Formal Semantics of Programming Languages

Introduction

Winter Semester 2019/20; 9 October, 2019

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

https://moves.rwth-aachen.de/teaching/ws-1819/qpa/

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

Outline

Overview

Aspects of Programming Languages

Syntax: “How does a program look like?”

- hierarchical composition of programs from structural components

$\Rightarrow$ *Compiler Construction*

Overview

Aspects of Programming Languages

Syntax: “How does a program look like?”

- hierarchical composition of programs from structural components

$\Rightarrow$ *Compiler Construction*

Semantics: “What does this program mean?”

- output/behaviour/... in dependence of input/environment/...

$\Rightarrow$ this seminar

Overview

Aspects of Programming Languages

Syntax: “How does a program look like?”

- hierarchical composition of programs from structural components

⇒ *Compiler Construction*

Semantics: “What does this program mean?”

- output/behaviour/... in dependence of input/environment/...

⇒ this seminar

Pragmatics: “Is the programming language practically usable?”

- length and understandability of programs
- learnability of programming language
- appropriateness for specific applications, ...

⇒ *Software Engineering*

Main Applications

- Implementation of algorithms
  - exact understanding of semantics avoids uncertainties and enables correctness proofs
- Design of (new) programming languages
  - missing details, ambiguities and inconsistencies can be recognised
- Implementation of compilers
  - correctness of translation and optimisation steps

Overview

Areas Covered in this Seminar

- Nondeterminism and Recursion
- Concurrency
- Pointers and Objects
- Software Verification
- Safety, Privacy and Security

Outline

Aims of this Seminar

Goals

Aims of this seminar

- Independent understanding of a scientific topic
- Acquiring, reading and understanding scientific literature
  - given references sufficient in most cases
- Writing of your own report on this topic
  - far more that just a translation/rewording
  - usually an “extended subset” of paper
    - “subset”: present core ideas and omit too specific details (e.g., extension of partial to total correctness)
    - “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 10–15 pages
- First milestone: detailed outline
  - not: “1. Introduction/2. Main part/3. Conclusions”
  - but: overview of structure (section headers, main definitions/theorems) and initial part of main section (one page)
- Complete set of references to all consulted literature
- Correct citation of important 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
- Language: German or English
- We expect the correct usage of spelling and grammar
  - $\geq$ 10 errors per page $\Longrightarrow$ abortion of correction
- LaTeX template will be made available on seminar web page

Requirements on Talk

Your talk

- Talk of 30 minutes
- Available: projector, presenter, [laptop]
- 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

- 4 November: Detailed outline of report due
- 2 December: Full report due
- 13 January: Presentation slides due
- 28/29 January (?): Seminar talks

Important Dates

Deadlines

- 4 November: Detailed outline of report due
- 2 December: Full report due
- 13 January: Presentation slides due
- 28/29 January (?): Seminar talks

Missing a deadline causes immediate exclusion from the seminar

Selecting Your Topic

Procedure

- You obtain(ed) a list of topics of this seminar.
- Classified according to BSc/MSc level.
  - MSc students please choose at least one “M-only” topic
- Indicate the preference of your topics (first, second, third).
- Return sheet here or by Monday (14 October) via e-mail (`noll@cs.rwth-aachen.de`) or to secretary.
- We do our best to find an adequate topic-student assignment.
  - disclaimer: no guarantee for an optimal solution
- Assignment will be published on web site next week.
- Then also your supervisor will be indicated.

Important Dates

Selecting Your Topic

Procedure

- You obtain(ed) a list of topics of this seminar.
- Classified according to BSc/MSc level.
  - MSc students please choose at least one “M-only” topic
- Indicate the preference of your topics (first, second, third).
- Return sheet here or by Monday (14 October) via e-mail (`noll@cs.rwth-aachen.de`) or to secretary.
- We do our best to find an adequate topic-student assignment.
  - disclaimer: no guarantee for an optimal solution
- Assignment will be published on web site next week.
- Then also your supervisor will be indicated.

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

The Topics

Recursion, Nondeterminism and Probabilities

Goal

Extensions of Hoare Logics to deal with “advanced” programming concepts

- recursion
- nondeterminism
- probabilistic choice

Topics

1. Proving total correctness of recursive procedures (B/M)
2. Hoare logics for recursive procedures and unbounded nondeterminism (B/M)
3. Semantics of probabilistic programs (B/M)

The Topics

Concurrency

Goal

Various models for defining the semantics of concurrency

- message passing/(relaxed) shared memory
- automata models and Petri nets

Topics

1. Formal justification of a proof system for Communicating Sequential Processes (B/M)
2. A Compositional Proof System for Shared Variable Concurrency (B/M)
3. Generative Operational Semantics for Relaxed Memory Models (M)
4. Compositional Modeling Formalisms for Hard and Softly Timed Systems (B/M)
5. Semantics of Petri Nets (B/M)
6. Model checking for weakly consistent libraries (M)

The Topics

Pointers and Objects

Goal

Analysing pointer-manipulating programs

- shape analysis
- extension by concurrency
- reduced calculi

Topics

1. Compositional Shape Analysis (B/M)
2. Concurrent separation logic I (M)
3. Concurrent separation logic II (M)
4. Featherweight Java (B/M)

The Topics

Software Verification

Goal

Formal methods for ensuring and proving correctness of software

- programs with arrays
- reachability analysis
- test generation
- ruling out undefined program behaviour

Topics

1. Property Checking Array Programs Using Loop Shrinking (M)
2. Software Verification with Property-Directed Reachability (B/M)
3. Parser-Directed Fuzzing (B/M)
4. Analyzing undefined behavior of C programs (B/M)

The Topics

Reliability, Privacy and Security

Goal

Approaches for addressing specific aspects of HW/SW systems

- failure behaviour
- privacy
- security

Topics

1. Semantics of dynamic fault trees (B/M)
2. State/event fault trees (B/M)
3. Programming language techniques for differential privacy (B/M)
4. Verification of information-flow security (B/M)

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.

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!