ECE.653
STQAM

Software Testing, Quality Assurance, and Maintenance

Fall 2023

Prof. Arie Gurfinkel

UNIVERSITY OF WATERLOO

University of Waterloo Territorial Acknowledgement

The University of Waterloo acknowledges that much of our work takes place on the traditional territory of the Neutral, Anishinaabeg and Haudenosaunee peoples. Our main campus is situated on the Haldimand Tract, the land granted to the Six Nations that includes six miles on each side of the Grand River. Our active work toward reconciliation takes place across our campuses through research, learning, teaching, and community building, and is co-ordinated within the Office of Indigenous Relations.

Anishinaabeg
"anish-nah-beg"

Haudenosaunee
"hoe-den-no-show-nee"

UNIVERSITY OF WATERLOO

https://uwaterloo.ca/indigenous/

Instructor and TA

Instructor

- Prof. Arie Gurfinkel

Teaching Assistants

- Roberto Emmanuel Valenzuela Armenta <revalenzuelaarmenta@uwaterloo.ca>
- Siddharth Priya siddharth.priya@uwaterloo.ca
- Haifeng Shi <haifeng.shi@uwaterloo.ca>

Course Web Page

- https://ece.uwaterloo.ca/~agurfink/stqam
- LEARN: https://learn.uwaterloo.ca/d2l/home/935816
- Campuswire: https://campuswire.com/p/G2011444A with code: **8854**

Instructor (me)

Prof. Arie Gurfinkel
@prof arie

TA: Roberto Emmanuel Valenzuela Armenta

"I'm Roberto Valenzuela doing a MASc in ECE with a "Computer Software" specialization. I'm doing research in the Real-Time Embedded Software Group working on a fuzzing tool that helps to detect undocumented commands and backdoors on embedded systems by using side-channel analysis. Before starting grad school, I developed firmware that did electrical validation of a new generation power inverter for John Deere.

TA: Siddharth Priya

Siddharth Priya is a PhD student working with Professor Arie Gurfinkel. His research interest is in program verification. Before embarking for graduate studies, Siddharth spent thirteen years in the software industry working in various software systems from web frontends, developer tools to embedded firmware.

TA: Haifeng Shi

Hi everyone! I am Haifeng, a second-year master student in ECE. My research is in Static Program Analysis and Software Verification. I have taken ECE653 and TA ECE453 before, look forward to discussing interesting topics with you!

Course Time and Location

Date: Monday, Friday

Location: E7 5343

Time:

- 11:30AM – 12:50 PM

Grading

Assignments: 35%

Final Exam: 50%

Project: 15%

Grades may be curved or adjusted at the Instructor's discretion

Assignments

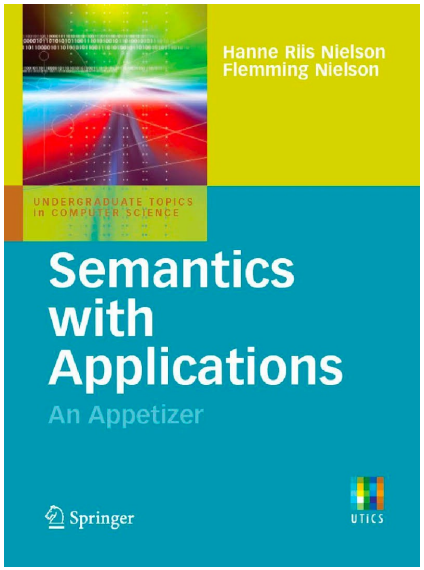
- Pen and paper exercises, and
- Programming assignments
  - mostly in Python

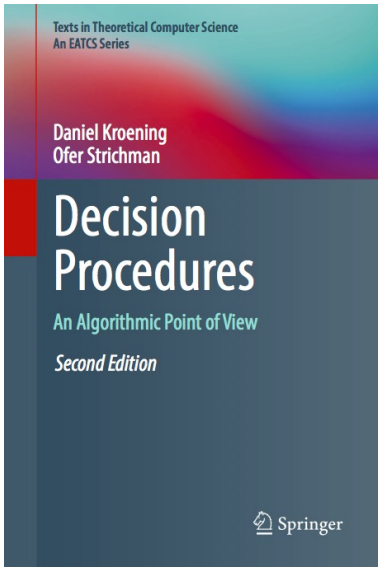
Details in the syllabus:
https://ece.uwaterloo.ca/~agurfink/stqam/syllabus.html

