Practical Course - Recent Advances in Model Checking

Alexandros Evangelidis
10 May 2022
1. Introduction

2. Sources of errors and proposed solutions

3. Conclusion
Introduction
- Correct Probabilistic Model Checking with Floating-Point Arithmetic, by Arnd Hartmanns.
The problem

- Probabilistic model checkers can return erroneous results.
The problem

- Probabilistic model checkers can return erroneous results.
- Computing reachability probabilities using numerical approximate methods (e.g., Value Iteration).
Value Iteration

- Initialize solution vector $x$.
- Iterate:
  - $x_{n+1}(s) = \max_{a \in A(s)} \sum_{s' \in S} \delta(s, a, s') \cdot x_n(s')$.
  - until convergence.
Sources of errors and proposed solutions
Sources of errors and proposed solutions

• Stopping criterion.

  Proposed solution: (Interval Iteration) Run two value iterations one from below and one from above. Terminate when the difference between the over and under approximation is \( \leq \epsilon \).
Sources of errors and proposed solutions

- Stopping criterion.
- Proposed solution: (Interval Iteration) Run two value iterations one from below and one from above.
• Stopping criterion.

• Proposed solution: (Interval Iteration) Run two value iterations one from below and one from above.

• terminate when the difference between the over and under approximation is \( \leq \epsilon \).
Sources of errors and proposed solutions

• Stopping criterion.
• Proposed solution: (Interval Iteration) Run two value iterations one from below and one from above.
• terminate when the difference between the over and under approximation is \( \leq \epsilon \).
Sources of errors and proposed solutions

• Roundoff errors.
Sources of errors and proposed solutions

- Roundoff errors.
- Potentially problematic since in iterative computations rounding may happen at every step.

Main claim of the paper: "Using a sound algorithm does not guarantee correct results."
Sources of errors and proposed solutions

- Roundoff errors.
- Potentially problematic since in iterative computations rounding may happen at every step.
- **Main claim of the paper**: “Using a sound algorithm does not guarantee correct results.”
IEEE 754 standard defines three directed rounding modes: round towards zero (i.e. truncation), round towards $+\infty$ (i.e., always round up), and round towards $-\infty$ (i.e. always round down).

**Proposed solution:** Control the rounding mode of the floating-point operations performed in the Interval Iteration algorithm.
IEEE 754 standard defines three directed rounding modes: round towards zero (i.e. truncation), round towards $+\infty$ (i.e., always round up), and round towards $-\infty$ (i.e. always round down).

**Proposed solution:** Control the rounding mode of the floating-point operations performed in the Interval Iteration algorithm.

For example, when checking whether the relative error $> \epsilon$, round towards $+\infty$, etc.
Conclusion
• You will learn a lot about the state of the art algorithms used in probabilistic verification.

• Control of the floating-point rounding mode however appears to be a rarely-used feature of IEEE 754 implementations.