On Mathematical Instrumentalism

Patrick Caldon and Aleksandar Ignjatović*

February 9, 2005

Abstract

In this paper we devise some technical tools for dealing with problems connected with the philosophical view usually called mathematical instrumentalism. These tools are interesting in their own right, independently of their philosophical consequences. For example, we show that even though the fragment of Peano's Arithmetic known as $I\Sigma_1$ is a conservative extension of the equational theory of Primitive Recursive Arithmetic (PRA), $I\Sigma_1$ has a super-exponential speed-up over PRA. On the other hand, theories studied in the Program of Reverse Mathematics that formalize powerful mathematical principles have only polynomial speed-up over $I\Sigma_1$.

1 Introduction

In this paper we discuss some aspects of the philosophical view that is usually called mathematical instrumentalism. An instrumentalist takes only a limited part of mathematics, $\mathcal{P}$, as fully meaningful (or special in some other way) and considers the rest of mathematics (or another larger part of it) $\mathcal{I}$ as a formal apparatus for facilitating proofs of statements from $\mathcal{P}$. Thus, to justify applications of such a mathematical apparatus in proofs of statements from $\mathcal{P}$, one must only show the soundness of the $\mathcal{I}$-proofs of statements from $\mathcal{P}$ without having to argue about the meaning of the part of mathematics embodied in the instrument $\mathcal{I}$. The best known such view is when $\mathcal{P}$ is finitistic mathematics; it was expounded by Hilbert in his Program. His hope was that the rest of mathematics formalized through proof

*This is a revised excerpt from the author's Ph.D. Thesis submitted at the University of California at Berkeley in 1990. The author is grateful to his adviser, Professor Jack Silver, for his support, many helpful discussions and for sharing his insights, to Professor Charles Chihara for discussions and encouragements, to the referees for many most useful comments which reshaped the paper.

theory could be proven consistent using purely combinatorial means and, hence, in a way acceptable to a finitist. This would have justified a belief in a paradox-free future of mathematics presupposing only the correctness of finitistic reasoning.

Even though Gödel's results showed (at least under certain assumptions of what constitutes a finitistically acceptable proof) that Hilbert's Program cannot be realized, the instrumentalist view of mathematics is still an attractive one. It might be quite informative to investigate those parts of mathematics (denoted by $\mathcal{P}$) which we feel that they have special status, either in the sense of having clearer meaning than the the rest of mathematics, or that we have a clear intuitive representation of objects which such parts seem to "talk about" (e.g. finite sequence of signs) or just that they are in a certain sense minimal nontrivial parts (see [21], p. 525). Then we can adjoin various other parts of mathematics, $\mathcal{I}$, that are conservative over $\mathcal{P}$ for all sentences of the language of $\mathcal{P}$, considering $\mathcal{I}$ as an instrument for facilitating proofs of such sentences. One can then analyze the relationship between $\mathcal{P}$ and $\mathcal{I}$ in the following terms:

- how much does $\mathcal{I}$ help make $\mathcal{P}$ proofs shorter or easier to understand?
- can we find some support for the belief in the consistency of $\mathcal{I}$ on the basis of $\mathcal{P}$?

This paper is devoted to devising technical tools for accomplishing such an analysis, as well as hinting how such tools can be used to draw philosophical conclusions.

2 Philosophical Considerations

In this paper we choose $\mathcal{P}$ to be the finitistic reasoning about numbers, accepting Tait's analysis and delimitation of finitism (see [21]). Thus, we take Finitism to be the part of mathematics that corresponds to the theory of natural numbers formalized as Primitive Recursive Arithmetic, either as an equational theory (which we will denote by $eqPRA$; see [8] for details) or as a first order theory (denoted as PRA, see [16]). In the first case, formulas are Boolean combinations of equations; in the second case we allow universal closures of formulas that can involve bounded quantifiers. Since the universal quantifiers can be replaced by free variables and the bounded quantifiers can be eliminated using functions defined by primitive recursion, according to Tait's thesis, such formulas are finitistically acceptable.

We will consider several theories which are conservative extensions of $eqPRA$ or Π^0_2 conservative extensions of PRA, which we denote by $\mathcal{I}$. Such

theories formalize mathematical principles of increasing strength to be used as instruments in our derivations. There are two directions one can take. We can either add stronger arithmetical principles, which seems to amount to adding more induction[1], or we can first expand the language with variables for new type of objects (e.g. sets) and then add new mathematical principles for these objects.

In the direction of adding only new arithmetical principles in the form of stronger induction, we are extremely limited by our conservativeness requirement: all we can add is Σ_1 induction, that is, the restriction of the induction schema of Peano's Arithmetic for Σ_1 formulas which is indeed a conservative extension of $eqPRA$; Σ_2 induction proves the consistency of PRA and thus is not a conservative extension of PRA (see [16]).

On the other hand, the second direction leaves much more space; several theories that formalize significant portions of mathematical practice are conservative extensions of $eqPRA$. Theories which we will consider here were introduced by Friedman and Simpson in the program of Reverse Mathematics (see [19] for details). The weakest one is called Recursive Comprehension (RCA) and it allows introduction of second order objects (i.e. sets of numbers) if they are simply definable (in a Δ_1^0 way) as well as the use of Σ_1^0 induction for formulas with second order parameters. The Weak König's Lemma (WKL) adds to this the power of the compactness principle which is one of the most fundamental mathematical tools. Further strengthening of such theories are obtained, for example, by adding a formalization of Baire's Category Theorem (WKL^+ of Simpson and Brown, see [3], [18] and [19]). Thus,

$$eqPRA \subset PRA \subset I\Sigma_1 \subset RCA \subset WKL \subset WKL^+ \subset ... \qquad (1)$$

Here $eqPRA$ is the only part of mathematics of "real interest" for us (of course only in our discussion of mathematical instrumentalism); in this chain $I\Sigma_1$ is the only purely arithmetical instrument conservative over $eqPRA$, whereas the other theories formalize set theoretical principles. One could expect that theories formalizing powerful mathematical tools would greatly speed up proofs of various universal propositions about numbers. On the other hand, even though the consistency of such theories is not provable finitistically, their importance and "relative modesty" should motivate us to look for alternative ways of supporting their consistency by appealing to some forms of finitistic evidence. For example in [10], it was shown that the consistency of $I\Sigma_1$, RCA, and WKL is provable using a version of the

[1] Isaacson offers an argument in support of this claim in [11].

"finitistically warranted" ω rule (of course, not acceptable on purely finitistic grounds). More precisely, it can be shown that there is a finitistically acceptable function f (in Tait's sense) for which one can prove in a finitistically acceptable way, that for all n, $f(n)$ is a proof of the statement "n is not (a code of) an inconsistency in WKL." We can further consider if this can be strengthened by, for example, restricting how fast f can grow.

Thus, the aim of the present work is to accurately evaluate the lengths of proofs of "real" statements within an "instrumental" theory in order to be able to independently evaluate other, more subtle features that such instrumental theory can have. This is then supplemented with a matching analysis of some types of consistency proofs of such instrumental theories.

