Advances in Model Checking

Introduction

Winter Semester 2016/17; 27 October, 2016

C. Dehnert, S. Junges, J.P. Katoen, T. Lange, T. Quatmann, M. Volk

Software Modeling and Verification Group

RWTH Aachen University

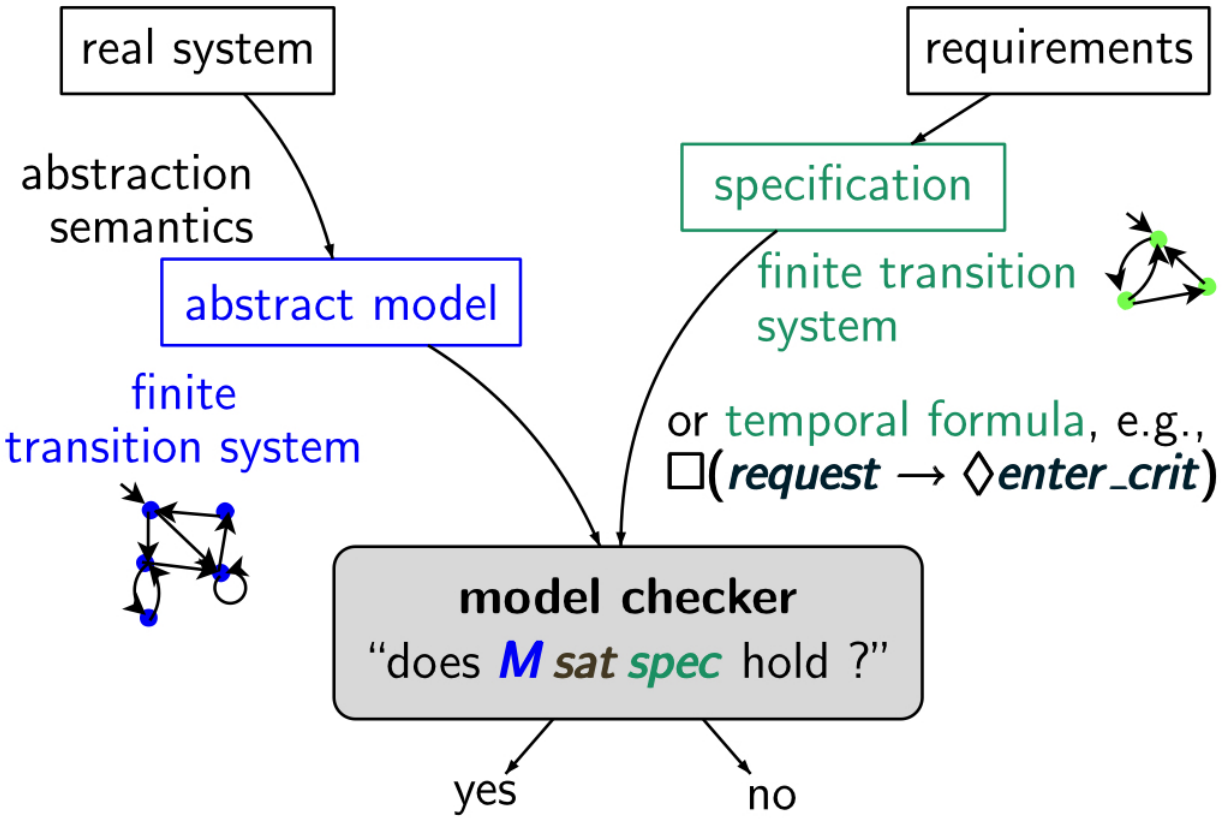
`https://moves.rwth-aachen.de/teaching/ws-1617/amc/`

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

Outline

Model Checking



Outline

Aims of this Seminar

Goals

Aims of this seminar

Independent understanding of a scientific topic

Acquiring, reading and understanding **scientific literature**

Writing of your **own report** on this topic

Oral presentation of your results

Aims of this Seminar

Requirements on Report

Your report

Independent writing of a report of $\approx$ **15 pages**

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

Report **template** will be made available on seminar web page

Aims of this Seminar

Requirements on Talk

Your talk

Talk of about **45 (= 40 + 5) minutes**

Focus your talk on the **audience**

Descriptive slides:

- $\leq$ 15 lines of text
- use (base) colors in a useful manner

Language: German or English

No spelling mistakes please!

Finish **in time**. Overtime is bad

Ask for **questions**

Final Preparations

Preparation of your talk

Setup laptop and projector **ahead** of time

Use a (laser) **pointer**

Number your slides

Multiple **copies**: laptop, USB, web

Have **backup slides** ready for expected questions

Outline

Important Dates

Deadlines

21 Nov: Detailed outline of report due

19 Dec: Report due

09 Jan: Presentation slides due

16/17 Jan: Seminar

Important Dates

Deadlines

21 Nov: Detailed outline of report due

19 Dec: Report due

09 Jan: Presentation slides due

16/17 Jan: Seminar

Missing a deadline causes **immediate exclusion** from the seminar

Selecting Your Topic

Procedure

You obtain(ed) a list of topics of this seminar.