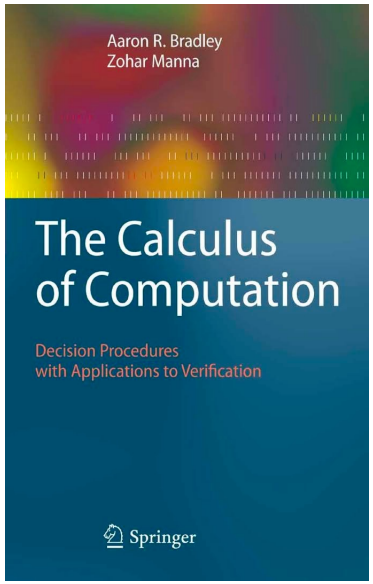
Textbook and Lecture Notes

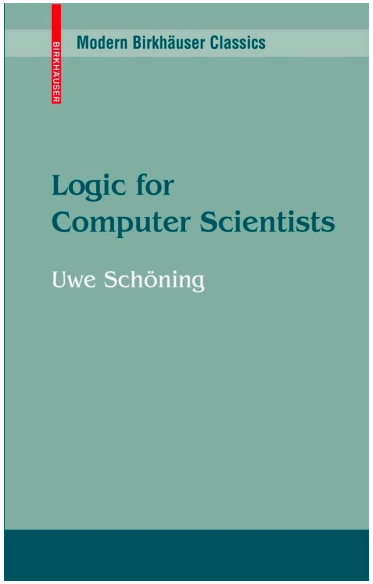
No required text book. Lecture slides and notes will be provided.

- https://ece.uwaterloo.ca/~agurfink/stqam
- LEARN: https://learn.uwaterloo.ca





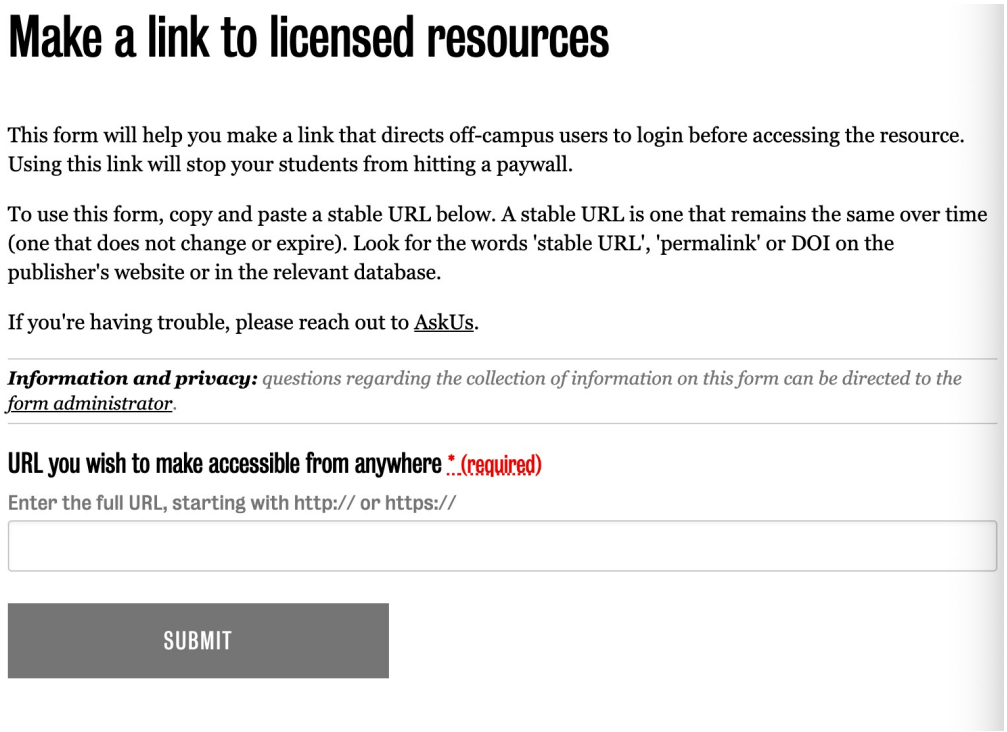




Accessing External Resources

https://uwaterloo.ca/library/make-link

Let's you access resources that are only available through university while you are at home!



Make a link to licensed resources

This form will help you make a link that directs off-campus users to login before accessing the resource. Using this link will stop your students from hitting a paywall.

To use this form, copy and paste a stable URL below. A stable URL is one that remains the same over time (one that does not change or expire). Look for the words 'stable URL', 'permalink' or DOI on the publisher's website or in the relevant database.