3 Preliminaries

Unless otherwise specified, we will work in the standard first order Hilbert style proof system (see [4]). Let p be a proof in a first order theory. We will denote the total length of the proof p by $|p|$, counting the length of the formulas of the proof (i.e. the total number of all symbols in p; see [15] for details). We denote by 2^n_m the stack of m two's ending with n as the last exponent:

$$2^n_m = \underbrace{2^{2^{\cdot^{\cdot^{2^n}}}}}_{m}$$

More formally, $2^n_0 = n$, $2^n_{m+1} = 2^{2^n_m}$. A function has *Kalmar elementary growth rate* if there exists a natural number m such that $f(x)$ is eventually majorized by 2^x_m. We say that a function f has a *roughly super-exponential growth rate* if it does not have a Kalmar elementary growth rate, but for some polynomial with natural coefficients $P(x)$, $f(x)$ is eventually dominated by $P(2^x_x)$ (i.e. the function obtained by replacing the variable x in $P(x)$ by 2^x_x; the function 2^x_x is called the *super-exponential function* and is the first function in the Wainer hierarchy which dominates all the elementary functions).

A function has a polynomial growth rate if it is eventually dominated by a polynomial with natural coefficients.

Definition 1 *Let T' and T be two theories such that $T' \subset T$ and let Φ be a subset of theorems of T'.*

1. *T has a roughly super-exponential speed-up over the theory T' with respect to the set Φ if there exists a sequence $\{\varphi_i\}_{i\in\omega}$ of formulas from*

Φ *such that if* p_n^T *and* $p_n^{T'}$ *are the shortest proofs of* φ_n *in* T *and* T'*, respectively, then: (i) no function* f *with Kalmar elementary growth rate satisfies* $|p_n^{T'}| < f(|p_n^T|)$ *for all* n*; (ii) there is a function* f *with a roughly super-exponential growth rate such that the above inequality holds for all* n*.*

2. *Theory* T *has at most a polynomial speed-up over the theory* T' *if there exists a polynomial* $P(x)$ *with natural coefficients such that for any theorem* φ *of* T'*, the following holds: if* p^T *and* $p^{T'}$ *are the shortest proofs of* φ *in* T *and* T'*, respectively, then* $|p_n^{T'}| < P(|p_n^T|)$ *for all* n*.*

We can now formulate the main problems we will consider.

Problem 1 *Are* $I\Sigma_1$*,* RCA*,* WKL*, and similar conservative extensions of* $eqPRA$ *useful and efficient instruments at all? More precisely, are the* $I\Sigma_1$ *proofs of* Π_1^0 *theorems of* PRA *much shorter than the* PRA *proofs which have the same conclusions? (Here we take* PRA *as a first order theory to eliminate the advantage that* $I\Sigma_1$ *might possibly have purely from its first order logic with cut.) Are* RCA *(*WKL*) proofs shorter than* $I\Sigma_1$ *(*RCA *respectively) proofs?*

We will show that $I\Sigma_1$ has a very significant, *roughly super-exponential* speed-up over PRA. We also show that RCA has at most polynomial speed-up over $I\Sigma_1$. In [9] we conjectured that WKL also has only a polynomial speed-up over RCA; this conjecture was proved independently by P. Hájek in [7] and by J. Avigad in [1] (each in light of [9]).

Note that in the above considerations, the speed-up is measured only in terms of lengths of proofs; this does not rule out a "conceptual speed-up," i.e. a formulation of the proof which uses concepts that make the proof easier to grasp, even if there is no speed-up in terms of length of formal proofs.

We now have to make a decision about which speed-up we consider significant and which we do not. One could argue that we should find a finite number of mathematically important Π_1 theorems about natural numbers and compare the lengths of their PRA proofs with, for example, the lengths of their WKL proofs. But if we want to draw conclusions of philosophical importance, we should consider mathematics as having an infinite collection of theorems, and in this case the growth rate of the sizes of proofs matters the most. Extensive research in complexity theory indicates that two procedures can be considered to belong to the same, naturally defined efficiency class if

the number of steps needed to execute either one of them is smaller or equal than the value of a polynomial evaluated at the number of steps needed to execute the other one (for the same input). We accept this for provability in formal theories, and, consequently, if a theory T has only a polynomial speed-up over a theory T', we consider T and T' as instruments whose efficiencies differ insignificantly.

Thus, since WKL has no significant speed-up over RCA (as shown in [1] and [7]), and since WKL^+ has no significant speed-up over WKL (which can be seen by suitably modifying arguments from [1] and [7]), it appears that (i) only stronger *arithmetical* principles embodied in the instrument make proofs of arithmetical propositions shorter *in length*, and (ii) conservative instruments that formalize stronger mathematical principles that are not of an arithmetical nature (e.g. set theoretical principles) could produce only "conceptual speed-up," i.e. they can perhaps make proofs conceptually clearer and easier to grasp without making formal proofs shorter in length.

To explain possible use of such results for an evaluation of mathematical instrumentalism, we consider instruments that can prove set theoretical formalization of important theorems of analysis (e. g., RCA and stronger theories of Reverse Mathematics, see [19]) and distinguish two possible cases.

Case 1. There is no significant body of finitistic truths whose proofs using such instruments are conceptually clearer than the purely arithmetical (i.e. $I\Sigma_1$) proofs of the same truths.

In this case, since we do not have any speed-up in terms of length of proofs, such instruments would be useless and so the particular case that we consider of the instrumentalist view of mathematics would collapse.

Case 2. There is a significant body of finitistic truths whose proofs which use such instruments are conceptually clearer than the purely arithmetical proofs of the same truths.

In this case, since the benefit of our instruments does not come from the mere shortening of the proofs but from some sort of more subtle, *conceptual* clarification and facilitation, an instrumentalist must explain how the part of formalized mathematics in these instruments can have less clear meaning than the "real" (in our case, finitistic) part of mathematics and yet provide conceptual facilitation.[2]

We now want to formulate the second problem we will consider. As proved by Sieg (see [16]), there is a finitary procedure for transforming

[2]In [9] it was claimed that this was not possible. However, one of the referees has made serious objections to such an argument. The referee's remarks have convinced me that determining the exact philosophical implications of the technical results of this paper is a much subtler task than I originally envisioned.

WKL proofs of Π_1 formulas into proofs of such formulas in PRA. Thus, for theories T like RCA or WKL we have:

$$PRA \vdash Con(T) \leftrightarrow Con(PRA) \tag{2}$$

Yet, such theories T formalize mathematical principles of increasing strength. Thus, one would like to find a finer method for measuring consistency strength of such theories, so that, say, the consistency of WKL in this new sense would be a stronger assumption than the consistency of PRA alone. As a consequence of Corollary 2 of [10], it is easy to see that there are primitive recursive functions f_{PRA}, f_{RCA} and f_{WKL}, such that if $Con_T(n)$ suitably formalizes *"there are no proofs of an inconsistency in T of length smaller or equal than n"*, then

$$PRA \vdash \forall x \exists y(|y| < f_T(x) \wedge Pr_{PRA}(y, Con_T(x))) \tag{3}$$

for $T = PRA, RCA, WKL$.[3] Thus, it is natural to ask the following question.

