Seminar

Formal Verification Meets Machine Learning

Introduction

Winter Semester 2021/22; October 13, 2021

Thomas Noll et al.
Software Modeling and Verification Group
RWTH Aachen University

`https://moves.rwth-aachen.de/teaching/ws-21-22/fvmml/`

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

Outline

Formal Verification Meets Machine Learning

Formal verification

- Computer-supported mathematical analysis methods for ensuring correctness of systems
  - model checking, theorem proving, ...
- Often applied to safety-critical systems
- Complementary to testing methods

Formal Verification Meets Machine Learning

Formal verification

- Computer-supported mathematical analysis methods for ensuring correctness of systems
  - model checking, theorem proving, ...
- Often applied to safety-critical systems
- Complementary to testing methods

Machine learning

- Algorithms learning from data that is observed in possibly unknown environments
  - autonomous systems, computer vision, video games, ...
- Increasingly applied in safety-critical settings

Formal Verification Meets Machine Learning

Formal verification

- Computer-supported mathematical analysis methods for ensuring correctness of systems
  - model checking, theorem proving, ...
- Often applied to safety-critical systems
- Complementary to testing methods

Machine learning

- Algorithms learning from data that is observed in possibly unknown environments
  - autonomous systems, computer vision, video games, ...
- Increasingly applied in safety-critical settings

Research issues

- Safety-related issues for machine learning (e.g., robustness)
- Explainability in AI and in model checking (and similar techniques)
- Scalability and applicability of formal verification techniques

Outline

Goals

Aims of this seminar

- Independent understanding of a scientific topic
- Acquiring, reading and understanding scientific literature
  - given reference(s) sufficient in most cases
- Writing of your own report on this topic
  - far more that just a translation/rewording
  - usually an “extended subset” of original literature
    - “subset”: present core ideas and omit too specific details (e.g., related work or optimisations)
    - “extended”: more extensive explanations, examples, ...
    - discuss contents with supervisor!
- Oral presentation of your results
  - can be “proper subset” of report
  - generally: less (detailed) definitions/proofs and more examples

Requirements on Report

Your report

- Independent writing of a report of 12–15 pages
- First milestone: detailed outline
  - not: “1. Introduction/2. Main part/3. Conclusions”
  - rather: overview of structure (section headers, main definitions/theorems) and initial part of main section (one page)
- Correct citation of all consulted literature
- Plagiarism: taking text blocks (from literature or web) without source indication causes immediate exclusion from this seminar
- Font size 12pt with “standard” page layout
  - LaTeX template will be made available on seminar web page
- Language: German or English
- We expect the correct usage of spelling and grammar
  - $\geq$ 10 errors per page $\Longrightarrow$ abortion of correction

Requirements on Talk

Your talk

- Organised as in-person or Zoom meeting
- Talk of 30 minutes
- Focus your talk on the audience
- Descriptive slides:
  - $\leq$ 15 lines of text
  - use (base) colors in a useful manner
  - number your slides
- Language: German or English
- No spelling mistakes please!
- Finish in time. Overtime is bad
- Ask for questions
- Have backup slides ready for expected questions
- LaTeX `beamer` template will be made available on seminar web page

Outline

Important Dates

Deadlines

- October 20: Topic preferences due
- November 15: Detailed outline due
- December 13: Full report due
- January 17: Presentation slides due
- January 31–February 4: Seminar talks (two days)

