Aspects of Quantitative Program Verification

Kick-off Meeting

Benjamin Lucien Kaminski

UNIVERSITÄT DES SAARLANDES

SS 2022, April 25, Universität des Saarlandes, Germany

Part I

Organizational Matters

Attendance Check

Please stand by. . .

Objectives of the Seminar

Objectives:

- Independent Understanding: "deciphering" a scientific paper authored by others
- Scientific Writing: Writing your own scientific report
- Presentation Skills: Giving a comprehensible scientific presentation
  to an educated and critical audience

Deliverables:

- Outline + 1 (draft) page of main part of the report
- Final report
- Presentation

Outline + 1-Pager

- What it is *not*: “1. Introduction 2. Main Part 3. Conclusion”
- What *is* expected:
  1. Detailed overview of the structure of the report
     - Section headers
     - Main definitions and theorems
  2. One (draft) page of the “main part” of the report
     - *Optional: Submit an entire draft report!*
- Of course, $\boxed{1}$ and $\boxed{2}$ can be combined in one document
- Helps *you* to sort your thoughts, tell a coherent story;
  helps *me* to see whether you’re on track and give you early feedback

The Report

Report: Objectives

- Replicate (not copy!) (main aspects of) the paper you've been assigned
  - Read and understand the paper
  - Develop an intuition for the theory
  - If needed: search, read, understand further background literature
  - Reformulate the main aspects of the paper/topic in your own words
    - Reformulate the theory in your own words
    - Describe *your* intuition of the theory
    - Find and describe more (any) examples than the original paper
    - Discuss advantages/shortcomings of the theory
- You did an excellent job if your report is
  more comprehensible than the original paper!

Report: Formalities

- Format:
  - Max. 10 pages, excluding bibliography
  - ACM proceedings format, see acmart-pacmpl-template.tex
  - More details will be provided on the website
- Cite (correctly) all consulted literature
- No plagiarism! Copying text blocks (from literature, internet, . . .) without source indication (citation) causes immediate failure of seminar
- Language: English or German (but you'll find that English is easier)
- I expect correct grammar and spelling
  - ≥ 10 gross errors per page is unacceptable and
    causes me to discontinue reading your outline / (preliminary) report

The Presentation

Presentation: Objectives

- Explain your paper / your report /your intuition in a comprehensive manner to us!
- Prepare your presentation for the audience!
- Prepare descriptive slides
  - Not too much text on one slide
  - Use graphical illustrations wherever possible
  - Use colors (if they make sense)
- Don't have spelling mistakes on your slides
- Finish your presentation on time. Overtime is bad!
- Prepare for expected questions (have slide numbers, have backup slides if need be)
- You did an excellent job if everybody understood what you were talking about!

Presentation: Formalities

- 30 minutes presentation + 10 minutes Q&A
- (hopefully) in-person
- Dates: 1 or 2 days in beginning of August (tentative, TBA on website)
- More details will be provided on the website
- Attending all presentations is mandatory!

Timeline & Bidding

Timeline

25.4. Kick-off Meeting

27.4. † **Bidding for Topics**

29.4. † Announcement of student-topic assignment

16.5. † Last chance to drop out (via LSF, not via email to me!)

27.5. † **Outline & 1-pager due**

1.7. † **Final report due**

18.7. † *Optional: Preliminary presentation slides draft due*

TBA.8. **Final presentations**

- Attending *all* presentations is mandatory

Missing any non-optional deadline causes immediate failure of the seminar.

The Bidding Procedure

today Me: I give you a short teaser on all available topics

27.4. † Each of you: Glance at papers that sparked your interest today.
Send me an email indicating:

1 paper that is first priority (your absolute favorite)

2 papers that are your second priority (still quite excited about)

3 papers that are your third priority (not excited, but still good)

3 papers that you absolutely *don't* want (OMG no way in hell!)

- every other paper will be treated as *neutral*

29.4. † Me: I announce student-topic assignment on the website

- No guarantee for an optimal assignment

30.4.–1.5. All of us: Have a good weekend!

