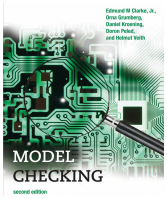

CISC 849.012: Model Checking

University of Delaware, Spring 2021

Syllabus

All information here is subject to change. Changes will be announced in class and on Canvas.

1. Fundamentals

Class meeting times: 3:30–4:45 PM, Tue/Thu from Tuesday, Feb. 16 to Tuesday, May 18, except Tuesday, March 30. Total number of classes: 26.

How class meets: This is an online synchronous class. Class meetings will take place via Zoom: `https://udel.zoom.us/j/99436778197`. You must authenticate through UD to join the meeting.

What you need: No special equipment is required. Only a reasonable desktop or laptop computer with a camera and microphone, a good, stable internet connection, and a quiet and safe place where you can work while participating in the class meetings.

Instructor: Stephen Siegel, `siegel@udel.edu`. Office hours: 10:45–11:45 AM, Tuesday through Thursday, or by appointment, via Zoom: `https://udel.zoom.us/j/97146059059`. Note the Zoom ID for my office hours is not the same as the ID for the class meetings.

Course Canvas page: `https://udel.instructure.com/courses/1567225`. The name of the site is `21S-CISC849-012`. Canvas will be used for class notes and grades.

Slack workspace: `https://modelchecking.slack.com`. To sign up, go to `https://join.slack.com/t/modelchecking/signup`. We will use Slack for asynchronous discussion of material and to ask and answer questions. Do not use Slack for discussion involving any confidential information, such as your grades or academic record—for these things, use email, phone, or Zoom conference.

Text: Model Checking, 2nd ed., by Edmund M. Clarke, Orna Grumberg, Daniel Kroening, Doron A. Peled, and Helmut Veith, MIT Press, 2018. There is no need to buy the book, since the UD library has reserved an electronic version of it here: `https://delcat.on.worldcat.org/oclc/1176304629`. (You must be logged on to the UD VPN to access this resource.) However, you may want to buy it since it is an excellent reference that will remain relevant for many years to come.

2. Course Abstract

Model checking is like testing, but taken to a radical new level: rather than checking the correctness of a single program run, one specifies, in a formal language, all possible correct behaviors, and then uses a model checker to confirm that all executions of the program conform to the specification. Model checking can be applied to parallel programs, networking or communication protocols, hardware designs, distributed algorithms, blockchain-based "smart contracts," and even biological systems. It is widely used throughout industry and the public sector, especially for systems where failure is not an option. Microsoft, Amazon, Intel, and NASA are some of the many organizations with active model checking teams.

Model checking was introduced in 1981 and quickly became a standard tool for verifying the correctness of integrated circuit designs. Shortly thereafter, researchers began extending the approach to verify software. Today, numerous companies involved in the production of complex software systems use model checking as a standard part of their development process.

The only pre-requisite is CISC 220 (Data Structures) or a similar course; all other background material will be covered in the course itself. The course will largely follow the excellent text

of Clarke et al., supplemented with material on the Spin model checker. Students will become proficient users of Spin for verifying the correctness of concurrency protocols and other problems, and will gain a firm understanding of the theoretical underpinnings of model checking.

3. Topics

Here is an approximate ordered list of topics we will cover, subject to change:

(1) Introduction: motivation, history, context. Chapters 1–2.
(2) Chapter 3: Modeling Systems
(3) Chapter 4: Temporal Logic
(4) The Spin model checker
(5) Chapter 7: Automata on Infinite Words and LTL Model Checking
(6) Chapter 12: Partial Order Reduction (POR)
(7) Chapter 9: Propositional Satisfiability (maybe)
(8) Chapter 10: SAT-based Model Checking (maybe)

The purpose of this strange order is to go deep fast. This will quickly give you an in-depth understanding of one specific model checking approach—automata-based LTL model checking with POR, which is the basis of Spin.

4. How this Class Will Operate

It's all about the book. I will assign some reading for each class. You should read the assigned sections carefully before class. It is very important that you take notes while reading. Reading should be an active process where you figure things out, write things down in a way that makes sense to you, note any points of confusion, create some examples of your own that clarify points in the text, etc. If you do these things, you will always be prepared for class.

During class, I will lead the discussion on the material read. I might present some slides and talk through them, or write notes, ask questions, or work out problems. I expect all students to participate in the discussion. Participation can involve: asking questions, perhaps about something in the reading that didn't make sense to you, answering questions, clarifying a point, talking about an example of your own, and so on. Interrupt me whenever you want.

In addition we will keep a class log on Canvas Pages. Entries may be solutions to problems, examples, clarifications of confusing points in the book, notes on errors in the book, references to related work, an original picture or diagram illustrating an idea, or any other relevant observations. Everyone is expected to make contributions to the log.

Finally, the last 3 weeks or so of the semester, each student will give a presentation on some topic of their choice. It could be on a section of the book we haven't read yet, a paper, an extended example or application you have worked out, or something else. I will list some options or you can submit an idea to me for approval. You should prepare a 25 minute presentation with slides. The slides will be submitted to me a week in advance so I can give you some feedback before you present. We will aim for 2 presentations per meeting.

5. Grading

Your grade will be 50% participation and 50% final project.

For an A participation grade, you should speak up approximately twice in each class, on average, and make something like two contributions to the log each week. These are rough guidelines. I will let you know how your participation is going at the 1/4, 1/2, and 3/4 marks through the semester so you can adjust as necessary.

The project grade will be based on the clarity and organization of your presentation, originality (your personal take on some of the ideas, an original example to illustrate a point, clarifications, etc.), the quality of your slides or notes, and the depth of your understanding of the material you present. I will give you plenty of feedback before you present on all of these points.

There is no curve or competition for grades and I would be perfectly happy if everyone earned an A.

Students auditing the class must fully attend at least 21 of the 26 meetings to receive a listener-pass grade.

6. Academic honesty

Copying any other person's work (off the Internet, for example) without proper acknowledgment is **plagiarism**, a serious offense, and will result in charges filed in accord with the University's Policy on Academic Honesty. If you do use someone else's work, (e.g., an example in your project presentation, or an image on a slide you copied from someone's web site), **be sure to acknowledge the source** fully and precisely.