Formal Methods:
Automated Reasoning & Formal Verification
Ch. 00: **Course Overview**

Roberto Sebastiani

DISI, Università di Trento, Italy – roberto.sebastiani@unitn.it
URL: https://disi.unitn.it/rseba/DIDATTICA/fm2023/
Teaching assistant: Giuseppe Spallitta – giuseppe.spallitta@unitn.it

M.S. in Computer Science, Mathematics, & Artificial Intelligence Systems
Academic year 2022-2023

last update: Friday 24th February, 2023, 10:12

Outline

Legal Notice

Important:

Please be aware that all classes are video-recorded (including students' questions & speeches) and that the recordings will be made available online.

Target

- The course is given in English.
- For students of M.S. “Computer Science” and “Mathematics”:
  “Formal Methods” is split into two consecutive modules:
  Module 1: Automated Reasoning [6CFU]
  Module 2: Formal Verification [6CFU]
- For students of M.S. “Artificial Intelligence Systems”:
  the above modules are mutuated respectively into the courses:
  - Automated Reasoning [6CFU]
  - Formal Verification [6CFU]
- These courses are open to whoever may be interested
  - in particular to PhD students of IECS school

Timetable

Timetable:

2^{nd} Semester, February 28^{th} – June 7^{th}

- CLASS: Tuesday 08.30-11.30 Room A110 (Povo 1)
- LAB: Wednesday 11.30-13.30 Room A110 (Povo 1)
- CLASS: Thursday 09.30-11.30 Room A110 (Povo 1)

The course is given in presence. Recordings of the classes will be made available (see later).

Office Hours & Forum

Office hours:

- No weekly fixed-day
- Anytime in the week, upon appointment only
- In presence (only after class) or via zoom
- Appointments to be set in class or via email
- Office hours only during class period (see above)!

Forum

A forum for Q&A is available at the course page in the Moodle platform

Note: You must register to Moodle!

Important: Email Communications

Important

Teaching this course is only part of our job, and we receive a huge amount of email. Thus:

- email for relevant reasons only
- email to both me and the teaching assistant
- use as subject "[Formal Methods]: ⟨*subject*⟩"
  (or "[Automated Reasoning/Formal Verification]: ⟨*subject*⟩")
- email only from your "official" UNITN email address "name.surname@studenti.unitn.it"
  - emails coming from any other source address will be ignored
- be polite and respectful, with both me and the T.A.
  (see e.g. "Bad Email Reply – What not to say to your professor"

PS: Notice that even professors use social media (example)

Outline

Motivations & Goals

- Automated reasoning & formal verification methods are increasingly used
  - as backend engines for many AI applications (e.g., planning, KR)
  - and backend engines for many NP-hard problems (e.g., criptanalysis, circuit designs,...)
  - as powerful specification, verification and early debugging methods in the development of industrial SW and HW systems.
- The course will concentrate on
  - Automated Reasoning (AR)
  - Formal verification (FV), with particolar attention to Model Checking (MC) technology
- A laboratory will be given in which the students will experience
  - the usage of AR techniques (SAT, SMT)
  - the usage of MC techniques (NuXMV)

Topics

Automated Reasoning

The main topics covered in the course/module are (not necessarily in order):

- Boolean Reasoning & Propositional Satisfiability (SAT)
- Ordered Binary Decision Diagrams
- Modern SAT Solving (CDCL)
- Extended SAT Functionalities
- Satisfiability Modulo Theories (SMT)
- Extended SMT Functionalities
- Temporal logics: LTL, CTL and CTL*
- Automated reasoning in Temporal Logics (LTL, CTL)
- Noteworthy Applications

Note: Depending on various circumstances, the covered topics might be subject to variations.

Topics (cont.)

Formal Verification

The main topics covered in the course/module are (not necessarily in order):

- Formal specification & formal validation
- Formal Representation of Systems
- Model Checking (MC): generalities
- Explicit-State MC and Symbolic MC
- CTL MC
- LTL MC
- SAT-based MC,
- abstraction in MC (hints)
- MC with Timed and Hybrid Systems

Note: Depending on various circumstances, the covered topics might be subject to variations.

Topics (cont.)

Laboratory:

- SAT solvers
- SMT/AR solvers
- The MC NuXMV

References

Both Automated Reasoning and Formal Verification courses/modules:

- Notes from the lessons
- Slides (available from the URL of the course)
- Other material (available from the URL of the course)

Formal Verification course/module only:

- The NuXMV manual
- Suggested books (in alternative):
  - *Edmund Clarke, Orna Grumberg and Doron Peled*.
    "Model Checking"
    MIT Press
  - *Christel Baier and Joost-Pieter Katoen* .
    "Principles of Model Checking"
    MIT Press

Acknowledgements

Some of the material presented in these slides (text, figures) is courtesy of the following people, listed in alphabetical order:

- Massimo Benerecetti (bene@na.infn.it)
- Alessandro Cimatti (cimatti@fbk.eu)
- Paritosh Pandya (pandya@tifr.res.in)
- Marco Pistore (pistore@fbk.eu)
- Marco Roveri (marco.roveri@unitn.it)
- Stefano Tonetta (tonettas@fbk.eu).

Furthermore, some examples are taken from the book:
[E. Clarke, O. Grunberg & D. Peled, “Model Checking”, MIT Press]

Role of Video Recordings

Disclaimer

Class video recordings are not mandatory for teachers. Nevertheless, I have decided to go on providing the recordings of classes, which will be available from both my personal web page and, in mode convenient form, from the Moodle platform. This said, I wish to clarify the following facts.

- There is no guarantee on the quality of video-recording (in particular of the audio), nor on the full coverage of the class period. (It has happened in the past that some pieces of the class got lost due to technical problems.)
- Video recordings just display slides with teacher voice on background. To this extent, they are not meant to cover any text written on the blackboard.
- When students ask questions, they may or may not be recorded in the recording, depending on the position of the microphone.

Remark

- Video recordings are not meant to substitute classes. Rather, they are intended to provide some "extra support" to students, who may want to listen again some part of interest
- From previous exam resultss, there is a clear correlation between exam success and class attendance in presence.

Requirements

- It is assumed some basic background in the following topics:
  - basic mathematics
  - algorithms and data structures
  - programming
- Some background in the following topics could be useful (but not strictly necessary):
  - Boolean logic
  - automata and formal languages
  - software engineering

Exam

Formal Methods module 1 & 2 – 12 CFU (M.S. in Computer Science or M.S in Mathematics)

2 parts:

- Script
  - lab test
  - the script test, on the topics of the course
- Oral Interview
  - interview on the topics of the course.

Automated Reasoning or Formal Verification – 6 CFU (M.S. in Artificial Intelligence Systems)

2 parts:

- lab test
- the script test, on the topics of the course

People from AIS M.S. willing to take both Automated Reasoning and Formal Verification (6+6 CFU) can alternatively take the Formal Methods exam for both.

- the same vote will be given to both courses

To copy at exams very dangerous is!