Indicate the preference of your topics (first, second, third).

Return sheet by Wednesday (02 Nov.) via e-mail/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 website by Thursday.

Then also your **supervisor** will be indicated.

Selecting Your Topic

Procedure

You obtain(ed) a list of topics of this seminar.

Indicate the preference of your topics (first, second, third).

Return sheet by Wednesday (02 Nov.) via e-mail/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 website by Thursday.

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

Topics

C. Dehnert

Topic 1

Counterexample-Guided Abstraction Refinement

Topic 2

Automated Assume-Guarantee Reasoning by Abstraction Refinement

Topics

S. Junges

Topic 3

An $\mathcal{O}(m \log(n))$ Algorithm for Stuttering Equivalence and Branching Bisimulation

Topic 4

Fairness for Infinite-State Systems

Topics

J.P. Katoen

Topic 5

Bounded model checking

Bounded model checking (BMC) is a powerful bug-hunting technique.

Is applied to hard- and software.

Its basis is to consider paths up to a certain depth k.

The transition system is encoded as Boolean formula.

Modern SAT solvers are applied to check for counterexamples.

Generalizations for liveness and arbitrary depths k do exist.

Topics

T. Lange

Topic 6

Configurable Software Verification

Configurable SW Verification:

- Static Analysis (SA) and Verification reducible to each other
- SA knows generic algorithm for decades
- Won Goedel medal ”for their contributions to the development of efficient verification methods and algorithms”

Adjustable Block Encoding

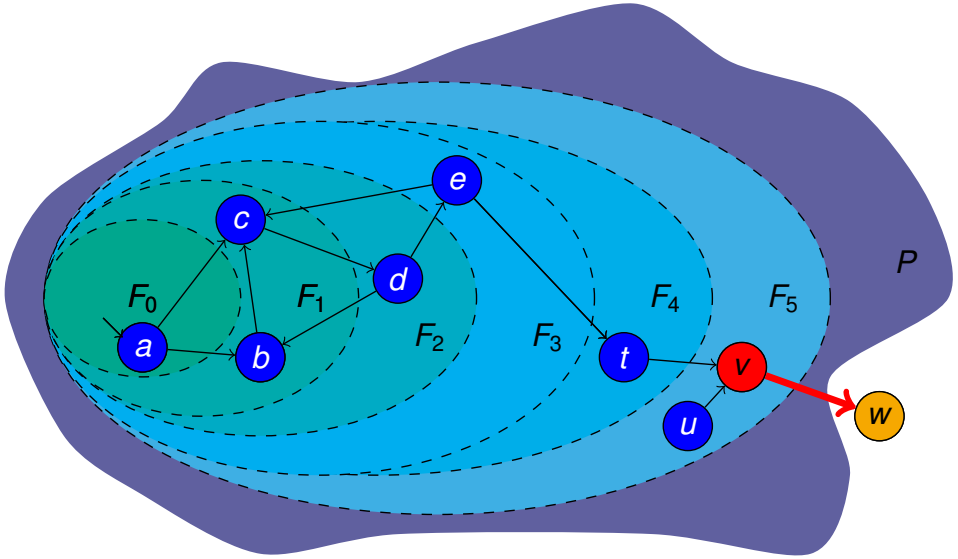
- CEGAR hampered by large programs, especially sequences
- Simplify program by folding sequences *[Beyer et al. 2009]*
- Folding until minimality sometimes not very efficient, follow spirit of CPA and make it adjustable

T. Lange

Topic 7

Pushing to the Top

Consider the transition system $\mathcal{M} = (X, I, T)$ and the prop. $P(X)$.



Topics

T. Quatmann

Topic 8

Lazy Probabilistic Model Checking without Determinisation

Given: Markov chain $\mathcal{M}$, LTL formula φ
Goal: compute the probability that φ holds in $\mathcal{M}$

Classic Approach:

1. get NBA $\mathcal{B}$ for $\neg\varphi$
2. determinise $\mathcal{B} \rightsquigarrow$ DRA $\mathcal{A}$
3. analyse $\mathcal{M} \otimes \mathcal{A}$

Problem: determinisation of $\mathcal{B}$ is expensive
Idea: consider simpler constructions for determinisation

Subset Construction: fast, can yield an inconclusive answer
Breakpoint Construction: slower, might also be inconclusive
Multi-Breakpoint Construction: very slow, always conclusive

Topics

M. Volk

Topic 9

Monte Carlo Model Checking

Scalable and applicable for large systems

Idea: Instead of complete state space only consider parts

Randomly sample paths

If path is counterexample: property not satisfied

Else: sample more paths

Result: confidence that property is safisfied

Topics

M. Volk

Topic 10

Concurrent depth-first search algorithms based on Tarjan's Algorithm

- Tarjan's algorithm used for finding strongly connected components (SCCs)
- Crucial in model checking
- DFS which tries to find backward edges to already visited nodes
- Idea: utilise multi-core processors
- Lift algorithm to concurrent algorithm

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!