The computational power of bounded arithmetic from the predicative viewpoint

January 5, 2007

Sam Buss
Department of Mathematics
U.C. San Diego

Predicative Theories — Interpretations $I\Delta_0$.

Defn. A theory is *predicative* (in the sense of E. Nelson) if it is interpretable in Q.

Since $I\Delta_0$ in interpretable in Q, a theory is predicative iff it is interpretable in $I\Delta_0$.

Historical motivations for $I\Delta_0$ and other weak theories:
- Philosophical [Bennett, Nelson, and others]
- (Near-)Feasible computation [Parikh, Paris, Wilkie, Buss, many others]
- Mathematical (models of fragments of PA). [also Kirby, Dimitracopolous, others].

Nelson's definition was motivated by his intuition that predicative theories are a framework for demonstrably correct reasoning that does not require mathematically dubious platonic assumptions.

Cut-interpretations

Let T be the theory Q or $I\Delta_0$.

Defn. A formula $\phi(x)$ defines a *cut-interpretation* if it defines an initial segment, i.e.,

$$T \vdash \phi(0)$$
$$T \vdash \forall x \forall y(\phi(x) \land y \leq x \rightarrow \phi(y)).$$

For cut interpretations, symbols such as 0, S, $+$, $\cdot$, etc. are interpreted by themselves (possibly may not be total). [Rk: If $\leq$ is not in the language of T, then "$y \leq x$" defined as "$\exists z(y + z = x)$".]

Interpretations in Q are generally cut-interpretations.

In particular, $I\Delta_0$, S_2^i, T_2^i, etc. are all cut-interpretable in Q.

Bounded Theories

Defn. A *bounded quantifier* is of the form $(\forall x < t)$ or $(\exists x \leq t)$. A formula is Δ_0 or *bounded* if all its quantifiers are bounded.

Defn. A *bounded theory* is axiomatized by $\forall\Delta_0$ formulas. (Universal closures of bounded formulas.)

Theories such as Q, $I\Delta_0$, S_2^i, T_2^i are all bounded theories.

Theories interpreted in Q are generally bounded theories.

This talk: characterize the functions that can defined in bounded theories which are cut-interpretable in Q. (or, equivalently, in $I\Delta_0$.)

The characterization will be in terms of their computational complexity.

Defn. f is defined in a bounded, cut-interpreted theory T provided

$$I\Delta_0 + T + T^* \vdash \forall x(f(x) = f^*(x)),$$

where T^* is formed from T by replacing every new function symbol g with g^*, and every new predicate symbol P with P^*, etc., and where $I\Delta_0$ includes induction for all bounded formulas in the combined languages.

This is the "uniqueness property" for f.

Main tools of cut interpretations.

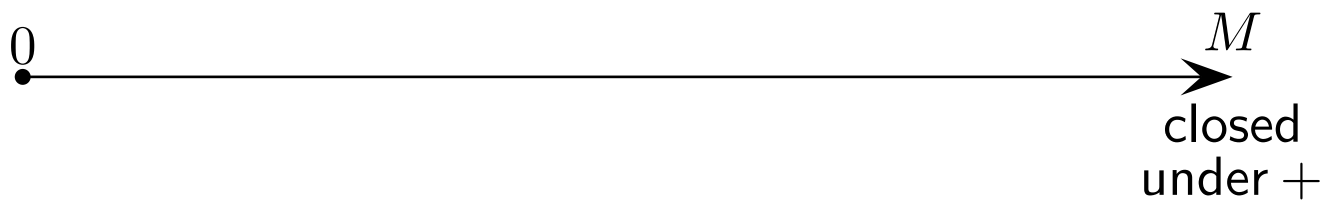
[Solovay, Nelson, ...]

Tool #0. Transitivity of cut-interpretability, allows us to work over a base theory stronger than Q, such as $I\Delta_0$ or S_2. So may assume presence of polynomial time functions, and validity of bounded induction, etc.

