THE CATHOLIC UNIVERSITY OF AMERICA

Department of Electrical Engineering and Computer Science

# Spring 2023 Seminar

## Ms. Katherine L. Kosaian

*Computer Science Ph.D. Program, Carnegie Mellon University*

## *"Formal Verification and Real Quantifier Elimination"*

**Thursday, January 26th, 2023**

**11:15 AM – 12:30 PM, Scullen Room**

*(All are welcome to attend)*

**Abstract:** Algorithms that are used in safety-critical settings (i.e., settings where errors can cause great financial loss or, in the worst case, loss of life) need to be highly trustworthy. Formally verifying an algorithm in a theorem prover—by first translating the algorithm into a rigorous logical setting and then providing rigorous associated proofs of correctness—allows us to achieve a high degree of trustworthiness. My work focuses on formally verifying algorithms for real quantifier elimination. Real quantifier elimination problems arise in important application domains, including the verification of cyber-physical systems and motion planning, which makes their correctness crucial. Unfortunately, efficient verified support for quantifier elimination is currently lacking, which necessitates the use of unverified software to resolve quantifier elimination problems that are relevant to safety-critical applications.

In this talk, I will detail my work on verifying two algorithms for real quantifier elimination, with a focus on the underlying mathematical intuition and the verification challenges. The first main result is the formal verification of the virtual substitution algorithm. This algorithm is incomplete in the sense that it is capable of solving only certain quantifier elimination problems, but it has the potential for very high efficiency and is widely used by unverified software to great practical benefit. We experimentally tested our verified algorithm, comparing its performance to that of several existing unverified tools on 423 benchmarks from the literature; our experiments also revealed correctness bugs in some of the existing tools. The second main result is the formal verification of a complete algorithm (that is, an algorithm which is capable of solving all quantifier elimination problems). Formalizations of complete quantifier elimination algorithms are quite rare, as these algorithms tend to be mathematically intricate. Our work identifies a perceived tradeoff between the computational complexity of an algorithm and its amenability to verification—that is, the most practical algorithms are also the most difficult to verify—and aims towards a potential sweet-spot within this tradeoff.