Comparing Mathematical Proofs*

Stefan Hetzl

Institut für Computersprachen (E-185),
TU-Vienna, Favoritenstraße 9,
1040 Vienna, Austria
hetzl@logic.at

August 22, 2006

The notion of proof has been introduced to mathematics by the ancient Greeks: A theorem is to be established by general, abstract reasoning. But for one and a single theorem there might exist more than one, and *different* proofs. For example, C.F. Gauss gave eight different proofs of the quadratic reciprocity theorem. From this one-to-many relation of a theorem to its proofs, the following question of the philosophy of mathematics arises naturally:

What is the relation between the different proofs of one theorem ?

This question is amenable to mathematical analysis: The systematic study of mathematical proof methods with *mathematical means* has been initiated by D. Hilbert: In proof theory, systems for formalizing mathematical proofs are studied. Questions from the philosophy of mathematics concerning properties of proofs can thus be made mathematically precise by speaking not about proofs, but instead of formal derivations (in such a system). The additional possibilities for a mathematically precise analysis come at the price of restricting oneself to a certain formal system.

In this talk we treat first-order sequent calculus, basically as introduced by G. Gentzen in [2]. The reasons for choosing this system is that - on the one hand - it is powerful enough to formalize not only toy examples but proofs of real mathematical interest but - at the same time - it is simple enough to allow a doable analysis.

In order to approach the question mentioned above we build on the notion of *characteristic clause set* that has been introduced in [1]. We adapt this notion with the aim of using a variant of characteristic clause sets for the comparison of proofs: For a given derivation we construct a pair of charac-

*supported by the Austrian Research Fund (project no. P17995)

teristic clause sets. This pair contains two dual components of which the first gives an account of the logical material taken from the *theorem* and the other of that taken from the *lemmata* to build the derivation.

We propose this pair of characteristic clause sets as a general framework for the analysis of questions concerning the similarity and equality of proofs formalized as first-order derivations. We show that this pair has the following remarkable properties:

1. It abstracts from a large number of syntactic details of the given derivation. For example it is insensitive to the choice of the concrete sequent calculus variant (multiplicative, additive,...). Furthermore, it is invariant under a number of transformations which are generally perceived not to change the mathematical proof underlying the formal derivation, e.g. rule permutations or the negation-normal-form-transformation.

2. While abstracting from many syntactic details it still contains all the used instances of quantified formulas and it is in these instantiations of quantified formulas where the ingenuity of a mathematical proof in first-order logic lies.

3. For the comparison of two pairs of characteristic clause sets there are other - and frequently more interesting - options than pure equality. For example subsumption is a syntactic - and thus restricted - form of implication and on the level of derivations, subsumption of characteristic clause sets provides a good account of generalization and its converse: specialization of proofs.

References

[1] Matthias Baaz and Alexander Leitsch. Cut-elimination and Redundancy-elimination by Resolution. *Journal of Symbolic Computation*, 29(2):149–176, 2000.

[2] G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210,405–431, 1934–1935.