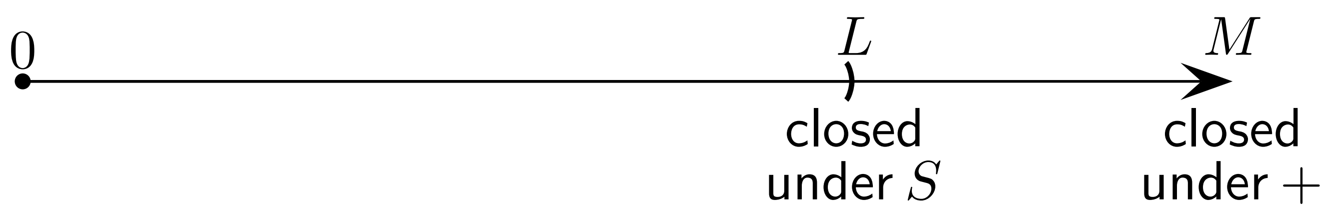
Tool #1. Define a cut based on existence of an exponential. Let $\phi(x)$ be $(\exists y)[y = 2^x]$. Or alternately, let $\phi(x)$ be $(\exists y)(|y| = x)$.

Then $\phi(x)$ defines an initial segment of elements for which exponentials exist (not nec. in the initial segment).

Tool #2. Given a cut closed under S (resp., $+$, $\cdot$, $\#_i$), one can define a cut closed under $+$ (resp., $\cdot$, $\#$, $\#_{i+1}$).

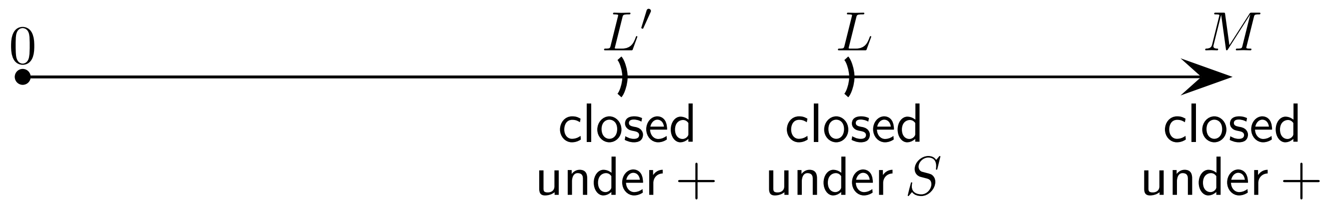


Given: a model M closed under $+$.



Given: a model M closed under $+$.

Tool $\#1$: Form cut $L = \{x : 2^x \text{ exists in } M\}$.
Note L is closed under successor.



Given: a model M closed under $+$.

Tool $\#1$: Form cut $L = \{x : 2^x \text{ exists in } M\}$.
Note L is closed under successor.

Tool $\#2$: Form sub-cut L' closed under $+$.
Exponentials of L' elements exist in M.

These tools allow one to define bounded theories in which (a) all polynomial time functions are defined, in fact all Ω_i-time functions are definable, and (b) induction holds for all bounded formulas.

So, $I\Delta_0 + \Omega_1$ and S_2 are cut interpretable in Q by these methods.

Defn. Define $\Omega_0(x) = 2^{2|x|}$. And $\Omega_{i+1}(x) = 2^{\Omega_i(|x|)}$..

Then, $\Omega_0(x) \approx x^2$ and $\Omega_1(x) \approx x\#x$ and $\Omega_i(x) \approx x\#_{i+1}x$.

Tool #2 allows us to predicatively define all Ω_i-time functions. This is in fact the best that can be done, at least in terms of <u>growth rate</u> of functions.

Defn. A function $f(x)$ is *dominated by* Ω_i if $f(x) < \Omega(x)$ for all sufficiently large x.

Growth closure properties of cuts.

The definable initial segments can be closed under Ω_i (but not under exponentiation):

Thm. [Wilkie, LC'84, formalized version]. Suppose T is a bounded theory, cut interpretable in Q, and f is a function symbol of T. Then f is dominated by some Ω_i. In fact, there is a finite extension T' of T which is bounded and cut-interpretable and which proves f is dominated by Ω_i.

Although this bounds the growth rate of functions in bounded predicative theories, it does not bound their computational complexity.

A lower bound

Defn. A function is defined to be Ω_i-TIME if it can by computed in time $\Omega_{i-1}(n^{O(1)})$-time. (n is the length of the input.)
It is in EXP^i-TIME if it can be computed in time $2^{\Omega_{i-1}(n^{O(1)})}$.