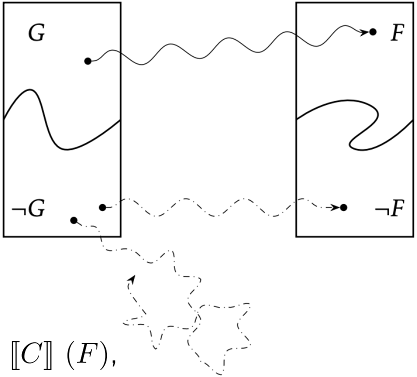
from 2.5. You: Start working the seminar

Part II

Topics

Generalized Hoare Logics and Predicate Transformers

Hoare Logics and Predicate Transformers



Predicate G, F: States $\rightarrow \{\text{true, false}\}$

Hoare triple $\langle\, G \,\rangle \; C \; \langle\, F \,\rangle$

- Executing program C on initial state $\sigma \models G$ terminates in a final state $\tau \models F$

Weakest precondition wp $[\![C]\!]\ (F)$

- Weakest / largest / “most true” predicate $G = \text{wp}\ [\![C]\!]\ (F)$, such that Hoare triple $\langle\, G \,\rangle \; C \; \langle\, F \,\rangle$ is valid

Generalized Hoare Logics and Predicate Transformers

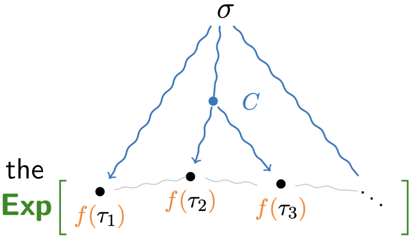
- Replace predicates by objects that map to a more general domain than $\{\text{true, false}\}$, for instance $\mathbb{R}$.

Generalized Hoare Logics Predicate Transformers

Quantity $f\colon \text{States} \to \mathbb{R}_{\geq 0}^{\infty}$

Example: Weakest preexpectation wp $\llbracket C \rrbracket\ (f)$

- wp $\llbracket C \rrbracket\ (f)$: States $\to \mathbb{R}_{\geq 0}^{\infty}$ maps initial state σ to the expected value of f after executing C on σ



Generalized Hoare Logics Predicate Transformers (Topics)

- *Atkinson & Carbin.* Programming and Reasoning with Partial Observability
- *Batz et al.* Weighted Programming — A Programming Paradigm for Specifying Mathematical Models
- *Kaminski et al.* Weakest Precondition Reasoning for Expected Run-Times of Probabilistic Programs **(BA)**
- *Batz et al.* Relatively Complete Verification of Probabilistic Programs: An Expressive Language for Expectation-based Reasoning **(BA)**
- *Klinkenberg et al.* Generating Functions for Probabilistic Programs **(BA)**
- *McIver & Morgan.* Correctness by Construction for Probabilistic Programs **(BA)**

Incorrectness Reasoning

Incorrectness Logic and Predicate Transformers

Incorrectness triple $[\,\varphi\,]\;C\;[\,\psi\,]$

- Every final state $\tau \models \psi$ is reachable by executing C on some initial state $\sigma \models \varphi$

Strongest postcondition $\mathsf{sp}\,[\![C]\!]\,(\varphi)$

- Strongest / smallest / "least true" predicate $\mathsf{sp}\,[\![C]\!]\,(\varphi)$,
  such that incorrectness triple $[\,\varphi\,]\;C\;[\,\psi\,]$ is valid

Used for bug finding: ψ is a bug and we would like to find out whether the bug / ψ can be reached

Generalized Predicate Transformers

- Again, replace predicates by objects that map to a more general domain

Incorrectness Reasoning (Topics)

- *O'Hearn.* Incorrectness Logic. **(BA)**
- *Zhang & Kaminski.* Quantitative Strongest Post —
  A Calculus for Reasoning about the Flow of Quantitative Information **(BA)**

Lower Bounds on Least Fixed Points

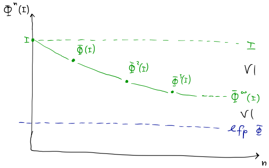
Lower Bounds on Least Fixed Points

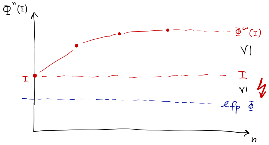
- Semantics of loops often characterized as lfp of some suitable function Φ
- Examples:
  - Weakest precondition wp $[\![\texttt{while}\,(\,\varphi\,)\,\{\,C\,\}]\!]\ (\psi) = \text{lfp}\ \Phi$
  - Weakest preexpectation: Expected value of a random variable after termination of a randomized loop
- Upper bounds have "easy" induction rule:

$$\Phi(I) \ \preceq\ I \qquad \text{implies} \qquad \text{lfp}\ \Phi\ \preceq\ I$$

- What about lower bounds?

