A New "Feasible" Arithmetic

S. Bellantoni* Martin Hofmann†

January 15, 1999

Abstract

A classical quantified modal logic is used to define a "feasible" arithmetic $\mathcal{A}_2^1$ whose provable functions are exactly the polynomial-time computable functions. Informally, one understands $\Box\alpha$ as "α is feasibly demonstratable".

$\mathcal{A}_2^1$ differs from a system $\mathcal{A}_2$ that is as powerful as Peano Arithmetic only by the restriction of induction to ontic formulas (an ontic formula is one whose type is $\Box$-free). Thus, $\mathcal{A}_2^1$ is defined without any reference to bounding terms, and admitting induction over formulas having arbitrarily many alternations of unbounded quantifiers, albeit for so-called "tier 0" values only. The system also uses only a very small set of initial functions.

To obtain the characterization, one extends the Curry-Howard isomorphism to include modal operations. This leads to a realizability translation based on recent results in higher-type ramified recursion. The fact that induction formulas are not restricted in their logical complexity, allows one to use the Friedman A translation in a way that would be impossible for conventional bounded arithmetics.

We claim that $\mathcal{A}_2^1$ provides a "foundational" definition of polytime provability. The development also leads us to propose a new Frege rule, the "Modal Extension" rule: if $\vdash \alpha$ then $\vdash A \leftrightarrow \alpha$ for new symbol A.

References

S. Bellantoni, "Ranking Arithmetic Proofs by Implicit Ramification", in *Proof Complexity and Feasible Arithmetics*, P. Beame and S. Buss, eds., DIMACS Series in Discrete Mathematics, v. 39, 1998.

Martin Hofmann, "Type systems for polynomial-time computation". Habilitationsschrift. Darmstadt University of Technology. 1998. Available via www.dcs.ed.ac.uk/home/mxh/.

Edward Nelson, "Understanding Intuitionism", presented at the *Rencontre du Reseau Georges Reeb*, March 24-28, 1997.

*Department of Computer Science, University of Toronto. The assistance of the Fields Institute for Research in Mathematical Sciences is gratefully acknowledged.

†Laboratory for Foundations of Computer Science, University of Edinburgh.