Problem 2 *Let T and T' be two conservative extensions of PRA, such that $T' \subset T$. Is it true that for the stronger theory T, the function f_T producing the least value $f_T(x)$ for which* (3) *holds grows significantly faster than the function $f_{T'}$ corresponding to a weaker theory T'?*

To answer the above question we will use a result of Pudlák[4] to conclude that f_{PRA} grows polynomially. We will also show that $f_{I\Sigma_1}$, f_{RCA} and f_{WKL} grow roughly super-exponentially (see (5) and (6)). Thus, a significant difference in the growth rates of the functions f_{PRA}, $f_{I\Sigma_1}$, f_{RCA} and f_{WKL} which generate proofs of "consistency up to n" within PRA of these theories occurs only between f_{PRA} and $f_{I\Sigma_1}$, while other functions have similar growth rate as $f_{I\Sigma_1}$. We conjecture that for any reasonable conservative extension T of PRA the function f_T grows at least as fast as what the speed-up of T over PRA is. The same could be true for a broad class of theories besides PRA. Also, it would be interesting to see if one

[3] As shown in [10], for some primitive recursive function f, $PRA \vdash \forall x Pr_{PRA}(f(x), \neg Pr_T(x, \lceil 1 = 0 \rceil))$. Since there are less than 2^{x+1} proofs in T of length at most x, they can be all combined together to get the value of a primitive recursive function f_T such that the above holds.

[4] Pudlák's Theorem 5.5 from [15] shows that for any theory, A, from a wide class of theories, there exists a polynomial, $P(x)$, such that for any natural number n, there is a proof of length $P(n)$ in A of the statement $Con_A(\underline{n})$. The proof of his statement takes place in the meta-theory but it is easy to see that it can be formalized in A. Thus, for $A = PRA$ we get the claim we need.

can find more refined ways of distinguishing among equiconsistent theories formalizing mathematical principles of different strength, using some other functions or predicates naturally related to the consistency predicates.

The above is also relevant to the following problem presented by Gödel. We quote Kreisel [12], Marginal Comments on page 241.

> ... one may modify Hilbert's (generalized) programme by taking into account the *lengths of proofs*. Thus given a formal system F and an area of evidence $\mathcal{P}$, let $\psi(n)$ be the length of the shortest proof in $\mathcal{P}$ of the consistency of F restricted to the proofs of length n. (If the number of proofs of bounded length in F is finite and F is consistent there will always be such a proof of their consistency.) If $\psi(n)$ is of the same order of magnitude as n, we should have a 'practical' reduction of F to $\mathcal{P}$. I first heard this interesting suggestion in a conversation with Gödel.

In our analysis of this idea we will take $\mathcal{P}$ to be finitistic evidence which is inherent in Hilbert's Program. We formalize "the consistency of F restricted to the proofs of length (at most) n" by by $Con_F(n) \equiv \neg\exists p(|p| \leq n \wedge Pr_F(p, \lceil 1 = 0 \rceil))$. Also, we have to make precise the informal description that "$\psi(n)$ is of the same order of magnitude as n" and the informal notion of a "practical reduction." We will accept the standards of complexity theory: $\psi(n)$ is considered to be of the same order of magnitude as n if it is bounded by a polynomial in n, i.e. if for all n

$$\psi(n) \leq P(n) \tag{4}$$

for some polynomial P with natural coefficients. If $d(n)$ are proofs of length $\psi(n)$ and the above holds, we will say that the sequence of proofs $d(n)$ is *feasible*. Both of the above two conventions are standard and discussed in length in the literature on complexity of proofs. Our third assumption will be more delicate and we defend it on the same grounds we defended the thesis in [10] about what instances of the ω rule could be considered finitistically warranted.

In order to have a "practical reduction" of F to $\mathcal{P}$ that is satisfactory from the standpoint of the area of evidence $\mathcal{P}$, not only do we have to have $\mathcal{P}$-proofs $d(n)$ of $Con_F(n)$ whose length $\psi(n)$ is smaller or equal $P(n)$, but this fact itself must be verifiable by means that all belong to the area of evidence $\mathcal{P}$, i.e., one should be able to justify, on the basis of the area of evidence $\mathcal{P}$, the statement "*For every n there is a $\overline{\mathcal{P}}$-proof $d(n)$ of $Con_F(n)$ whose length*

is at most $P(n)$." Here $\overline{\mathcal{P}}$ stands for a formal system corresponding to $\mathcal{P}$; the requirement that $\mathcal{P}$ is formalizable is built into the problem: to be able to measure the length $\psi(n)$ of proofs $d(n)$, these proofs must be formalized as sequences of symbols whose length is counted. The above motivates us to introduce the following meta-definition which will replace the informal notion of a "practical reduction."

Meta-definition 1 *The consistency of a theory T is feasibly reducible to the area of evidence $\mathcal{P}$ if one can give a $\mathcal{P}$-proof of the statement* "there is a feasible sequence d of $\overline{\mathcal{P}}$-proofs $d(n)$ of the assertion that there is no proof of an inconsistency in T of length shorter than n."

Having in mind that we identify finitistic provability with provability in PRA, a theory is feasibly reducible to the finitistic area of evidence if there is a polynomial $P(x)$, such that

$$PRA \vdash \forall x \exists y(|y| < P(x) \wedge Pr_{PRA}(y, Con_T(x))). \tag{5}$$

The adaptation of the result of Pudlák mentioned in the previous problem shows that the consistency of PRA is indeed feasibly reducible to the finitistic area of evidence. Thus, it is natural to consider the following question.

Problem 3 *Is there a theory T in which one can formalize a significant portion of mathematical practice and whose consistency is feasibly reducible to the finitistic area of evidence?*

Proposition (5) proved in the next section and already mentioned in the comments after Problem 2 shows that this is not the case for any theory containing $I\Sigma_1$. As it is shown by Simpson and Smith, $I\Sigma_1$ is necessary to prove some of the most basic mathematical theorems (see [17]). Thus, it is safe to say that no significant theory from the point of view of mathematical practice is "practically reducible" to the area of finitistic evidence with a finitistic justification of such a reduction.

4 Technical Results

We now prove the technical results we discussed. We denote by $I\Sigma_1$ the fragment of Z (where Z is an extension of PRA with the induction schema for all formulas of the language of PRA) with the induction schema restricted to Σ_1

formulas;[5] RCA is a fragment of second order arithmetic containing, aside from the few usual basic axioms, only Δ^0_1 comprehension and Σ^0_1 induction (with free second order variables in these schemas); again we assume that the language of RCA contains symbols for all primitive recursive functions. Let $\mathcal{L}_{PRA}(y)$ be a formula formalizing *"y is a functional symbol of PRA"*, and let $\mathcal{L}_{PRA}(x, y)$ be a formalization of *"y is a functional symbol of PRA (whose Gödel code[6] is) smaller or equal than x."* $\mathcal{T}_{PRA}(x, y)$ is a formula formalizing *"y is a closed term of PRA containing only functional symbols smaller or equal than x."* Notice that this restricts only the language and not the size of the term — an important feature for the cut-elimination procedure to be used later. In all standard coding procedures all these formulas are at most Δ^0_1. We denote primitive recursive functions which operate on codes for various syntactical objects of PRA by capital letters. $Ar(f)$ represents the arity of the functional symbol f; $< a_0, \ldots, a_{lh(x)\dot{-}1} >$ represents one of the usual functions for coding a sequence x of numbers with $lh(x)$ representing the length of the sequence, and $(s)_i$ representing the i^{th} element of the sequence s. All such functions used in coding are primitive recursive. $\mathcal{G}(f) =< 0, g_f, h_f >$ if f is defined by primitive recursion from g_f and h_f (i.e. if $f(0, \vec{x}) = g_f(\vec{x})$ and $f(y + 1, \vec{x}) = h_f(y, f(y, \vec{x}), \vec{x})$ are axioms of PRA), and $\mathcal{G}(f) =< 1, h_f, g^f_1, ..., g^f_k >$ if f is defined by composition from $h_f, g^f_1, ..., g^f_k$. The usual codings have the property that for all (non atomic) f, $(\mathcal{G}(f))_i < \mathcal{G}(f)$. $\underline{x}$ denotes a primitive recursive function producing the Gödel code of the x^{th} numeral.

