Abstract:

For the past 40 years computer scientists generally believed that NP-complete problems are intractable. In particular, Boolean satisfiability (SAT), as a paradigmatic NP-complete problem, has been considered to be intractable. Over the past 20 years, however, there has been a quiet, but dramatic, revolution, and very large SAT instances are now being solved routinely as part of software and hardware design.

In this talk I will review this amazing development and show that we can leverage SAT solving to accomplish other Boolean reasoning tasks. Counting the number of satisfying truth assignments of a given Boolean formula or sampling such assignments uniformly at random are fundamental computational problems in computer science with numerous applications. While the theory of these problems has been thoroughly investigated in the 1980s, approximation algorithms developed by theorists do not scale up to industrial-sized instances. Algorithms used by the industry offer better scalability, but give up certain correctness guarantees to achieve scalability. We describe a novel approach, based on universal hashing and Satisfiability Modulo Theory, that scales to formulas with hundreds of thousands of variables without giving up correctness guarantees.