Candidate: Benjamin Kiesl
Supervisors: Martina Seidl and Hans Tompits
Reviewers: Olaf Beyersdorff (Friedrich-Schiller-University Jena) and Christoph Weidenbach (Max-Planck-Institute for Informatics, Saarbrücken)
Title: Structural Reasoning Methods for Satisfiability Solving and Beyond

Abstract:
Automated-reasoning tools have various applications in artificial intelligence and formal verification, ranging from the detection of bugs in software and hardware to the solution of long-standing mathematical problems. In this thesis, we present automated-reasoning methods that modify the syntactic structure of logical formulas. In particular, we deal with formulas from propositional logic and first-order logic as well as with quantified Boolean formulas.

In the first part of the thesis, we introduce so-called redundancy properties that characterize cases in which formulas can be modified without affecting their satisfiability or unsatisfiability. Based on some of these redundancy properties, we then define new strong proof systems for propositional logic. As we demonstrate, these proof systems are not only highly expressive but also well-suited for automation. Harnessing their advantages, we define a satisfiability-solving paradigm that generalizes the well-known conflict-driven clause learning (CDCL) paradigm by pruning the search space more aggressively. In an empirical evaluation, we show that a solver based on our paradigm can solve formulas that are—due to theoretical evaluation—too hard for ordinary CDCL solvers.

In the second part of the thesis, we lift several popular redundancy properties from propositional logic to first-order logic. Many of these redundancy properties have been successfully used in satisfiability solving but it was unclear if they could be lifted to first-order logic. We lift them in a uniform way by introducing the principle of implication modulo resolution, which is a generalization of so-called quantified implied outer resolvents known from the theory of quantified Boolean formulas. Using these redundancy properties, we then define corresponding clause-elimination techniques and analyze their confluence properties in detail. To illustrate their practical usefulness, we implemented and evaluated a preprocessing tool that boosts the performance of theorem provers by eliminating blocked clauses from first-order formulas.

Finally, we show how satisfiability-preserving formula modifications can be used to clarify the relationship between two important proof systems for quantified Boolean formulas—the long-distance-resolution calculus and the QRAT proof system. Recently, it has been shown that long-distance resolution is remarkably powerful both in theory and in practical QBF solving. It was, however, unknown how long-distance resolution is related to QRAT, a proof system introduced for certifying the correctness of QBF-preprocessing techniques. We show that QRAT polynomially simulates long-distance resolution.