THE JOURNAL OF SYMBOLIC LOGIC
Volume 67, Number 1, March 2002

A NEW "FEASIBLE" ARITHMETIC

STEPHEN BELLANTONI[†] AND MARTIN HOFMANN[‡]

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

$\mathscr{A}_2^1$ differs from a system $\mathscr{A}_2$ that is as powerful as Peano Arithmetic only by the restriction of induction to ontic (i.e., $\Box$-free) formulas. Thus, $\mathscr{A}_2^1$ is defined without any reference to bounding terms, and admitting induction over formulas having arbitrarily many alternations of unbounded quantifiers. 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 directly.

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.

§1. Introduction. In recent years considerable effort has been dedicated to defining and exploring logical and arithmetic systems in which the reasoning involved is not only constructive but "feasibly constructive". In most cases this is understood to mean that the constructive content of the proof – however that might be defined – is polynomial time computable. In any case, an important litmus test for feasibility of a first order arithmetic is that the functions for which a suitable convergence statement can be proved, are at most the polynomial time computable functions. For this test to be of any significance, of course, the system must have enough expressive power to discuss a wider class of functions, say all the primitive recursive functions. Buss's system $\mathscr{S}_2^1$ of bounded arithmetic [7] is fundamental to this subject; see Krajicek [16] for a discussion of related work.

At the same time, researchers in recursion theory have developed systems in which computational complexity is controlled by type information rather than by explicit resource bounds [24], [3], [17], [14], [5]. Each of the various types ι, $\Box\iota$, $\Box\Box\iota$, ... in a ramified system is a different intension for the same extensional values. Typically, one may recurse on a value that is comprehended through a type $\Box\iota$ reference, while one may only access a few low-order bits from a value referred to by a type ι variable. A related area of work is the "descriptive complexity" characterizations

Received January 20, 2000; revised October 16, 2000.

[†]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.

© 2002, Association for Symbolic Logic
0022-4812/02/6701-0007/$2.30