FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

for(syte)
Formal Methods
in Systems Engineering

Rely-Guarantee Reasoning for Automated Bound Analysis of Non-Blocking Algorithms

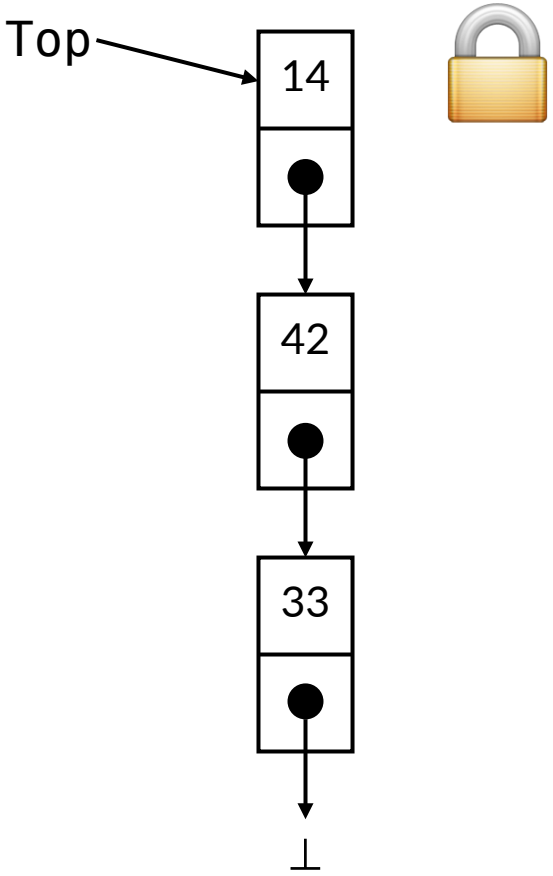
Thomas Pani, Georg Weissenbacher, Florian Zuleger

FMCAD Student Forum ’18 · Oct 31, 2018

A concurrent stack

Thread 1

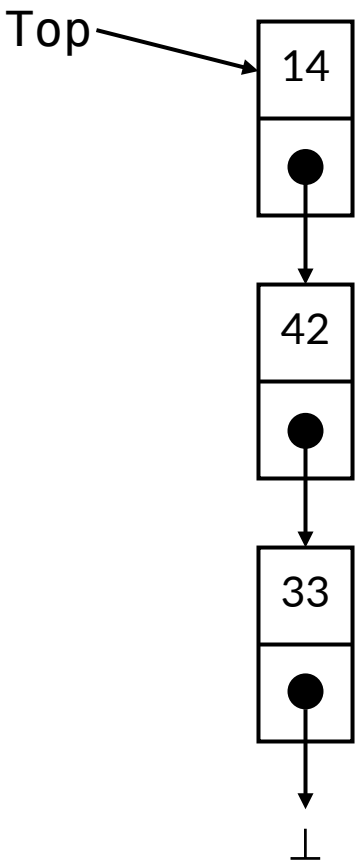
Thread 2



A concurrent non-blocking stack

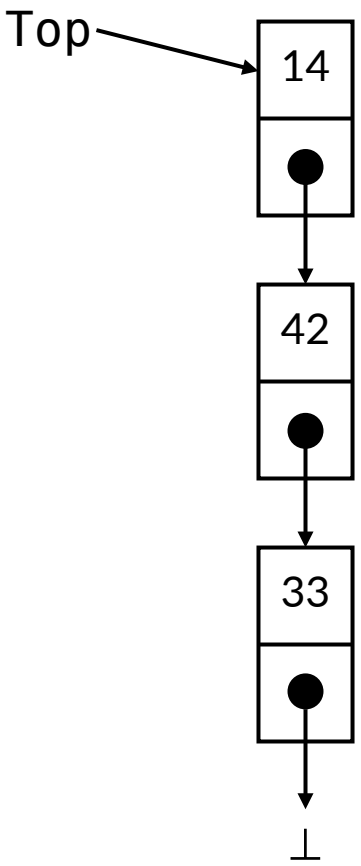
Thread 1

Thread 2



A concurrent non-blocking stack

Thread 1



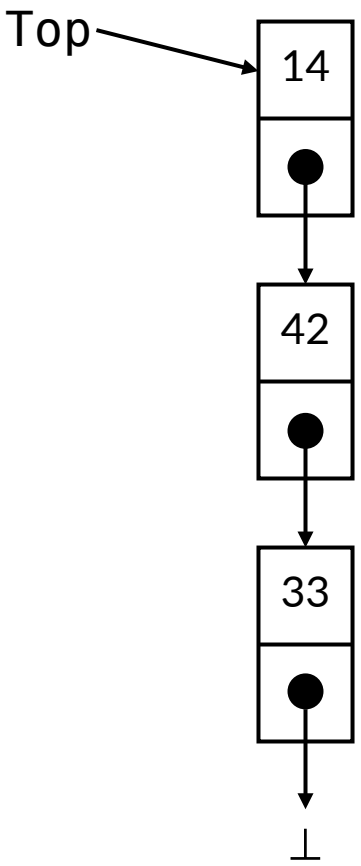
Thread 2

Use **strong primitives to synchronize** (e.g., compare-and-swap).

Concurrent modifications cause **retry (loop)**.

A concurrent non-blocking stack

Thread 1



Thread 2

Use **strong primitives to synchronize** (e.g., compare-and-swap).

Concurrent modifications cause **retry (loop)**.

Complexity?

Linear in the number of threads.

Contributions

Present first **automated procedure to compute** linear **complexity** of popular non-blocking data structures:

1. **Extend rely-guarantee reasoning** to bound analysis.
2. **Reduce bound analysis** of concurrent programs to bound analysis of sequential programs.

Ongoing work

1. Extending the bound analysis
2. Supporting other algorithms / protocols
3. Applying our abstraction to safety properties
4. Improving our implementation

Coffee break / poster session