By a cut in a theory T, we mean a formula J such that

$$T \vdash J(0) \wedge \forall x(J(x) \rightarrow (J(x + 1) \wedge \forall z < x\ J(z))) \tag{6}$$

In our proofs we use the fact that Σ^0_1 induction, Π^0_1 induction, the Σ^0_1 least number principle and the Π^0_1 least number principle (all with free second order variables) are all equivalent over a weak base theory (see [16]).

Proposition 1 *There is a cut J_{RCA} in RCA such that*

$$RCA \vdash \forall x(J_{RCA}(x) \rightarrow \neg Pr_{PRA}(x, \ulcorner 1 = 0 \urcorner)) \tag{7}$$

[5]Even though $I\Sigma_1$ formulated on the language $\{+, \cdot, =, <, 0\}$ suffices to introduce all primitive recursive functions in an extension by definitions, we prefer that the language of our instruments extends the language of our base theory PRA. This also has an advantage that all formulas with bounded quantifiers only are equivalent to quantifier-free formulas by replacing bounded quantifiers with their primitive recursive definitions.

[6]In the sequel we will identify functional symbols, terms, formulas, and proofs with their Gödel codes and consequently omit the text in the parentheses above.

We define a truth predicate for variable-free sentences of some restrictions of the language of PRA and then prove the soundness of PRA restricted to such languages with respect to the variable-free sentences of these restrictions. To simplify our formalism, we will use similar notation for codes of formulas as for the formulas themselves; what we mean will be clear from the rest of the expression. Thus, in

$$S(\underline{x}) = \underline{y} \in E \leftrightarrow S(x) = y \tag{8}$$

$S(\underline{x}) = \underline{y}$ denotes a number that is a code of the formula built from the x^{th} and y^{th} numerals and the symbols for the successor function and equality, while $S(x) = y$ is just a formula of the language of PRA. In the rest of the paper $\vec{x}$ stands for $(x)_0, ...(x)_{lh(x)\dot{-}1}$, and capitals (e.g. E) are used for set variables whereas lower case letters (e.g. x) are used for number variables; in particular f is a numeral coding for a functional symbol in the following formulas. Consider the following formulas of RCA:

$$\begin{array}{lcl}
\Theta_1(n, E) & \equiv & \forall t(\mathcal{T}_{PRA}(n, t) \rightarrow \exists! y(t = \underline{y} \in E)) \\
\Theta_2(n, E) & \equiv & \forall x \forall y[(S(\underline{x}) = \underline{y} \in E \leftrightarrow S(x) = y) \wedge (\underline{x} = \underline{y} \in E \leftrightarrow x = y) \\
& \wedge & (\underline{y} = \underline{0} \in E \leftrightarrow y = 0)] \\
\Theta_3(n, E) & \equiv & \forall f[[\mathcal{L}_{PRA}(n, f) \wedge (\mathcal{G}(f))_0 = 0 \rightarrow \forall x, y, z(Ar(f) = lh(x) + 1 \\
& \rightarrow & (f(\underline{0}, \vec{\underline{x}}) = \underline{z} \in E \leftrightarrow g_f(\vec{\underline{x}}) = \underline{z} \in E) \wedge (f(\underline{y+1}, \vec{\underline{x}}) = \underline{z} \in E \\
& \leftrightarrow & h_f(\underline{y}, f(\underline{y}, \vec{\underline{x}}), \vec{\underline{x}}) = \underline{z} \in E))] \wedge [\mathcal{L}_{PRA}(n, f) \wedge (\mathcal{G}(f))_0 = 1 \\
& \rightarrow & \forall x, y(f(\vec{\underline{x}}) = \underline{y} \in E \leftrightarrow \exists z(lh(z) = Ar(h_f) \wedge h_f(\vec{\underline{z}}) = \underline{y} \in E \\
& \wedge & \forall i < lh(z)(g_i^f(\vec{\underline{x}}) = \underline{(z)_i} \in E)]] \\
\Theta_4(n, E) & \equiv & \forall t \forall z[\mathcal{T}_{PRA}(n, t) \rightarrow (t = \underline{z} \in E \leftrightarrow \exists f, y, v(\mathcal{L}_{PRA}(n, f) \\
& \wedge & lh(y) = lh(v) = Ar(f) \wedge \forall i < lh(y)(\mathcal{T}_{PRA}(n, (y)_i) \\
& \wedge & (y)_i = \underline{(v)_i} \in E \wedge t = f(\vec{y}) \wedge f(\vec{\underline{v}}) = \underline{z} \in E)]
\end{array}$$

Thus, Θ_1 asserts that E contains a unique evaluation of each term of the language of PRA restricted to the functional symbols smaller or equal than n. Θ_2 asserts that E contains all closed instances of the graphs of the initial functions and equality, while Θ_3 says that E contains all closed instances of the rules of primitive recursion and composition that define new functional symbols from the previous ones. The above properties of E imply that E correctly evaluates all standard primitive recursive functions. Θ_4 asserts that E evaluates terms inductively according to how they are built, which implies that E correctly evaluates all standard terms. Finally let $\Theta(n, E) \equiv \bigwedge_{i \leq 4} \Theta_i(n, E)$ and $J_{RCA}(n) \equiv \exists E \Theta(n, E)$.

Lemma 1 *$J_{RCA}(n)$ defines a cut in RCA*

Proof: The proof uses familiar techniques used for defining a (partial) truth predicate. Let the set E_0 consist of the codes of all formulas of the form $S(\underline{x}) = \underline{y}$ for all x and y such that $S(x) = y$ and of the codes of all formulas of the form $\underline{x} = \underline{x}$. It is easy to see that this set is Δ_1^0 definable and thus its existence can be proved in RCA. Assume now that there is an E_n such that $\Theta(n, E_n)$ holds for some n; we show that then there is an E_{n+1} such that $\Theta(n+1, E_{n+1})$ also holds;[7] this is sufficient to show that J_{RCA} is a cut in RCA as claimed. If n is not a functional symbol of $\mathcal{L}_{PRA}$ then set $E_n = E_{n+1}$; if it is, then in order to avoid possible notational confusion, denote n by a more standard letter f and consider the following two cases: *Case 1:* f is defined by primitive recursion from some g and h such that $g, h < f$; *Case 2:* f is defined by composition from some $h, g_1, ...g_k$, such that $Ar(h) = k$ and $h < f$, $g_i < f$ (here k can be nonstandard).

Case 1 (primitive recursion): Define first an auxiliary set $\overline{E_{n+1}}$ which extends evaluation for the function f; E_{n+1} will be obtained by extending such evaluation to all terms involving functional symbols smaller or equal to f. Thus, let

$$\overline{E_{n+1}} = E_n \cup \{f(\underline{y}, \vec{\underline{x}}) = \underline{z} : (y = 0 \wedge g(\vec{\underline{x}}) = \underline{z} \in E_n) \vee \exists v(g(\vec{\underline{x}}) = \underline{(v)_0} \in E_n \\ \wedge (\forall i < y) h(\underline{i}, \underline{(v)_i}, \vec{\underline{x}}) = \underline{(v)_{i+1}} \in E_n) \wedge (v)_y = z)\}$$

$\overline{E_{n+1}}$ is obviously definable via a Σ_1^0 formula ψ that corresponds to the right hand side of the above equation. By using the usual arguments, Σ_1^0 least number principle and the properties of E_n, it is easy to show that $\overline{E_{n+1}}$ has also a Π_1^0 definition in RCA (i.e. is Δ_1^0) and that $\forall f, y, x \exists! z(\mathcal{L}_{PRA}(n+1, f) \rightarrow \psi(f(\underline{y}, \vec{\underline{x}}) = \underline{z}))$.

