2 --sym-args 1 10 10--sym-files 2  
2000 --max-fail 1 code.bc
```

Algorithm and Techniques:

- ▶ Symbolic Execution.
- ▶ Maintaining of path condition of the path.
- ▶ Classify dangerous operation and when bug identified use SMT solver to find concrete value.

Application:

KLEE was applied and reach a coverage of 81% of GNU Coreutil. It found totally 10 errors and even some bugs in heavily-tested code.

Tool Survey: `ASTREE` of `AbsInt`

Toolset: Check C code for runtime error: `ASTREE`.

Check code guideline: `RULECHECKER`.

Compiling: `COMP CERT`.

Check Stack usage: `STACKANALYZER` .

Analyze execution time: `AIT`, `TIMEWEAVER`.

Tool Survey: ASTREE

ABSINT focuses on non-functional program errors.

Capability: Check

- ▶ Division by zero
- ▶ Out-of-bounds array indexing.
- ▶ erroneous pointer manipulation and dereferencing
- ▶ integer and floating-point arithmetic overflow
- ▶ read uninitialized variables
- ▶ data races
- ▶ inconsistent locking
- ▶ violation of user-given assertions
- ▶ unreachable code

Summary of Tools

- ▶ CBMC: verifies memory safety (array bounds and safe use of pointers), check for exceptions. Algorithm used: bounded model checking.
- ▶ NuSMV: a symbolic model checker utilizing BDD library and able to model and check.
- ▶ CPAchecker: a static analyzing tool capable of doing data-flow analysis and automatic testing. Algorithm used: CPA algorithm which integrates several static analysis algorithms based on abstract interpretation, symbolic execution for automatic testing and CEGAR loop for refining.
- ▶ Infer: A static analysis tool used mainly for finding bugs for programs that manipulate heaps and memory. Algorithm: inference of separation logic and invariant synthesis using shape analysis, incorrectness logic inference.
- ▶ KLEE: A testing tool based on LLVM use symbolic execution for automatic testing.
- ▶ ASTREE: A static analyzer detecting runtime errors. Algorithm: Abstract interpretation.

Functionalities of Tools

Toolname	AI	CE	BMC	SMC	SE	Conc	SA
CBMC		×	×		×		
CPACHECKER	×	×	×(dep.)		×		×
INFER							×
KLEE				×			
ASTREE	×			×		×	

Trace Abstraction

Combination with Sample-based Algorithm