Important

Missing a deadline causes immediate exclusion from the seminar

Selecting Your Topic

Procedure

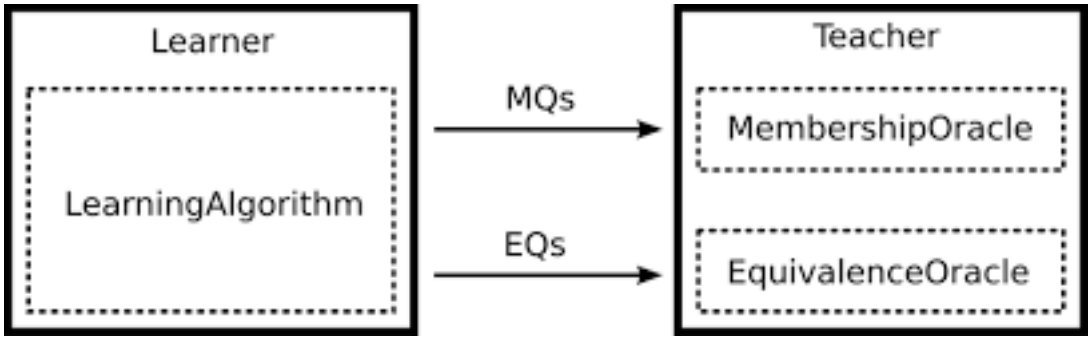
- Check out Foodle poll at `https://terminplaner.dfn.de/V7a9RyKh8wxFAwRL`
- Please give at least three “Yes” votes ✓
- Preferably additional “Maybe” votes (✓)
- Give as comment:
  - preference of topics (if desired)
  - language of report and talk (English/German)
- **Fill form by Wednesday, October 20**
- We do our best to find an adequate topic-student assignment
  - disclaimer: no guarantee for an optimal solution
- Assignment of topics and supervisors will be published on web site by mid next week

Withdrawal

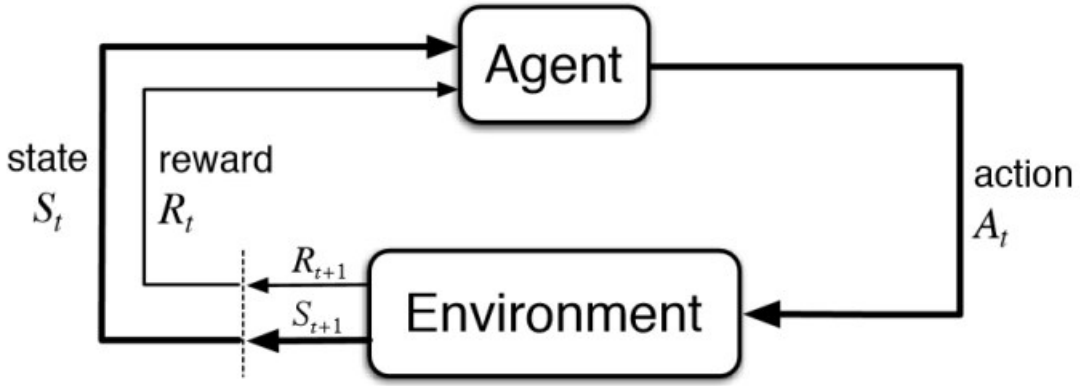
- You have up to three weeks to refrain from participating in this seminar.
- Later cancellation (by you or by us) causes a not passed for this seminar and reduces your (three) possibilities by one.