Define now E_{n+1} as the set of all formulas of the form $t = \underline{k}$ such that there are v, h, w satisfying: $lh(v) = lh(w)$; v codes the sequence of terms from which t is inductively built, with $(v)_{lh(v) \dot{-} 1} = t$; h codes the sequence of functional symbols used to build higher complexity subterms of t from some of the simpler ones; w codes a sequence of numerals that represent the values of all the subterms of t. Thus, for all $i < lh(v)$, $(v)_i$ is built from some $(v)_{j_1}, ..., (v)_{j_s}, j_1, ..., j_s < i$ and a functional symbol $f_i = (h)_i$ of arity s. Also, whenever $(v)_i$ is a numeral, then $(v)_i = (w)_i$; otherwise, if $(v)_i = f((\vec{v})_j)$ then $(w)_i = f((\vec{w})_j) \in \overline{E_{n+1}}$; finally $(w)_{lh(w) \dot{-} 1} = \underline{k}$.

Exactly as before, E_{n+1} is Δ_1^0 definable and, consequently, a set in RCA. It is easy to check that if $\Theta(n, E_n)$ holds, then $\Theta(n+1, E_{n+1})$ holds as well.

[7] Here n is just a number variable of RCA and not necessarily a standard number.

Case 2 (composition) is handled similarly. ■

Lemma 2 *1. For all standard primitive recursive functions f we have:*

$$RCA \vdash \forall x, y, E, k[k > f \wedge \Theta(k, f) \rightarrow (f(\vec{\underline{x}}) = \underline{y} \in E \leftrightarrow f(\vec{x}) = y)]$$

2. For every standard term t of the language of PRA and for any sufficiently large k, RCA proves that if E satisfies $\Theta(k, E)$, then $\forall x(t = \underline{x} \in E \leftrightarrow t = x)$ holds.

Proof: Several facts about $\Theta(m, E)$ can be established; it is possible to verify that if $m > n$ and E_m and E_n are such that $\Theta(m, E_m)$ and $\Theta(n, E_n)$, then E_m and E_n "agree" about the evaluation of terms t such that $\mathcal{L}_{PRA}(n, t)$. In this sense the sequence of sets is monotonic.

Working within RCA, assume that $\Theta(k, E)$ holds for all t, k, E where t is a term of PRA all of whose free variables are among $x_1, ..., x_s$ and all functional symbols are smaller or equal than k. Assume also that $t_1, ..., t_s$ is a sequence of closed terms such that $\forall i < s\ \mathcal{T}_{PRA}(k, t_i)$, and $\forall m, n_1, ..., n_s(\forall i < s)t_i = \underline{n_i} \in E$. Then $t(\underline{n_1}, ..., \underline{n_s}) = \underline{m} \in E$ if and only if $t(t_1, ..., t_s) = \underline{m} \in E$. This is proved by an easy Π^0_1 induction on the complexity of t, using the properties of E given by $\Theta(k, E)$.

Finally, by an easy Π^0_1 induction on the complexity of t, using the properties of E given by $\Theta(k, E)$, we can verify that it is provable in RCA that for all t, k, E, if $\Theta(k, E)$ holds and t is a term of PRA all of whose free variables are among $x_1, ..., x_s$ and all functional symbols are smaller or equal than k and $t_1, ..., t_s$ is a sequence of closed terms such that $\forall i < s\ \mathcal{T}_{PRA}(k, t_i)$ then for all $m, n_1, ..., n_s$ if $(\forall i < s)\ t_i = \underline{n_i} \in E$ then $t(\underline{n_1}, ..., \underline{n_s}) = \underline{m} \in E$ if and only if $t(t_1, ..., t_s) = \underline{m} \in E$.

We can now define a truth predicate for all *variable-free* formulas whose functional symbols are smaller or equal than k, providing that k belongs to the cut J_{RCA}. Note that by induction on the complexity of formulas it is easy to define a primitive recursive function L such that for every variable-free formula φ, $L(\varphi)$ is a term t such that φ is equivalent to the equation $t = 0$.

Let $\mathcal{F}_{PRA}(n, \varphi)$ be a formalization of "φ is a variable-free sentence of PRA such that all functional symbols appearing in it are less than or equal n"; then define $\Omega(n, E, T)$ by

$$\Omega(n, E, T) \equiv (\Theta(n, E) \wedge \forall \varphi(\varphi \in T \leftrightarrow (\mathcal{F}_{PRA}(n, \varphi) \wedge L(\varphi) = \underline{0} \in E))) \quad (9)$$

and

$$\overline{\Omega}(n, T) \leftrightarrow \exists E \Omega(n, E, T). \quad (10)$$

Then $\overline{\Omega}(n,T)$ satisfies the usual properties of a truth definition for all variable free formulas φ such that $\mathcal{F}_{PRA}(n,\varphi)$ holds. This can be easily proved using Π^0_1 induction and the above facts.

Note that whenever $\Theta(n,E)$ holds, then for T defined by $T_n = \{\varphi : \mathcal{F}_{PRA}(n,\varphi) \wedge L(\varphi) = \underline{0} \in E_n\}$, we have $\Omega(n,E,T)$. Thus, whenever $J_{RCA}(n)$, there exists some T such that $\overline{\Omega}(n,T)$ holds.

In particular, (i) for each standard variable-free formula φ one can prove in RCA the formula

$$\forall n, T(\overline{\Omega}(n,T) \wedge n > \lceil\varphi\rceil \rightarrow (\lceil\varphi\rceil \in T \leftrightarrow \varphi)); \tag{11}$$

(ii) RCA proves that for all n, T, t, m and φ, if $\overline{\Omega}(n,T)$ and if φ is a quantifier-free formula all of whose free variables are among $x_1, ..., x_s$ then $(\forall i < s)(\mathcal{T}_{PRA}(n,(t)_i) \wedge t_i = \underline{(m)_i} \in T \rightarrow (\varphi(\vec{t}) \in T \leftrightarrow \varphi(\underline{(m)_i}) \in T)$.

The proof is by Π^0_1 induction on the complexity of φ.

Finally, using the definition of $\Omega(n,E,T)$, it is easy to verify within RCA the following fact. Assume that $\theta(\vec{x})$ is either an equality axiom or an axiom of PRA which is not an induction axiom, and that $\theta(\vec{x})$ has only functional symbols smaller or equal to n. Also assume that n, E, T, and $\vec{t}$ are such that $\Omega(n,E,T)$ holds. Then $(\forall i < lh(t))(\mathcal{T}_{PRA}(n,(t)_i)) \rightarrow \theta(\vec{t}) \in T$. ■

For the next step of the proof of (1) we must switch from the Hilbert type proof system to a Gentzen type proof system (see [22]) because we want to use a partial cut elimination theorem. The equivalence of these two proof systems is provable in $I\Sigma_1$, and the proof transformation converting a Hilbert style proof into a Gentzen style proof does not change the language of the formulas of the proof. We use the following fact whose proof is effective and thus formalizable in $I\Sigma_1$ (PRA in fact). For a proof, see [22], p. 116.

