Exploring The Relationship Between Unwind Bound and Model Checking Complexity in CBMC

TU Delft

1. Introduction

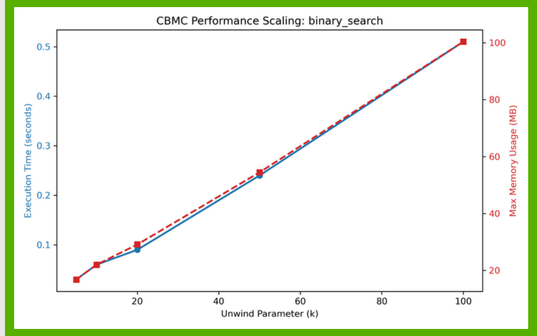
- Software correctness is critical in modern systems.
- Formal verification tools like CBMC (C Bounded Model Checker) offer a way to mathematically guarantee that a C program satisfies its specifications, by converting the program into a SAT problem and checking it automatically.
- CBMC controls how deeply it explores loops and recursion via a parameter called the unwind bound (k).
- The CBMC manual notes that larger k values lead to more resource-intensive verification, but this relationship has never been systematically measured
- We measure complexity using three metrics: verification time, memory usage, and the size of the generated SAT instance (variables and clauses)

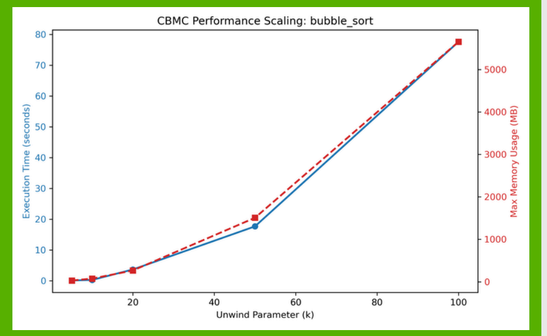
2. Research Question

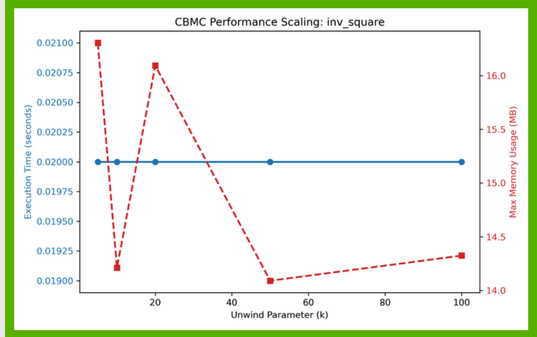
What is the impact of the unwind bound (k) on model checking complexity in CBMC? .

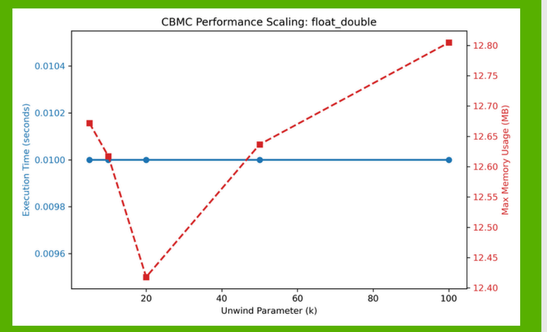
We hypothesize that model checking complexity scales with the algorithmic time complexity of the program under verification.

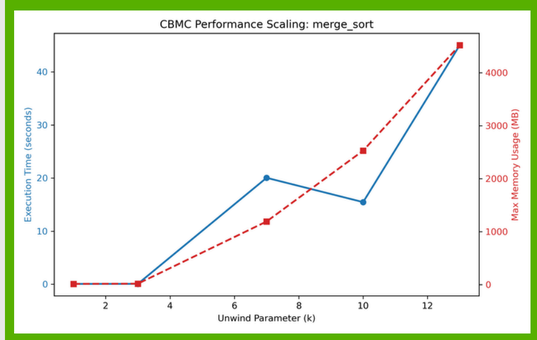
3. Results

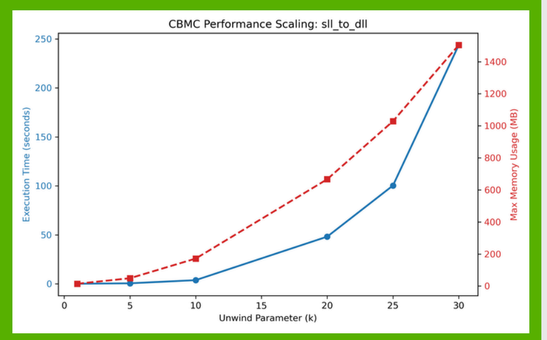












4. Conclusions and Limitations

- Our results reject the initial hypothesis: Model checking complexity does not mirror algorithmic time complexity, but rather loop structure and operation cost
- No loops → constant complexity regardless of k
- Nested loops → quadratic growth with k
- Heap operations per iteration → high polynomial or exponential growth with k
- We recommend increasing k incrementally rather than setting a large bound upfront, to avoid unnecessary resource consumption.

Limitations:

- Small number of case studies
- Results are machine-specific
- Larger production-code benchmarks may show different behaviour.

5. Future Work

- Automatic k-value recommendation based on program structure heuristics
- Benchmarking on larger, production-scale C programs
- Systematic study of floating-point programs with k-dependent loops
- Comparison of k-complexity across different SAT solver backends

Author: **Mihai-Filip Frânculescu**
M.F.Franculescu@student.tudelft.nl

Supervisors: **Dr. Benedikt Ahrens**
Dr. Anna Lukina