Mixed Fixed-Point and Floating-Point Symbolic Execution

Thom Hughes, Daniel Schemmel, Martin Nowack, Cristian Cadar

Motivation

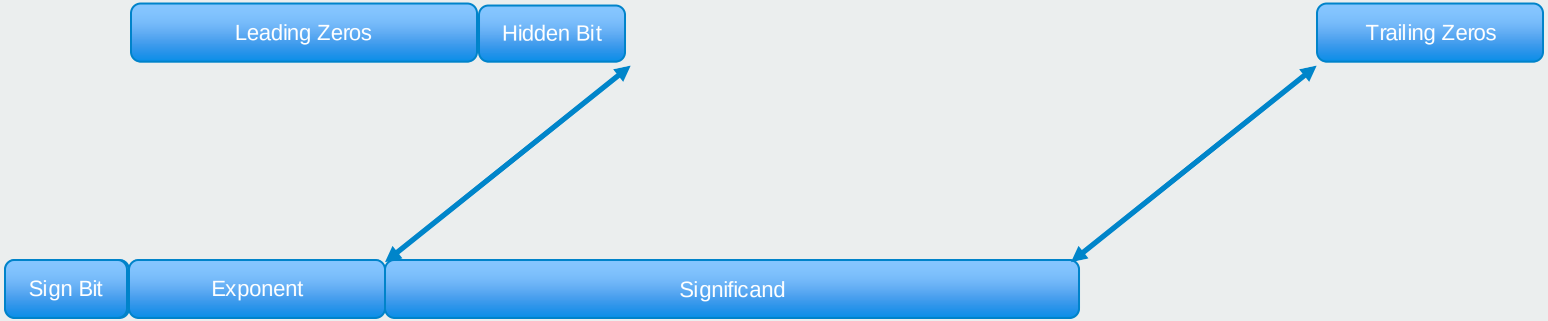
- KLEE currently concretizes floating-point operations
  - One arbitrary model chosen
- Exact floating-point reasoning is computationally expensive
  - As demonstrated in KLEE float paper (Liew et al. 2017)

Our Approach

- Approximate using fixed-point numbers during solving
- Don’t sacrifice accuracy during concrete execution

Transformation Between Representations

Fixed Point Representation (Size Specified At Runtime)



Symbolic Bytes (As IEEE Float)

Aggregated Runtime, Coverage & Effectiveness

Implementation	Branches Covered	Runtime (mins)	True Positives
KLEE Mixed Point	1 420	219	11
KLEE Float	1 564	784	20
KLEE Mainline	688	37	1

Summary

- Mixed approach succeeds in sacrificing accuracy for speed
  - Only with symbolic floating-point expressions

- Ongoing work
  - long double support
  - sqrt implementation unfinished