Proposition 2 *There is a primitive recursive procedure for transforming any proof p in PRA of a sequent $\Gamma \Rightarrow \Delta$ into a proof p^* of the same sequent such that p^* has the following properties:*

(i) the language of p^* contains only functional symbols of the language of p;

(ii) all initial sequents of p^* are of the form $\varphi(\vec{t})$ where $\varphi(\vec{x})$ is either a logical axiom or an equality axiom or an (open) axiom of PRA which is not an induction axiom and where $\vec{t}$ is a sequence of terms of the appropriate length;

(iii) instead of the induction axioms of PRA we have the induction rule of the form

$$\frac{\Gamma, \varphi(a) \Rightarrow \varphi(a+1), \Delta}{\Gamma, \varphi(0) \Rightarrow \varphi(t), \Delta}$$

where φ is a quantifier-free formula and t is a term; the variable a cannot appear in $\Gamma, \varphi(0), \Delta$, or t. (As is usual in proof-theory, we use the first few letters of the alphabet to denote free variables while the last few denote the bound ones.)

(iv) all cuts of p^* are on quantifier-free formulas only.

Such proofs are called *free cut-free proofs*. The free cut-free proofs can be much lengthier than proofs involving arbitrary cuts, but, as we noted above, the process of partial cut elimination does not change the *language* of such proofs. Let $\mathcal{FP}_{PRA}(n, p)$ be a formalization of "p is a free cut-free proof of a quantifier-free sequent such that all formulas of the proof contain only functional symbols smaller or equal than n."

Working within RCA, consider a proof p^* such that $\mathcal{FP}_{PRA}(n, p^*)$ holds for some n and let T be such that $\overline{\Omega}(n, T)$ holds, where $\overline{\Omega}$ is defined identically to the previous lemma. We want to associate to each such proof p^* and such T a tree of sequents $\overline{p}$ which contains only variable-free sentences of PRA and which we call *a proof transform of p^* relative to T*. To do so, we move backwards through the proof p^* (i.e. from the conclusions towards the axioms). We first replace all the free variables of the conclusion of the proof by 0's throughout the proof. Assume we are at a height i. If the inference from a sequent at height $i+1$ to a sequent at height i is by a propositional rule we move one step upwards without changing anything. Since all cuts are on quantifier-free formulas and the conclusion of the proof contains no formulas with quantifiers, no quantifier rules are used in the proof. If the inference is a cut on a quantifier-free formula $\varphi(\vec{x})$, replace $\vec{x}$ by $0, 0, ..., 0$ in the entire part of the proof above and including the cut. If it is an application of the induction rule of the form

$$\frac{\Gamma, \varphi(a) \Rightarrow \varphi(a+1), \Delta}{\Gamma, \varphi(0) \Rightarrow \varphi(t), \Delta}$$

then all variables in t must have been previously replaced by numerals and so we can assume that t is closed. Replace a by a numeral $\underline{m \dot{-} 1}$ such that

$$m = \mu x \leq k(\varphi(\underline{x}) \notin T)$$

for a unique k such that $t = \underline{k} \in T$ and where the bounded μ-operator is defined as usual: $(\mu x \leq k)\theta(x)$ is the least $x \leq k$ such that $\theta(x)$ holds if such an x exists, and $x = k+1$ otherwise. Such an m always exists by the least number principle applied to the simple formula $\varphi(\underline{x}) \notin T \vee x = k+1$.

It is easy to see that the statement "p^* is a proof transform of a proof p such that $\mathcal{FP}_{PRA}(n, p)$ holds" can be formalized by a Δ_1^0 formula.

The following Claim can easily be proved by Σ_1 induction on the length of the proof p.

Claim 1 *RCA proves that for all p, n, T such that $\mathcal{FP}_{PRA}(n, p)$ and $\Omega(n, T)$ hold, there exists p^* such that p^* is a proof transform of p with respect to T.*

Proof of Proposition (1), i.e. that

$$RCA \vdash \forall x(J_{RCA}(x) \rightarrow \neg Pr_{PRA}(x, \lceil 1 = 0 \rceil))$$

We work inside RCA; assume p is a proof of $1 = 0$ in PRA such that $J_{RCA}(p)$ holds. Let T_p be such that $\overline{\Omega}(p, T_p)$ holds. We first transform this proof into a Gentzen style proof of $\Rightarrow 1 = 0$ and then get a free cut-free proof p^* of $\Rightarrow 1 = 0$ of the *same* language as p. Thus, all functional symbols of p^* are smaller than p, and consequently $\mathcal{FP}_{PRA}(p, p^*)$ holds.

Let now $\overline{p}$ be a proof transform of p^* with respect to T_p. All the initial segments of $\overline{p}$ belong to T_p since they are of the form $\psi(\vec{t})$ where $\psi(\vec{x})$ is a logical axiom, an equality axiom, or an axiom of PRA which is not an induction axiom, and t is a closed term. An easy induction on height i, smaller or equal to the height of $\overline{p}$, shows that if all the formulas in Γ of a sequent $\Gamma \Rightarrow \Delta$ on the height i belong to T_p, then there is a formula in Δ that also belongs to T_p. The induction step in proving this claim is easy; in the case of a propositional or cut rule, it follows immediately from the properties of T_p, whereas in the case of the induction rule it, follows from our choice of m in defining the proof transform of a proof. More precisely, consider

$$\frac{\Gamma, \varphi(\underline{m \dot{-} 1}) \Rightarrow \varphi(\underline{m}), \Delta}{\Gamma, \varphi(0) \Rightarrow \varphi(t), \Delta}$$

Assume that all formulas in Γ and $\varphi(\underline{0})$ belong to T_p but neither $\varphi(t)$ nor any formula in Δ belong to T_p. This implies that there is a least $x \leq t$ such that $\varphi(\underline{x}) \notin T_p$ and it must be m by our choice. Since $\varphi(0) \in T_p$ then $m \dot{-} 1 \neq m$ and $\varphi(\underline{m \dot{-} 1}) \in T_p$. But then all formulas in Γ and $\varphi(\underline{m \dot{-} 1})$ belong to T_p and no formula in Δ or $\varphi(\underline{m})$ belong to T_p which contradicts the inductive hypothesis. Thus, since the final sequent is $\Rightarrow 1 = 0$, we conclude that $1 = 0$ belongs to T_p, which contradicts the demonstrated properties of T_p. This finishes our proof of Lemma (1). ■

The presence of second order objects (e.g. sets) and Δ_1^0 comprehension are not essential; it is possible to carry out a proof of the analogous claim for the first order theory $I\Sigma_1$, by using codes for recursive sets rather than the sets themselves. However, using sets rather than codes is arguably more intuitive. The corresponding result for $I\Sigma_1$ follows from the following well know fact.

Proposition 3 *RCA is interpretable in $I\Sigma_1$ with unchanged domain of numbers.*

The interpretation **I** does not change the domain of numbers and all first order operations and relations remain the same. Let $Tr_{\Sigma_1}((x,y)$ be the usual truth definition in $I\Sigma_1$ for the first order Σ_1 formulas. The domain of sets is defined by $\Sigma(w) \equiv \forall y(Tr_{\Sigma_1}((w)_0, y) \leftrightarrow \neg Tr_{\Sigma_1}((w)_1, y))$, while $y \in X$ is interpreted as $Tr_{\Sigma_1}((w_X)_0, y)$. It is easy to see that under this interpretation all of the axioms of RCA are satisfied.

