Course syllabus

Faculty of Technology

Department of Computer Science and Media Technology

4DV701 Formella metoder, 5 credits
Formal methods

Main field of study
Computer Science

Subject Group
Informatics/Computer and Systems Sciences

Level of classification
Second Level

Progression
A1F

Date of Ratification
Approved by Faculty of Technology 2018-10-08
The course syllabus is valid from autumn semester 2019

Prerequisites
4DV650 Systems modeling and simulation, 5 credits

Objectives

After completing the course the student shall be able to:

- Reason about what safety and security means for a software program or system, and which properties are required,
- describe methods and challenges to formally verify safety and security properties of software systems and what limitations these methods have,
- describe the stateof the art of formal methods and verification,
- describe how runtime-monitoring can be used to enforce security and safety requirements,
- define safety properties in concurrent systems and programs using different types of logic,
- use different methods to verify the correctness, safety, and security of modelled and implemented systems,
- use the most common tools to describe and verify software systems and programs,
- reason about the societal impact (including socio-economical costs) caused by faulty and in-secure software can cause and how formal methods can be used to

reduce this impact.

Content

The course gives an introduction to formal verification and introduces, e.g., temporal logic.

The following topics are covered:

- Introduction to formal verification.
- Classification of different verification techniques.
- Process algebra (CCS), and how it can be extended with time delays.
- Timed automata
- Propositional and predicate logic, and temporal logic (LTL, CTL)
- Programming languages semantics
- Program verification using Hoare logic and separation logic
- LTL and CTL model checking
- Runtime monitoring

Type of Instruction

The instruction consists of lectures, seminars, and teacher-supervised laboratory sessions. The course also contains a series of guest lectures where representatives from industry and research discusses how and why they use formal verification in their work, including which methods and tools.

Examination

The course is assessed with the grades A, B, C, D, E, Fx or F.

The grade A constitutes the highest grade on the scale and the remaining grades follow in descending order where the grade E is the lowest grade on the scale that will result in a pass. The grade F means that the student’s performance is assessed as fail (i.e. received the grade F).

Assessment of student performance is made through formal verification of a software program (written assingments), formal verification of a systems model (written assignments) and a written exam. Students who do not pass the regular examination will be offered retrials close to the regular examination.

To pass the course, grade E or higher is required for all parts. The final grade is decided from: formal verification of a software program (written assingments) (20%), formal verification of a systems model (written assignments) (20%), and written exam(60%).

Course Evaluation

During the course or in close connection to the course, a course evaluation is to be carried out. The result and analysis of the course evaluation are to be communicated to the students who have taken the course and to the students who are to participate in the course the next time it is offered. The course evaluation is carried out anonymously. The compiled report will be filed.

Other

Grade criteria for the A–F scale are communicated to the student through a special document. The student is to be informed about the grade criteria for the course by the start of the course at the latest.

The course is conducted in such a way that the course participants' experiences and knowledge are made visible and developed. This means, for example, that we have an inclusive approach and strive for no one to feel excluded. This can be expressed in different ways in a course, for example by using the gender neutral example.

Required Reading and Additional Study Material

Luca Aceto, Anna Ingólfsdóttir, Kim Guldstrand Larsen och Jiri Srba, *Reactive Systems: Modelling, Specification and Verification*, Cambridge University Press, latest edition. Pages: 150 av 281.

Michael Huth, och Mark Ryan, *Logic in Computer Science: Modelling and Reasoning about Systems*, Cambridge University Press, latest edition. Pages: 300 av 412.

- Compendium of Scientific Articles.