Proposal for a CPSC 448 on Formal Verification

When: 2023W2 (aka. "now") **Who:** Mark Greenstreet will be the faculty supervisor. Plan is to have a group of about five students in the 448.

Overview:

Formal verification is a standard part of digital hardware design. Advances in SAT solvers, SMT solvers, and theorem provers have enabled a growing impact of formal methods in industrial software development. For example, there are large verification groups at Amazon, Microsoft, and many other leading technology companies. Following up on an interest expressed in Honours Seminar, I (Mark Greenstreet) am proposing a small group CPSC 448 for 2023W2.

The first half of the term will focus on giving students hands-on experience with two verification tools: the ACL2 theorem prover, and the Z3 SMT solver. The students will be encouraged to install these tools on their computers and work through their respective tutorials. For ACL2, we will use the Introduction to the theorem prover. For Z3, we will use the Z3 Python API and associated tutorial tutorial. During this time, we will meet weekly to discuss examples and challenges with these tools. We will also discuss roughly one paper a week on the topics of SAT solvers, SMT solvers, theorem provers, model checkers, and their applications. I will come up with a list of about 10 papers, and we'll follow the interests of the group to determine which ones to cover. I will be happy to append a draft reading list to this proposal upon request.

The second half of the term will branch out to other examples of tools while continuing to read and discuss papers. The tools that I have in mind include:

The Concurrency Workbench (from Galois).

Coq, a theorem prover widely used in the programming languages community.

Something on dependent types:

- I'll invite William Bowman to lead the group for one or two weeks, or he might appoint one of his students to join us.

Lean, a theorem prover by the author of Z3.

Viper and separation logic

- I'll invite Alex Summers to lead the group for one or two weeks, or he might appoint one of his students to join us.

During this time, students in this 448 will do individual or partner projects to explore one uses of one of these tools, or to delve deeper into applications of ACL2 and/or Z3 from the start of the term.

This course will introduce students to key concepts of formal verification: this is mainly computability theory, algorithms, and heuristics. All of these will be motivated by real-world examples and hands-on use of real-world tools.

Grading will be based on completing the tutorials, participating and presenting in the paper discussions, and the projects undertaken in the second half of the semester.