Corollary 1 *There is a cut $J_{I\Sigma_1}$ in $I\Sigma_1$ such that*

$$I\Sigma_1 \vdash \forall x(J_{I\Sigma_1}(x) \rightarrow \neg Pr_{PRA}(x, \ulcorner 1 = 0 \urcorner))$$

Proof: By Proposition (1) there is a cut J_{RCA} in RCA such that

$$RCA \vdash \forall x(J_{RCA}(x) \rightarrow \neg Pr_{PRA}(x, \ulcorner 1 = 0 \urcorner))$$

Thus, denoting by $J^{\mathbf{I}}_{RCA}$ the **I**-interpretation of $J^{\mathbf{I}}_{RCA}$, we have

$$I\Sigma_1 \vdash \forall x(J^{\mathbf{I}}_{RCA} \rightarrow \neg Pr_{PRA}(x, \ulcorner 1 = 0 \urcorner)) \tag{12}$$

Notice that if J_{RCA} is a cut in RCA then $J^{\mathbf{I}}_{RCA}$ is a cut in $I\Sigma_1$; use the fact that the interpretation **I** neither changes numbers nor the arithmetical operations and relations. Hence, we can take $J_{I\Sigma_1} = J^{\mathbf{I}}_{RCA}$. ■

We now introduce some notation from [15].

Definition 2 $Con_T(n) \equiv \neg\exists p(|p| \leq n \wedge Pr_T(p, \ulcorner 1 = 0 \urcorner))$.

Lemma 3 *There exists a cut K in $I\Sigma_1$ such that*

$$I\Sigma_1 \vdash \forall x(K(x) \rightarrow Con_{PRA}(x)) \tag{13}$$

Proof: To prove the Lemma we use Solovay's cut shortening technique [20] to get a cut $K(x)$ such that $\forall x(K(x) \rightarrow J_{I\Sigma_1}(2^x))$. K obviously satisfies ((3)). ■

We now prove a proposition analogous to Theorem 4.2 of [15], with $I\Sigma_1$ in place of GB and PRA in place of ZF.

Proposition 4 *There exists $\epsilon > 0$ and a polynomial p such that for every natural number k*

(i) $I\Sigma_1$ has a proof of length $p(k)$ of $Con_{PRA}(2^0_k)$;

(ii) PRA has no proofs of length $(2^0_k)^\epsilon$ of $Con_{PRA}(2^0_k)$.

Proof: Replace GB by $I\Sigma_1$ and ZF by PRA in the proof of Theorem 4.2 of [15], with the exception of the proof that there is a cut I in GB such that

$$GB \vdash \forall x(I(x) \rightarrow Con_{ZF}(x)); \tag{14}$$

instead we apply our Lemma (3).[8]

Part (i) of Proposition (4) follows from Lemma (3) and the fact that for any cut K there are polynomial size proofs of $K(2^0_n)$. This is based on Lemma 2.2 of [15], which describes how given a cut I one can construct a cut I_k such that $A \vdash I_k(x) \rightarrow \exists y(y = 2^x_k \wedge I(y))$, such that the proof is polynomial in k, where A contains or interprets Q; see [15] for details.

Part (ii) of Proposition (4) is proved via a modified Gödel type argument diagonalizing "$\varphi(x)$ is provable in PRA with a proof of length $\leq x$" rather than just "φ is provable in PRA" which we diagonalize in the standard Gödel argument. Again, for details see [15]. ■

Corollary 2 *$I\Sigma_1$ has roughly super exponential speed-up over PRA for quantifier free formulas.*

Proof: Since $Con_{PRA}(2^0_n)$ can be formalized as a quantifier-free sentence in the language of PRA by replacing the bounded quantifiers with their primitive recursive substitutes we can apply Proposition (4) to conclude that speed-up of $I\Sigma_1$ over PRA is not Kalmar-elementary. However, the usual cut elimination argument shows that the speed up is bounded by $P(2^x_x)$ for a suitable polynomial. Thus, the speedup is roughly super-exponential. ■

Proposition (3) also implies that RCA has at most polynomial speed-up over $I\Sigma_1$. The proof is straightforward, by estimating the size of the $I\Sigma_1$-interpretation of a proof in RCA. The exact speed-up depends on the particular type of the proof system one uses. For example, if we choose a Hilbert style proof system that allows the rule of universal generalization for several variables simultaneously and its axioms allow simultaneous instantiations of universal formulas by a sequence of terms, then the speed up is

[8]The usual proof of (4) is rather different from the proof of Lemma 2. The cut I is obtained by shortening a cut L that consists of all x for which there exists a satisfaction class in GB for all Π_x sentences of the language of ZF. Then one uses a formalized version of Montague's Reflection Theorem, in which a satisfaction class is used rather than the real truth in the set-universe to obtain a set model of the Π_x part of ZF whenever x belongs to L; we then apply the usual soundness argument for all proofs that belong to the cut L, which is possible since the complexity of each formula in the proof is smaller than the (Gödel code of) the proof itself. In our case such model theoretic argument is replaced by our proof theoretic considerations.

easily seen to be at most linear. For any other Hilbert style proof system the speed up is at most quadratic. The details are given in [9].

It was conjectured in [9] that in order to get a similar result for WKL versus RCA, one could try to adapt Harrington's forcing proof of the conservativeness of WKL over RCA for arithmetical sentences such that the proof in fact produces an interpretation of WKL in RCA which does not change the domain of numbers. This was shown to be the case in [1].

We now turn to Problems 2 and 3, and prove the following Propositions.

Proposition 5 *For any natural number n*

$$I\Sigma_1 \nvdash \forall x \exists y(|y| < 2_n^x \wedge Pr_{PRA}(y, \lceil Con_{I\Sigma_1}(\underline{x})\rceil).$$

Proof: Assume the opposite and let n be a natural number such that

$$I\Sigma_1 \vdash \forall x \exists y(|y| < 2_n^x \wedge Pr_{PRA}(y, \lceil Con_{I\Sigma_1}(\underline{x})\rceil).$$

Consider the shortening $S(x)$ of the cut $K(x)$ constructed in the proof of Lemma (3). $S(x)$ is closed for $+$ and $\cdot$ and thus also for any polynomial with natural coefficients; now take a shortening $S_n(x)$ of the cut $S(x)$ with the property

$$I\Sigma_1 \vdash \text{“}S_n(x) \text{ is a cut contained in } S\text{”} \wedge \forall x(S_n(x) \rightarrow S(2_n^x))$$

S_n can be constructed by iterating the technique of Solovay from [20] mentioned in the proof of Lemma 2; see also [14]. By a result of Pudlák (Theorem 2.1 of [14]), there exists a model $\mathcal{A}$ of $I\Sigma_1$ containing in S_n an $\mathcal{A}$-proof p of a contradiction from $I\Sigma_1$, i.e. such that $\mathcal{A} \models S_n(p) \wedge Pr_{I\Sigma_1}(p, \lceil 1 = 0\rceil)$. Since we can check in PRA the syntax of a sequence of formulas and determine whether it is a correct proof in $I\Sigma_1$, and since this can be done in polynomially many steps in the length of the sequence, there is a proof $p^* \in \mathcal{A}$ of length polynomial in the length of p such that

$$\mathcal{A} \models Pr_{PRA}(p^*, \lceil Pr_{I\Sigma_1}(p, \lceil 1 = 0\rceil)\rceil)$$

Thus, for some polynomial $P(x)$ with natural coefficients and some p' obtained from p^* in the obvious way, we get

$$\mathcal{A} \models Pr_{PRA}(p', \lceil \neg Con_{I\Sigma_1}(|p|)\rceil) \wedge |p'| \leq P(|p|)$$

On the other hand, by assumption, for some $\overline{p} \in \mathcal{A}$,

$$\mathcal{A} \models Pr_{PRA}(\overline{p}, \lceil Con_{I\Sigma_1}(|p|)\rceil) \wedge |\overline{p}| < 2_n^{|p|}$$

Thus, since $|p| < p$, $S_n(|p|)$ and so $S(|\overline{p}|)$. Combining p' and $\overline{p}$ we can clearly get a proof $p^{\#}$ of an inconsistency in PRA whose length is polynomial in the lengths of $\overline{p}$ and p, and so by our assumption about closure properties of the cut S, $S(|p^{\#}|)$ which is a contradiction since S is a shortening of K and $I\Sigma_1 \vdash \forall x(K(x) \rightarrow Con_{PRA}(x))$.

