Formal Methods:
Automated Reasoning & Model Checking
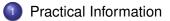## Ch. 00: **Course Overview**

Roberto Sebastiani

DISI, Università di Trento, Italy – roberto.sebastiani@unitn.it
URL: http://disi.unitn.it/rseba/DIDATTICA/fm2021/
Teaching assistant: Giuseppe Spallitta – giuseppe.spallitta@unitn.it

M.S. in Computer Science, Mathematics, & Artificial Intelligence Systems
Academic year 2020-2021

last update: Tuesday 13th April, 2021, 13:53

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 will be 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: Model Checking [6CFU]
- For students of M.S. "Artificial Intelligence Systems":
  the above modules are mutuated respectively into the courses:
    - Automated Reasoning [6CFU]
    - Model Checking [6CFU]
- These courses are open to whoever may be interested
    - in particular to PhD students of ICT school

Timetable

Timetable:

2nd Semester, March 1st – June 11th

- CLASS: Tuesday 08.30-11.30 Room A205 (Povo 1)
- LAB: Wednesday 11.30-13.30 Room B106 (Povo 2)
- CLASS: Thursday 09.30-11.30 Room A205 (Povo 1)

The course is given in "mixed" remote/in presence modality (a.k.a. "blended"), 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*⟩"
- email only from your "official" UNITN email address "name.surname@studenti.unitn.it"
- 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

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

Topics

Automated Reasoning

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

- Boolean Reasoning & Propositional Satisfiability (SAT)
- Ordered Binary Decision Diagrams
- Modern SAT Solving (CDCL)
- Extended SAT Functionalities
- First-Order Automated Reasoning
- Satisfiability Modulo Theories (SMT)
- Extended SMT Functionalities
- Automated-Reasoning in Modal & Description Logics (hints)
- Noteworthy Applications

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

Topics (cont.)

Model Checking

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

- Formal specification & formal validation
- Formal Representation of Systems
- Model Checking (MC): generalities
- Temporal logics: LTL, CTL and CTL*
- 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 Model Checking courses/modules:

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

Model Checking 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

Disclaimer

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@disi.unitn.it)
- Marco Roveri (roveri@fbk.eu)
- Stefano Tonetta (tonettas@fbk.eu).

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

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 Model Checking – 6 CFU each
(M.S. in Artificial Intelligence Systems)

2 parts:

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

To copy at exams very dangerous is!

Outline

Remote attendance & Lesson Recordings

- Due to the handling of the COVID-19 pandemic, and modulo further different decisions, the course classes will be given in "mixed" remote/in presence modality (a.k.a. "blended"):
  - for a restricted number of students, in turn, it will be possible to follow the class physically in the classroom following the safety access protocols
  - for everybody else it will be possible to follow the classes remotely in synchronous modality, via the Zoom platform
- Classes will be video-recorded, the recordings will be made available at the URL of the course
- Zoom links are available at the course page in the Moodle platform

Notice: Safe Behaviour for COVID-19 at DISI

The following rules are STRICT

All students are always supposed:

- to access DISI only if personally autorized (via the UNITN app)
- to follow the access rules:
    - to check-in/check-out with the app
    - to follow the paths
- to wear a mask, covering both mouth and nose
- to sanitize hands when both entering and exiting classes
- to respect inter-personal safety distance ($\geq 1m$)
- to access/exit rooms one at a time, respecting safety distances
- to sit only on admissible and available seats
- after breaks, to sit in the same seats as before the break
- ...

Notice: Safe Behaviour for COVID-19 at DISI [cont.]

- ...
- not to enter the classroom after the class has begun
- not to exit the class before the class has finished
- to minimize movements inside the classroom
- to bring only indispensable material with them
- to bring a backup mask (latex gloves might be of help)
- to avoid any exchange of personal items
- to avoid putting items in the intermediate empty seats/desks
- ...

Notice: Safe Behaviour for COVID-19 at DISI [cont.]

What if...

- If a student feels sick at home, in particular with flu/COVID-like symptoms, he/she must stay at home!
- If a student feels sick in classrooms, in particular with flu/COVID-like symptoms:
  - he/she (and classmates) must immediately notify the teacher
  - he/she must immediately leave the room and move to outside the porter, avoiding any contact $\implies$ he/she will be taken care of
  - classmates must stay away from him/her and not touch him/her without safety gloves
- if a student who has previously attended classes is found positive to COVID, he/she must immediately inform DISI

Remark

If a student willingly refuses to comply to the rules (e.g., to wear a mask) the teacher is supposed to take his/her data and to call the DISI COVID19-safety responsible, who is supposed to call the police. (No kidding!)

Marsellus Wallace doesn't like students who don't wear masks...

©"Pulp Fiction", by Q. Tarantino