Formalizing mathematics, ft. Isabelle/HOL.

Katherine Kosaian (Iowa State University)

Many mathematical algorithms are used in safety-critical contexts. Correctness of these algorithms, and the mathematical results underlying them, is crucial. In formal methods, a piece of software called a theorem prover can be used to formally verify algorithms. In this approach, code for an algorithm is accompanied by a rigorous proof of correctness that only depends on the logical foundations of the theorem prover. Algorithms that have been verified in this way are highly trustworthy and thus safe for use in safety-critical applications.

The theorem prover Isabelle/HOL is well-suited for formalizing mathematics. This talk will motivate formalized mathematics, exhibit how mathematics is formalized in Isabelle/HOL, and discuss the challenges that may arise, with a focus on three different use cases: 1) verifying algorithms for real quantifier elimination, 2) verifying Coppersmith's method, 3) verifying Pick's theorem.