This theorem clearly justifies our conclusion concerning Problem 3.

Proposition 6 *There is a function g_{WKL} with a roughly super-exponential growth rate such that*

$$PRA \vdash \forall x \exists y(|y| < f(x) \wedge Pr_{PRA}(y, \ulcorner Con_{WKL}(\underline{x}) \urcorner))$$

Proof: From a result of Sieg (see [16]), there exists a primitive recursive function g such that if $\Pi_2(x)$ formalizes the predicate that recognizes (codes of) Π_2 sentences in the language of PRA, then

$$PRA \vdash \forall \varphi \forall p(\Pi_2(\varphi) \rightarrow (Pr_{WKL}(p, \varphi) \rightarrow Pr_{PRA}(g(p), \varphi))$$

Any such g formalizes a proof transformation procedure that first eliminates cuts and then performs some other proof transformations that do not increase lengths of proofs significantly compared to the roughly super-exponential growth rate of the cut elimination procedure. Therefore, g is dominated by a monotone function h of roughly super-exponential growth rate; consequently, we have

$$PRA \vdash \forall x(Con_{PRA}(h(x)) \rightarrow Con_{WKL}(x))$$

As a consequence of Pudlák's result as mentioned above, we have that

$$PRA \vdash \forall x \exists y(|y| < (h(x))^k \wedge Pr_{PRA}(y, Con_{PRA}(\underline{h(x)})))$$

We also conclude from Sieg's theorem that for a standard natural number c

$$PRA \vdash Pr_{PRA}(\underline{c}, \ulcorner \forall x(Con_{PRA}(h(x)) \rightarrow Con_{WKL}(x)) \urcorner)$$

which obviously implies that there is a function f with a roughly super-exponential growth rate such that

$$PRA \vdash \forall x \exists y(|y| < f(x) \wedge Pr_{PRA}(y, Con_{WKL}(x))$$

Since we have $PRA \subset I\Sigma_1 \subset RCA \subset WKL$, (and provably so in PRA for the corresponding representation of the axioms of these theories) Propositions 5 and 6 imply that $f_{I\Sigma_1}, f_{RCA}$, and f_{WKL} all have a roughly

super-exponential growth rate, which justifies the claims we made in the comments after Problem 2.

We conclude with the following remark. As we have seen, the relationship between $I\Sigma_1$ and PRA is quite similar to the relationship between GB and ZF. It is now natural to ask if there are other, natural pairs of theories with similar relationship, both stronger that the pair $I\Sigma_1$ and PRA, say some fragments of Predicative Analysis, as well as weaker than this pair, say for theories of Second Order Feasible Arithmetic and First Order Feasible Arithmetic like Buss' Bounded Arithmetic S_2^1 (see[2]).

References

[1] J. Avigad: *Formalizing forcing arguments in subsystems of second-order arithmetic*, *Annals of Pure and Applied Logic*, vol. 82, 1996, pp. 165-191.

[2] S. Buss: *Bounded Arithmetic*, Bibliopolis, 1986.

[3] D.K. Brown: *Subsystems of Second Order Arithmetic*, Ph.D. Thesis, Pennsylvania State University, 1987.

[4] H. Enderton: *A Mathematical Introduction to Logic*, Academic Press, 1972.

[5] S. Feferman: *Systems of Predicative Analysis*, *The Journal of Symbolic Logic*, vol. 29, 1964, pp. 1-30.

[6] P. Hájek: On interpretability of theories containing arithmetic. II, *Commentationes Mathematicae Universitatis Carolinae*, vol. 22, 1981, pp. 667-688.

[7] P. Hájek: *Interpretability and fragments of arithmetic*, in *Arithmetic, Proof Theory, and Computational Complexity*, editors Peter Clote and Jan Krajíček, Oxford, 1993, pp. 185-196.

[8] D. Hilbert and P. Bernays: *Grundlagen der Mathematik* I, II; 2. Auflage, Springer, Berlin, 1968/70

[9] A. Ignjatović: *Fragments of first- and second-order arithmetic and length of proofs*, Ph.D. Thesis, University of California at Berkeley, Berkeley, California, 1990.

[10] A. Ignjatović: *Hilbert's Program and the ω-rule*, *The Journal of Symbolic Logic*, vol. 59, Number 1, 1994, pp. 322-343.

[11] D. Isaacson: *Arithmetical truth and hidden higher-order concepts*, in *Logic Colloquium '85*, edited by the Paris Logic Group, North Holland, 1987.

[12] G. Kreisel: *What can be done for Mathematical Logic*, in Schoenman, Ralph (ed.), *Bertrand Russell: Philosopher of the Century*, Allen and Unwin, London, pp. 273-303.

[13] J. Paris and C. Dimitracopulos, *A note on undefinability of cuts*, *JSL* vol. 48, 1983, pp. 564-569.

[14] P. Pudlák: *Cuts, Consistency Statements and Interpretations*, *The Journal of Symbolic Logic*, vol. 50, 1985, pp. 423-441.

[15] P. Pudlák: *On the length of proofs of finitistic consistency statements in first-order theories*, *Logic Colloquium '84*, J.B. Paris, A.J.Wilkie and G.M.Wilmers (Editors) North-Holland, 1986.

[16] W. Sieg: *Fragments of arithmetic*, *Annals of Pure and Applied Logic*, vol. 28, 1985, pp. 33-71.

[17] S. G. Simpson and R.L. Smith: *Factorization of polynomials and Σ^0_1-induction*, *Annals of Pure and Applied Logic*, vol. 31, 1986, pp. 289-306.

[18] S. G. Simpson: *Partial realization of Hilbert's Program*, *Journal of Symbolic Logic*, vol. 53, 1988, pp. 349-363.

[19] S.G. Simpson: *Subsystems of Second Order Arithmetic*, Springer-Verlag, 1998.

[20] R. Solovay: *Letter to P. Hájek*; see also [6] and [13].

[21] W. W. Tait: *Finitism*, *Journal of Philosophy*, vol. 78, 1981, pp. 524-546.

[22] G. Takeuti: *Proof Theory*, second edition, North-Holland, 1987.

[23] S. S. Wainer. *Ordinal recursion, and a refinement of the extended Grzegorczyk hierarchy*, *The Journal of Symbolic Logic*, vol 37, 1972, pp. 281-292,

School of Computer Science and Engineering
The University of New South Wales
Sydney, NSW 2052, Australia

and

National ICT Australia
Sydney, NSW 2052, Australia