Formalization of Logic in the Isabelle Proof Assistant

Isabelle is a proof assistant, i.e. a computer program that helps its user to define concepts in mathematics and computer science as well as to prove properties about them. This process is called formalization. Proof assistants aid their users by ensuring that proofs are constructed correctly and by conducting parts of the proofs automatically. A logical calculus is a set of rules and axioms that can be applied to construct theorems of the calculus. Logical calculi are employed in e.g. tools for formal verification of computer programs. Two important properties of logical calculi are soundness and completeness, since they state, respectively, that all theorems of a given calculus are valid, and that all valid statements are theorems of the calculus. Validity is defined by a semantics, which gives meaning to formulas. This thesis describes formalizations in Isabelle of several logics as well as tools built upon these. Specifically this thesis explains and discusses the following contributions of my PhD project:

• A formalization of the resolution calculus for first-order logic, Herbrand’s theorem and the soundness and completeness of the calculus.
• A formalization of the ordered resolution calculus for first-order logic, an abstract prover based on it and the prover’s soundness and completeness.
• A verified automatic theorem prover for first-order logic. The prover is a refinement of the above formalization of an abstract prover. This explicitly shows that the abstract notion of a prover can describe concrete computer programs. • The Natural Deduction Assistant (NaDeA), which is a tool for teaching first-order logic that allows users to build proofs in natural deduction. The tool is based on a formalization of natural deduction and its soundness and completeness.
• A verified proof assistant for first-order logic with equality. It is based on an axiomatic system and constitutes a tool for teaching logic and proof assistants.
• A formalization of the propositional fragment of a paraconsistent infinite-valued higherorder logic. Theorems about the necessity of having infinitely many truth values are proved and formalized. Proof assistants are built to reject proofs that contain gaps or mistakes. Therefore, the formalized results are highly trustworthy. The tools based on formalized calculi consequently have an increased trustworthiness. The above formalizations revealed flaws and mistakes in the literature. In addition to the formalizations and tools themselves, my PhD project contributes solutions that repair these flaws and mistakes.