Report on the doctoral thesis
Some problems concerning lengths of proofs
by Pavel Hrubeš

The thesis is devoted to the study of the complexity of proofs in various logical calculi. It is divided into two parts of two chapters each, where every chapter is concerned with questions concerning one type of logical system, with the chapters in each part being closely related.

Chapter 1 deals with systems of first order arithmetic, in particular extensions of Peano arithmetic, and studies Kreisel's conjecture for these systems. This conjecture states for a sytem T that if all instances of a universal statement have proofs in T of bounded length, then the general statement is provable as well. Whether this holds for Peano arithmetic itself is a well-known open problem. Here it is shown that it fails for certain extensions of Peano arithmetic. It is known that for this it is sufficient to show that all true equations of the form $k \cdot n = m$ have proofs of bounded length. This is shown to hold for several extensions of Peano arithmetic.

Chapter 2 studies calculi for classical propositional logic with an axiom or rule of identity, that allows substitution of equivalent subformulas. The relation with Chapter 1 is that this makes propositional formulas behave similar to terms in a first-order system. An upper bound on the number of proof lines in these systems for any tautology is shown that depends only on the number of variables. Non-constant lower bounds for these and related sytems are shown, and these are compared in strength with respect to a newly introduced simulation relation suitable for studying constant bounds on the number of proof lines.

Chapter 3 and 4 deal with systems of modal and intuitionistic propositional logic, respectively. The issue studied in both cases is the length of proofs in the systems in question, on which exponential lower bounds are proven. The technique used for showing these lower bounds is *monotone interpolation*, which allows to reduce the problem to the known lower bounds on the size of monotone boolean circuits.

In Chapter 3, a monotone interpolation theorem is proven and applied to prove exponential lower bounds for various systems of modal logic, namely the systems known as K, K_4, Gödel-Löb logic, S and S_4. On the other hand, short proofs in the system $K_{4,5}$ are constructed for one of the modal tautologies considered, implying an exponential speed-up of this system over those mentioned above. The results can either be obtained as lower bounds on the number of applications of modal rules in general, or with a little additional effort more sharply as bounds on the number of applications of one particular modal rule, the distributivity rule.

Chapter 4 presents a monotone interpolation theorem and the following exponential lower bounds for intuitionistic propositional logic, either formulated as a Gentzen sequent calculus or as a Hilbert-style axiom system. These results can either be obtained directly by methods similar as those employed in Chapter 3, or be reduced to results in Chapter 3 via a translation of intuitionistic into modal logic.

With the exception of the upper bounds in Chapter 2, which were known before (the author acknowledges this), the theorems proven in this thesis are new and valuable scientific results. In particular, the results of Part II (Chapters 3 and 4) constitute in my view important contributions to the field of proof complexity, and the methods employed there offer the potential to be useful for the study of the complexity of further logical calculi. The main theorem of Chapter 4 especially, the lower bound for intuitionistic sequent calculus, gives the solution to a major open problem in the area, to which various researchers had devoted some effort.

The results in Part I are, while still interesting, more marginal in my opinion. Nevertheless, Chapter 1 provides some progress towards understanding Kreisel's conjecture, and generally the role of terms played in formal arithmetical proofs.

The presentation of the thesis could be improved in some places, but overall the writing is clear, concise and understandable.

Summarizing, I think the submitted thesis shows conclusively that the author is able to perform and communicate original scientific work, and I recommend to accept it as a docoral thesis and grant the doctoral degree.

München, 29. 11. 2007

[redacted]