$I \ \preceq\ \Phi(I)$ ~~implies~~ $I\ \preceq\ \text{lfp}\ \Phi$

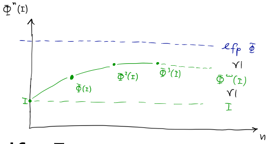




Lower Bounds on Least Fixed Points (Topics)

- What about lower bounds?

$$I \;\preceq\; \Phi(I) \qquad \text{~~implies~~} \qquad I \;\preceq\; \mathsf{lfp}\ \Phi$$



- Solution:

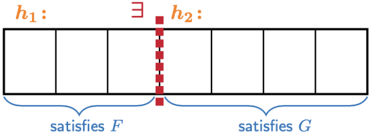
$$I \;\preceq\; \Phi(I) \quad \bigwedge \quad \begin{matrix}\text{some}\\ \text{side}\\ \text{conditions}\end{matrix} \qquad \text{implies} \qquad I \;\preceq\; \mathsf{lfp}\ \Phi$$

- *Hark et al.* Aiming Low Is Harder: Induction for Lower Bounds in Probabilistic Program Verification
- *Baldan et al.* Fixpoint Theory — Upside Down

Separation Logic

Separation Logic

- Reasoning about dynamic memory / heap
- Classical conjunction: $F \wedge G$
  - Entire heap satisfies specification F
  - AND entire heap satisfies specification G
- Separating conjuntion: $F \star G$
  - Heap can be separated into two disjoint parts h_1 and h_2, such that
    - heap part h_1 satisfies specification F
    - AND heap part h_2 satisfies specification G
  - Enables local reasoning!



Separation Logic (Topics)

- *Reynolds.* Separation Logic: A Logic for Shared Mutable Data Structures **(BA)**
- *Batz et al.* Quantitative Separation Logic:
  A Logic for Reasoning about Probabilistic Pointer Programs **(BA)**
- *Barthe, Hsu, & Liao.* A Probabilistic Separation Logic
- *Bao et al.* A Bunched Logic for Conditional Independence
- *Bao et al.* A Separation Logic for Negative Dependence

Probabilistic Programming

Probabilistic Programming

- “Normal” programs with random coin flips
- Often: sampling from continuous distributions
- Used not as a *randomized algorithm* but as a *description of a statistical model*
- Difficult to give semantics to

Probabilistic Programming (Topics)

- *Lee et al.*
  Towards Verified Stochastic Variational Inference for Probabilistic Programs
- *Vákár, Kammar, & Staton.*
  A Domain Theory for Statistical Probabilistic Programming

Conditioning in Probabilistic Programming

Conditioning in Probabilistic Programming

- Program describes a probability distribution
- Observations block certain undesired traces
  - Example:

```
$x$ := $0$ ;
while ( $c = 1$ ) {
    { $c$ := $0$ } [$1/2$] { $x$ := $x + 1$ }
} ;
observe $x$ even
```

- Probability mass of the *desired* traces should be renormalized according to the total mass of desired traces
- Difficult to give semantics to!
  - Observing events of probability 0, nontermination, . . .

Conditioning in Probabilistic Programming (Topics)

- *Jules Jacobs.* Paradoxes of Probabilistic Programming: And How To Condition on Events of Measure Zero with Infinitesimal Probabilities
- *Baudart et al.* Reactive Probabilistic Programming
- *Jacobs.* The Mathematics of Changing One's Mind, via Jeffrey's or Pearl's Update Rule

Neural Networks

Tropical Geometry of Neural Networks

- "Normal" / High School Algebra
  - $+$ The usual addition: $1 + 2 = 3$
  - $\cdot$ The usual multiplication: $2 \cdot 3 = 6$
  - 0 The number 0 we all know: $0 + 3 = 3$
  - 1 The number 1 we all know: $1 \cdot 3 = 3$
- Tropical algebra
  - $\oplus$ The maximum operation: $1 \oplus 2 = \max\{1, 2\} = 2$
  - $\otimes$ The usual addition: $2 \otimes 3 = 2 + 3 = 5$
  - $\mathbf{0}$ Negative infinity: $\mathbf{0} \oplus 3 = \max\{-\infty, 3\} = 3$
  - $\mathbf{1}$ The number 0 we all know: $\mathbf{1} \odot 3 = 0 + 3 = 3$
- *Zhang, Naitzat, & Lim.* Tropical Geometry of Neural Networks

Part III

Final Thoughts

Final Thoughts

- Be thorough: Allow a good amount of time to really understand the literature
- Be proactive: Look for additional literature;
  contact me well in advance if you foresee any trouble meeting a deadline, . . .
- Be social: Discuss your report / paper with other students
- Be prepared: Prepare meetings with your supervisor well
- Be realistic: Don’t expect that you can
  prepare a presentation or a report in a day or two
- Be assured: I wish you all good luck and success for this seminar! $\ddot\smile$

Final remark: I am looking for PhD students!!!