CSCI-699: Theory and Algorithms for Formal Verification

Units: 4
Spring

Location: TBD

Instructor: Jyotirmoy (Jyo) V. Deshmukh
Office: SAL 340
Office Hours: 11am to 12pm on Fridays
Contact Info: Email: jyotirmoy.deshmukh@usc.edu,
[Response within 24 hours]

Course Description

Complex software systems are everywhere. How do we reason about the correctness of software programs, from distributed message-passing programs to shared-memory concurrent programs to autonomous cyber-physical systems? The area of formal verification provides you with tools that allow you to express the correctness of software programs in a mathematically precise fashion and algorithms that can check for correctness, often with minimal human intervention or input.

This course will provide you with the necessary background to reason about topics such as correctness of sequential and concurrent programs, safety of autonomous cyber-physical systems including those that use AI, and core ideas from requirement formalisms based on temporal logic and automata theory. We will examine the theory and algorithms for formal verification in discrete software programs as well as hybrid and nonlinear continuous dynamical systems. This course is meant to be a depth course that focuses on the theoretical considerations for concurrent/distributed programs, timed and probabilistic systems, and hybrid and nonlinear dynamical systems.

Learning Objectives and Outcomes

- Gain familiarity with formal verification
- Get acquainted with automata over infinite length words and trees, timed automata and hybrid automata
- Learn how to analyze the complexity of verification algorithms
- Learn about temporal logic
- Understand the theoretical and practical challenges of applying formal verification techniques in practice

Recommended Preparation:

a) CSCI 270, 570
b) CSCI 610 (Preferred but not required)

Course Notes:

Course Structure. In this course, most of the teaching will be accomplished through lectures. In addition, we will have 4 written homework assignments through the semester, and a final exam.

Technological Proficiency and Hardware/Software Required

None required.

Required Readings and Supplementary Materials

The course will cover material from the following textbooks:

1) Principles of Model Checking by Christel Baier and Joost Pieter Katoen, MIT Press
2) Verifying Cyber-Physical Systems by Sayan Mitra, MIT Press
3) Principles of Cyber-Physical Systems by Rajeev Alur, MIT Press

Some lectures will cover material from expository survey papers, and will be made available on the course website.

Description and Assessment of Assignments
There will be 4 written assignments that will test the theoretical understanding of the techniques and algorithms introduced. Homeworks will be fun challenge problems that encourage collaboration among students. Final will be a take-home open-book test.

Grading Breakdown

Category		**Points**	**% of Grade**
Homeworks	HW1	100	20
	HW2	100	20
	HW3	100	20
	HW4	100	20
Final Exam		100	20
TOTAL			100

Grading Scale (Example)
Course final grades will be determined roughly using the following scale
A 90-100
A- 85-89
B+ 80-84
B 75-79
B- 70-74
C+ 65-69
C 60-64
F 59 and below

Assignment Rubrics
1. Homework assignments and exams will be graded for correctness of answers and provided explanation/proofs. Partial credit will be given wherever applicable.
2. The class will use Slack for online discussions related to the concepts covered in the class. Students will be expected to ask and answer questions during in-class lectures and participate in discussions on Slack.

Assignment Submission Policy
Assignments are expected to be turned in to the instructor/TA by 11:59.59pm Pacific Time on the deadline. There will be a 5% penalty for every late day for 7 days. Assignments submitted 7 days after the deadline will be returned with a zero grade.

Grading Timeline
Graded assignments will be returned to students in a time period not exceeding 2 weeks from the submission of the assignment.

Course Schedule: A rough weekly Breakdown
Please see up-to-date schedule at:
https://jdeshmukh.github.io/teaching/cs699-theory-of-fv-spring-2022/schedule.html

	Topics/Daily Activities	Deliverable/ Due Dates
Week 1	Course overview, Pre-history of verification (Floyd, Hoare, and Dijkstra)	
Week 2	Modeling concurrent/distributed systems as labelled transition systemsords	
Week 3	Linear Temporal Logic and Automata on Inifite Words	HW1 posted
Week 4	Computation Tree Logic and Tree Automata	
Week 5	Mu-calculus and Model checking	
Week 6	Trace Equivalences, Counterexamples, Abstraction-Refinement	HW2 posted
Week 7	Ameliorating State Explosion	
Week 8	Timed Automata and Verification	
Week 9	Metric Temporal Logic and Signal Temporal Logic	HW3 posted
Week 10	Probabilistc Systems: Markov chains, Markov Decision Processes, Probabilistic Timed Automata, Continuous-Time Markov Chains	
Week 11	Probabilistic CTL, Probabilistic/Stochastic Bisimulations, and Prob. Model Checking	
Week 12	Nonlinear Dynamical Systems	HW4 posted
Week 13	Verification for Hybrid and Continuous Dynamical Systems: Reachability analysis	
Week 14	Simulation-guided Reachability Analysis and Deductive Methods	
Week 15	Verifying neural network-based systems, Data-driven verification	
Finals Week		Final Exam (Take Home)

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in SCampus in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

Support Systems:

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention and Services (RSVP) - (213) 740-9355(WELL), press "0" after hours – 24/7 on call
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED)- (213) 740-5086 | Title IX – (213) 821-8298
equity.usc.edu, titleix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants. The university prohibits discrimination or harassment based on the following *protected characteristics*: race, color, national origin, ancestry, religion, sex, gender, gender identity, gender expression, sexual orientation, age, physical disability, medical condition, mental disability, marital status, pregnancy, veteran status, genetic information, and any other characteristic which may be specified in applicable laws and governmental regulations. The university also prohibits sexual assault, non-consensual sexual contact, sexual misconduct, intimate partner violence, stalking, malicious dissuasion, retaliation, and violation of interim measures.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office of Equity and Diversity |Title IX for appropriate investigation, supportive measures, and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.