So, Ω_2-TIME is the same as polynomial time. EXP^2-TIME is exponential time.

For $i > 2$, Ω^i-TIME is "only slightly larger than" polynomial time. and EXP^i-TIME is "only slightly larger than" exponential time.

One should think of "only slightly larger than" as meaning "morally equivalent to".

Thm. Every EXP^i-TIME predicate is definable in a bounded, predicative theory.

Thm. Every EXP^i-TIME function dominated by some Ω_i is definable in a bounded predicate theory.

Pf. Let P be an EXP^i-Turing machine. Over $I\Delta_0 + \Omega_i +$ "a single exponential exists": introduce function symbols $Q(t,x)$, $T(t,p,x)$, $H(t,x)$ that define, at time t, $P(x)$'s state, head position, and tape content at position p. Then, working in a cut where Ω_{i+1} is total, restrict to a cut where single exponentials exist in the original model. Let T be the theory in this language with the enlarged language, and with appropriate (bounded) axioms describing the values of Q, T, H. By construction, Q, T, H and the "predicate P accepts" are uniquely defined in T.

An identical construction works for the second theorem.

The upper bound.

Thm. Any predicate or function definable in a bounded theory T cut-interpreted in Q is in NEXP^i-TIME $\cap$ coNEXP^i-TIME. Furthermore, this holds provably in a suitable bounded predicative theory.

Pf (idea). By compactness, T is w.l.o.g. finitely axiomatized. And every function in T is bounded by some Ω_i. Given x, calculate $f(x)$ by nondetermininistically guessing every value $P(y)$ and $g(y)$ for all predicates P and all functions g and all $y < \Omega_i(x) + O(1)$. (The bound on y comes from compactness.) By the uniqueness property, $f(x)$ is uniquely determined by this process.

To show this holds provably, formalize the above argument in a suitable predicative theory. $\square$

Closing the gap.

So far:

- Lower bound: EXP^i-time functions/predicates.
- Upper bound: $\mathrm{NEXP}^i \cap \mathrm{coNEXP}^i$-time functions/predicates.

Suppose a bounded predicate theory T proves $P \in \mathrm{NEXP}^i \cap \mathrm{coNEXP}^i$. Then

$$P(x) \Leftrightarrow (\exists f_1) N_1(x, f_1) \Leftrightarrow (\forall f_2) N_2(x, f_2).$$

for some EXP^i-TIME N_1 and N_2.
Extend T with new function symbol f and with axioms

$$(\forall x)[N_1(x, f) \vee \neg N_2(x, f)].$$

This is a predicative bounded extension. (Existence condition for f follows by assuming sufficient exponentials exist in the original model.)

This proves:

Thm. The functions definable in bounded, cut-interpreted extensions of Q are precisely the functions which are dominated by some Ω_i and are provably in $\mathrm{NEXP}^i \cap \mathrm{coNEXP}^i$-time.

Coro. The PSPACE predicates and functions (of polynomial growth rate) are predicative in the sense of Nelson.

Coro. The exponential time predicates and functions (of polynomial growth rate) are predicative in the sense of Nelson.

Implications / Applications / Open problems.

Implication: The predicative constructions are essentially the exponential time and $\mathrm{NEXP} \cap \mathrm{coNEXP}$ constructions of polynomial size objects (this includes extensions to the "morally equivalent" Ω_i growth rate).

Applications: This puts computational limits on what can be formalized predicatively, e.g., the formalizations of Fernandez and Ferreira of real analysis are possible in part since polynomial space and exponential time constructions suffice (c.f. Friedman-Ko). It potentially has applications for reverse mathematics over predicative base theories.

Open question: From Wilkie [LC'84], it is still open whether a Σ^0_{k+1} formula can define a cut closed under Ω_k. More generally, it would be nice to have better streamlined proofs of Wilkie's theorem.

E. Nelson, Predicative Arithmetic,, Princeton, 1986.

A. Wilkie, *On sentences interpretable in systems of arithmetic,* in Logic Colloquium '84.

A. Fernandez and F. Ferreira, *Groundwork for weak analysis,* JSL, 2002.

S. Buss, *The computational power of bounded arithmetic from the predicative viewpoint,* to appear in CIE'05 volume. Available on web.