The Number of Axioms

Juan P. Aguilera
Department of Mathematics
Ghent University
Gent, Belgium
aguilera@logic.at

Matthias Baaz
Institute of Discrete Mathematics and Geometry
Technische Universität Wien
Vienna, Austria
baaz@logic.at

Jan Bydžovský
Institute of Discrete Mathematics and Geometry
Technische Universität Wien
Vienna, Austria
jan.bydz@gmail.com

We explore lower bounds on the number of axioms needed to prove theorems. We deal with first-order logic, formalized as a version of the *sequent calculus* LK introduced by Gentzen [2] (see also Takeuti [6] for additional background): A *sequent* is an expression of the form

$$\Gamma \vdash \Delta \tag{1}$$

where Γ and Δ are finite *multisets* of formulae. The interpretation of (1) is "if all formulae in Γ hold, then some formula among Δ holds". In LK, one starts with axioms and infers other sequents through various *rules of inference*. We measure the length of a proof by the number of sequents that appear in it; we measure the length of a sequent by the number of symbols in it. It is well known that one cannot give a recursive bound on the least possible length of a proof of a provable sequent S in terms of the length of S itself. Below, we prove the following strengthening:

Theorem 1. *There is no recursive bound on the least possible number of distinct axioms in an* LK*-proof of a sequent in terms of its length.*

Here, we do not consider two occurrences of the same axiom $A(a)$ as "distinct," but we do consider as distinct different instances of the same axiom, such as $A(a)$ and $A(b)$. Theorem 1 says that as one considers longer sequents, their minimal proofs not only become "longer," but also "wider," and moreover so in a way that cannot be accounted for by the repetition of axioms.

Intuitionistic logic can be formalized as one of many variants of Gentzen's LJ, which is obtained from LK by adding the restriction that all sequents $\Gamma \vdash \Delta$ contain at most one formula on the right-hand side. All our arguments below apply to intuitionistic logic and to many other related systems. In particular, we have:

Theorem 2. *There is no recursive bound on the least possible number of distinct axioms in an* LJ*-proof of a sequent in terms of its length.*

Among the usual inferences in sequent calculi figures the *cut* rule:

$$\frac{\Gamma \vdash \Delta, A \qquad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}$$

Gentzen's *Cut-Elimination Theorem* says that the cut rule is redundant, however. Cut-free proofs are useful because they have the *subformula property*: in a proof of a sequent S with no instances of the cut rule, one only finds formulae which are substitution instances of subformulae of formulae in S. This is a desirable property for automated proof search, and other applicatinos. The main tool in the proof of Theorem 1 is the following lower bound on the number of axioms in cut-free proofs:

Theorem 3. *Let S be a provable* LK*-sequent of length s. Denote by m the minimal length of a cut-free* LK*-proof of S and by α the minimal number of* distinct *axioms in a cut-free* LK*-proof of S. Then*

$$\sqrt[s^2]{\frac{1}{s^4}\log_2(m)} \leq \alpha.$$

Finally, we mention another application of Theorem 3. Recall that cut elimination has a high computational cost. A function $f : \mathbb{N} \to \mathbb{N}$ is *elementarily bounded* if it is bounded by a function of the form

$$x \mapsto 2^{2^{\cdots^{2^x}}}.$$

An algorithm is *elementary* if it runs in an amount of time which is elementarily bounded. A classical theorem due independently to Orevkov [3] and Statman [5] states that there can be no elementary cut-elimination algorithm for first-order logic. By inspecting Schütte's proof of Gentzen's cut-elimination theorem (see e.g., Schwichtenberg [4]), one sees that this result is optimal, in the sense that the cut-elimination theorem requires computations as simple as possible among non-elementary classes. More precisely, it is easily shown that the cut-elimination theorem is equivalent to the totality of the superexponential function (which maps a natural number n to the result of applying the exponentiation function $x \mapsto 2^x$ n times) over Elementary Arithmetic (EA) (see e.g. Beklemishev [1] for more on relevant subsystems of arithmetic); however, this leaves open the possibility of strengthening the result in other directions; namely, Orevkov and Statman's proofs show that there is a sequence of first-order sequents the nth of which has a proof of length $\mathcal{O}(n)$, but whose shortest cut-free proofs have lengths which cannot be elementarily bounded. Using Theorem 3 we can strengthen this result by showing that those cut-free proofs must necessarily have non-elementarily many distinct axioms.

Theorem 4. *There is no elementary bound on the least possible number of* distinct *axioms of a cut-free* LK*-proof of a sequent in terms of the least possible length of an* LK*-proof of the same sequent.*

References

[1] Beklemishev, L. D. Reflection principles and provability algebras in formal arithmetic. *Russian Math. Surveys 60* (2005), 197–268.

[2] Gentzen, G. K. E. Untersuchungen über das logische Schließen, I. *Math. Z. 39* (1934), 176–210.

[3] Orevkov, V. P. Lower Bounds for Increasing Complexity of Derivations after Cut Elimination (in Russian). *J. Soviet Math.* (1982), 2337–2350.

[4] Schwichtenberg, H. Proof theory: Some applications of cut-elimination. In *Handbook of Mathematical Logic*, J. Barwise, Ed. 1982, pp. 867–896.

[5] Statman, R. Lower Bounds on Herbrand's Theorem. *Proc. Amer. Math. Soc. 75* (1979), 104–107.

[6] Takeuti, G. *Proof Theory (Second ed.).* Dover Publications, 2013.