Outline

Approaches to Machine Learning



1. Introduction to Automata Learning
2. Introduction to Reinforcement Learning

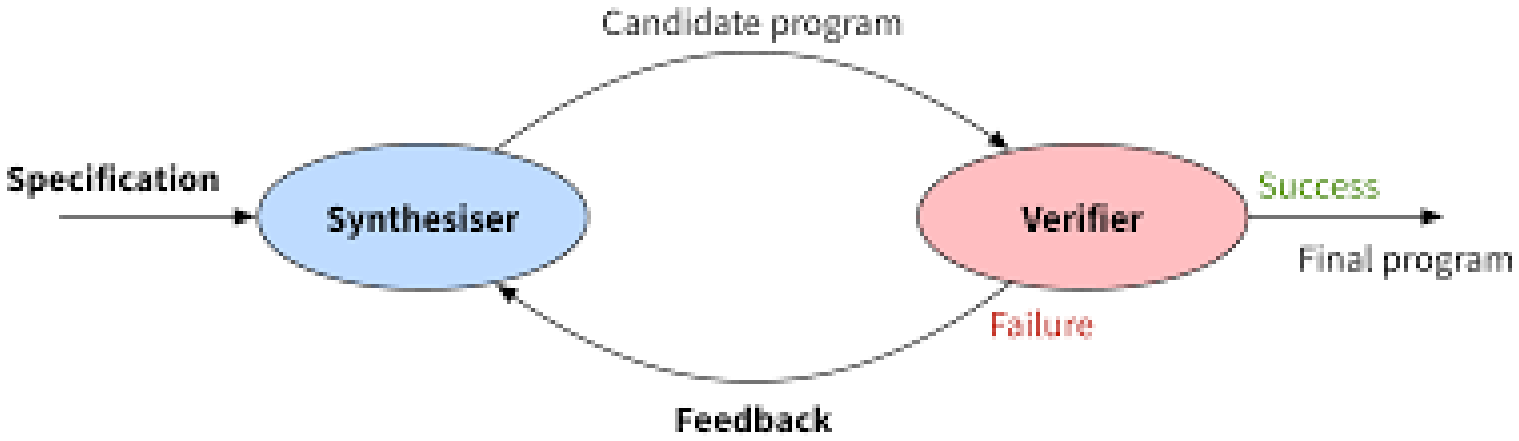


Learning for Program Verification

$$\text{(while)}\ \frac{\{A \wedge b\}\, c\, \{A\}}{\{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{A \wedge \neg b\}}$$

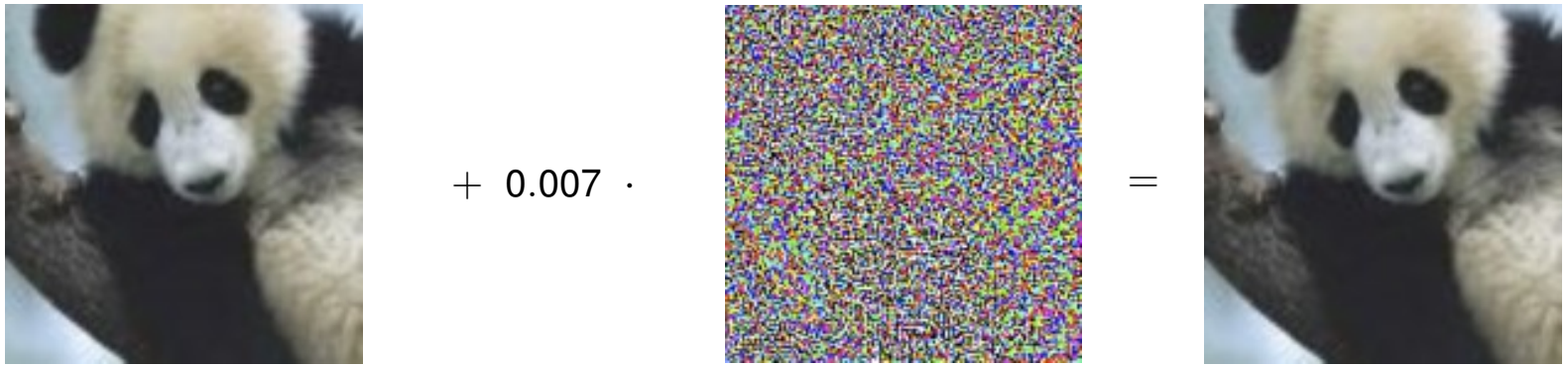
3. Learning Loop Invariants
4. Model Checking vs. Machine Learning
5. Reinforcement Learning of Invariants
6. Termination Analysis of Probabilistic Programs

Learning for Program Synthesis



7. Programming by Example
8. Synthesis of Probabilistic Programs
9. Learning Controllers under Safety Conditions
10. Combining Program Synthesis and Reinforcement Learning
11. Deep Learning for Code Synthesis
12. Learning Programs from Noisy Data
13. Supervised Learning for Program Correctness

Verification of Deep Neural Networks



Adversarial Example [Goodfellow 2015]

14. An Abstract Domain for Certifying Neural Networks
15. Efficient Neural Network Verification via Adaptive Refinement and Adversarial Search
16. Correctness Verification of Neural Networks
17. Fast and Precise Certification of Transformers
18. Robustness Certification with Generative Models
19. Provable Repair of Deep Neural Networks
20. Verifying Recurrent Neural Networks Using Invariant Inference
21. Scalable Polyhedral Verification of Recurrent Neural Networks
22. Property-Directed Verification of Recurrent Neural Networks

Outline

Some Final Hints

Hints

- Take your time to understand your literature.
- Be proactive! Look for additional literature and information.
- Discuss the content of your report with other students.
- Be proactive! Contact your supervisor on time.
- Prepare the meeting(s) with your supervisor.
- Forget the idea that you can prepare a talk in a day or two.

We wish you success and look forward to an enjoyable and high-quality seminar!