If you're having trouble, please reach out to AskUs.

Information and privacy: *questions regarding the collection of information on this form can be directed to the form administrator.*

URL you wish to make accessible from anywhere * (required)

Enter the full URL, starting with http:// or https://

SUBMIT

Course Website & LEARN

The course website is the definitive source

- When in doubt, consult the web page
- Check syllabus for final grade computation

YOUR responsibility to check for updates!

- Course website
- LEARN (http://learn.uwaterloo.ca)

Campuswire

We will use campuswire as our main communication medium

On campuswire you can

- Ask questions of me or our TAs
- Post questions to be seen by everyone
- Answer questions of other students
- Create group and private chat rooms

To join the course on campuswire, use link and code posted on LEARN (or earlier in this slide deck)

Independent Work

All work turned in must be of that individual student unless stated otherwise.

Violations will result in zero credit to all students concerned. University of Waterloo Policy 71 will be followed for any discovered cases of plagiarism.

Policy on Late Assignments

You have 2 days of lateness for assignments that you can use throughout the term

- These are TWO days for the term. Not for each assignment!

Each day the assignment is late consumes one day of lateness

For example,

- You can be 2 days late on assignment A1, or
- One day late on A1, and one day late on A3, or
- You can hand all the assignments on time ☺

Is this course for me?

Not a TESTING course!

- Foundations of Testing / Coverage
- Foundations of Symbolic Execution and Symbolic Reasoning
- Foundations of Deductive Program Verification
- (Possibly) Foundations of Automated Verification

Enough background?

- Can you code? (Python?) https://docs.python.org/2.7/tutorial/
- Have you used a Unix/Linux machine before?
  - command line, shell, editor…
- Do you know Logic / Automated Reasoning?
  - Propositional logic: AND, OR, NOT, Boolean SATisfiability
- Do you have a basic understanding of how compilers work?
  - Control Flow Graphs, Operational Semantics, Intermediate Representation
- Have you used a SAT / Theorem Prover / Constriant Solver / SMT ?

Contact

Office Hours

- by appointment
- best time is before/after lectures

Email (email address on the course web page)

- https://ece.uwaterloo.ca/~agurfink/stqam
- Identify yourself
  - Originated from your uwaterloo email address, or
  - Signed with your full name and student ID
- Start **Subject** of email with **[STQAM]**

Use Campuswire

A little about me

2007, PhD University of Toronto

2006-2016, Principle Researcher at Software Engineering Institute, Carnegie Mellon University

