2LS: Arrays and Loop Unwinding

(Competition Contribution)

Viktor Malík[3], František Nečas[3], Peter Schrammel[12], Tomáš Vojnar[3]

[1]Diffblue Ltd., UK

[2]University of Sussex, UK

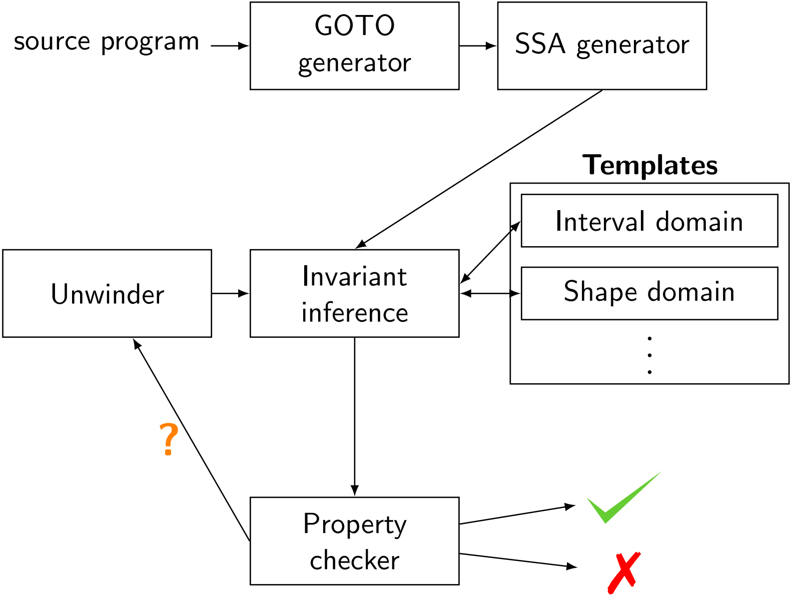
[3]Brno University of Technology, FIT, CZ

April 24, 2023

The 2LS Framework

- Static Analysis tool for C programs built upon the CProver infrastructure
- Computes loop invariants
- kIkI = k-induction, bounded model checking and abstract interpretation

The 2LS Framework

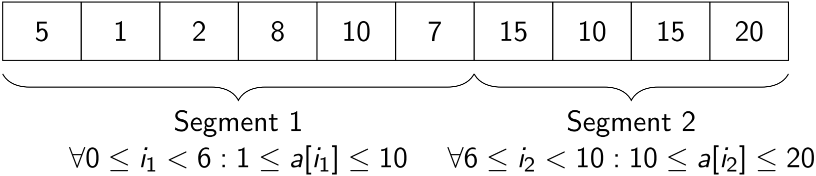


The 2LS Framework

- Static Analysis tool for C programs built upon the CProver infrastructure
- Computes loop invariants
- kIkI $=$ k-induction, bounded model checking and abstract interpretation
- SSA internal representation facilitates usage of an incremental SMT solver

New Array Domain

- Invariants are computed based on templates
- Arrays are split into contiguous, non-overlapping segments. A different invariant can be computed for each segment.
- Segment borders are determined from indices used to write into the array.



5	1	2	8	10	7	15	10	15	20

Segment 1

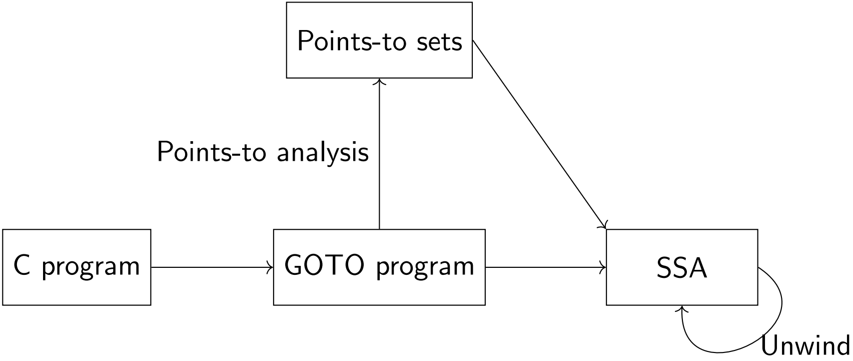
$\forall 0 \leq i_1 < 6 : 1 \leq a[i_1] \leq 10$

Segment 2

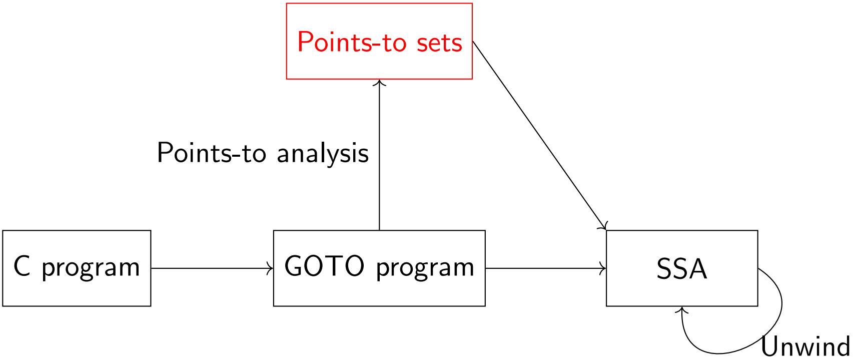
$\forall 6 \leq i_2 < 10 : 10 \leq a[i_2] \leq 20$

- Array domain invariant is a conjunction of segment invariants

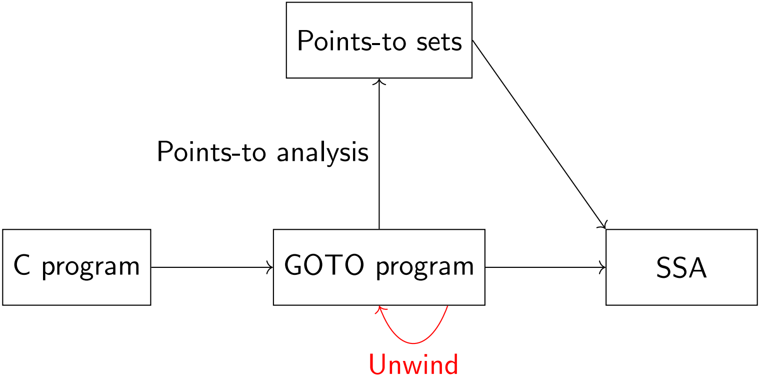
Loop Unwinding



Loop Unwinding



Improved Loop Unwinding



Results

- Results from SV-COMP 2023 before last-minute disqualifications
- Heap improvements (MemSafety and ReachSafety-Heap categories):
  - correct false: 110 → 177
  - correct true: 51 → 82
- 2 → 17 tasks solved in ReachSafety-Arrays
- Future work: more robust array domain, incremental SAT solving for loop unwinding