Sep 2016, Associate Professor, University of Waterloo

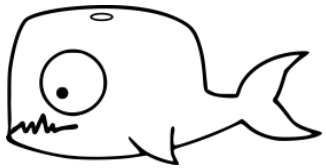
వింత

UFO

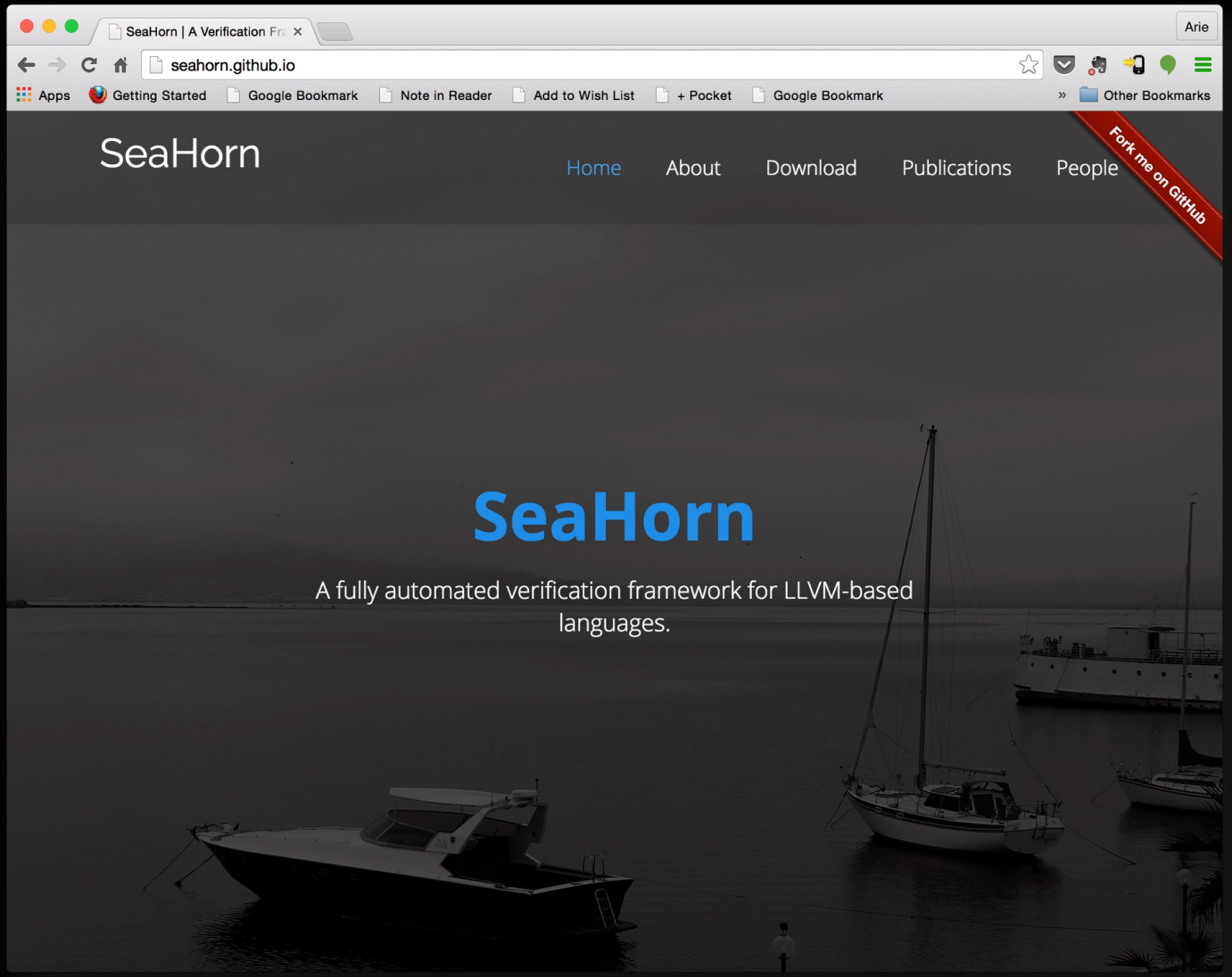
FrankenBit

SPACER

Avy



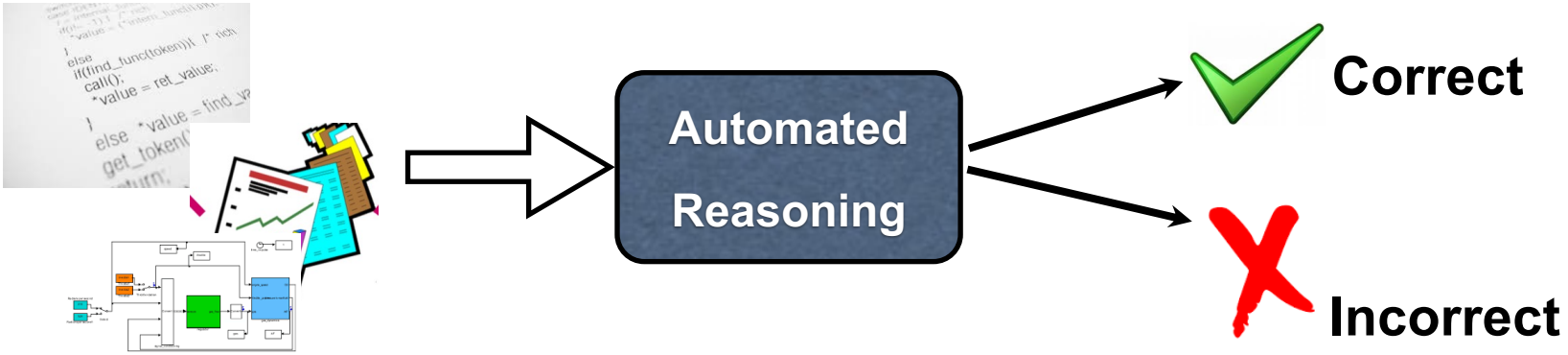
SeaHorn



http://seahorn.github.io

Automated (Software) Verification

Program and/or model

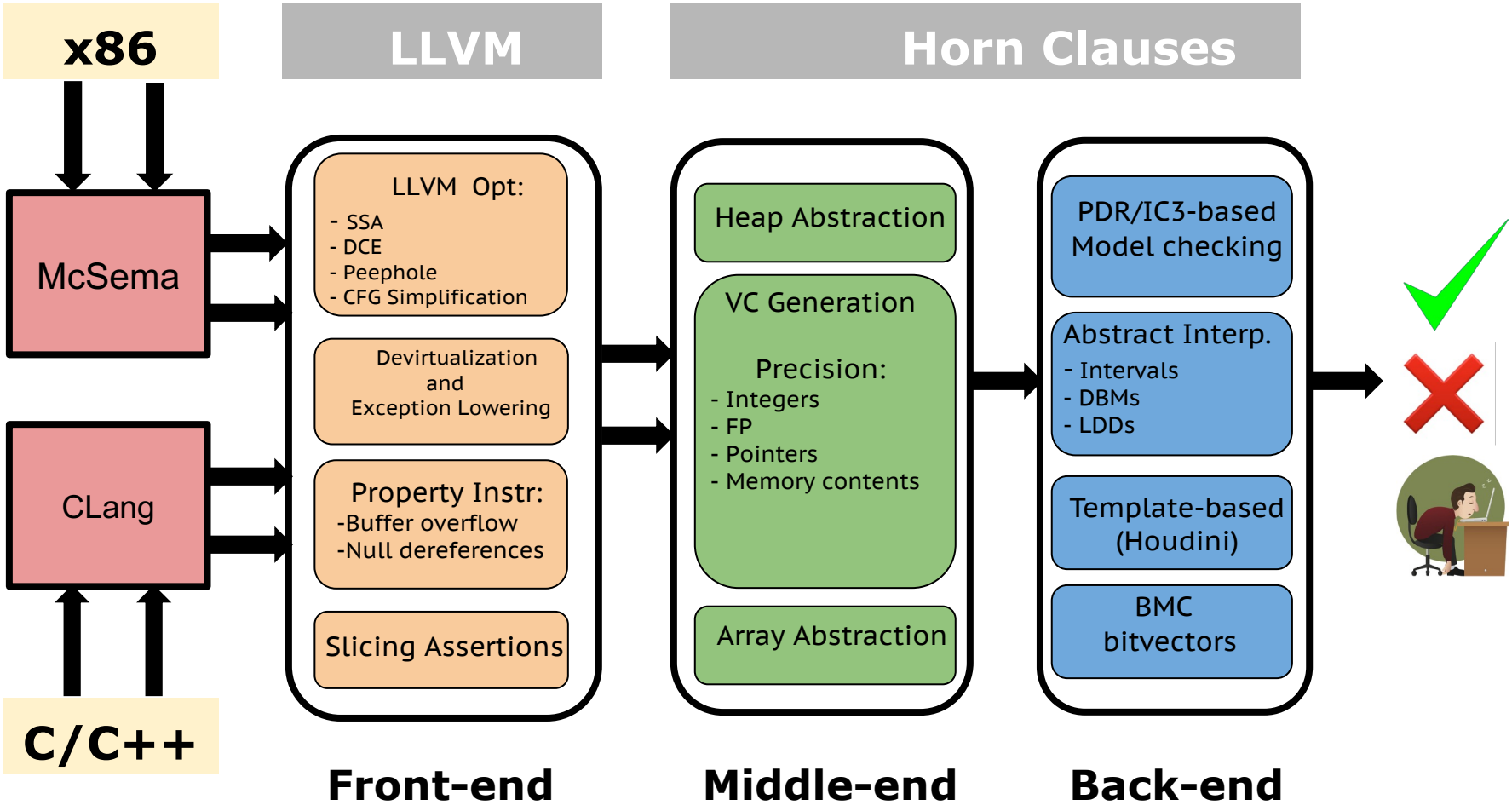


Alan M. Turing. 1936: “Undecidable”

Alan M. Turing. ”Checking a large routine” 1949

How can one check a routine in the sense of making sure that it is right?

programmer should make a number of definite assertions which can be checked individually, and from which the correctness of the whole programme easily follows.


x86
LLVM
Horn Clauses
McSema
CLang
C/C++
LLVM Opt:
- SSA
- DCE
- Peephole
- CFG Simplification
Devirtualization
and
Exception Lowering
Property Instr:
-Buffer overflow
-Null dereferences
Slicing Assertions
Heap Abstraction
VC Generation
Precision:
- Integers
- FP
- Pointers
- Memory contents
Array Abstraction
PDR/IC3-based
Model checking
Abstract Interp.
- Intervals
- DBMs
- LDDs
Template-based
(Houdini)
BMC
bitvectors
Front-end
Middle-end
Back-end