Logic, Methodology and Philosophy of Science IX
D. Prawitz, B. Skyrms and D. Westerståhl (Editors)

THE WITNESS FUNCTION METHOD AND PROVABLY RECURSIVE FUNCTIONS OF PEANO ARITHMETIC

SAMUEL R. BUSS*

Department of Mathematics
University of California, San Diego, La Jolla, CA 92093-0112, USA
sbuss@ucsd.edu

1. Introduction

The witness function method has been used with great success to characterize some classes of the provably total functions of various fragments of bounded arithmetic [2, 4, 18, 23, 17, 16, 5, 6, 1, 7, 8]. In this paper, it is shown that the witness function method can be applied to the fragments $I\Sigma_n$ of Peano arithmetic to characterize the functions which are provably recursive in these fragments. This characterization of provably recursive functions has already been performed by a variety of methods; including: via Gentzen's assignment of ordinals to proofs [9, 27], with the Gödel Dialectica interpretation [12, 13], and by model-theoretic methods (see [20, 15, 26]). The advantage of the methods in this paper is, firstly, that they provide a simple, elegant and purely proof-theoretic method of characterizing the provably total functions of $I\Sigma_n$ and, secondly, that they unify the proof methods used for fragments of Peano arithmetic and for bounded arithmetic.

The witness function method is related to the classical proof-theoretic methods of Kleene's recursive realizability, Gödel's Dialectica interpretation and the Kreisel no-counterexample interpretation; however, the witness function method does not require the use of functionals of higher type. We feel that the witness function method provides an advantage over the other methods in that it leads to a more direct and intuitive understanding of many formal systems. The classical methods are somewhat more general but are also more cumbersome and more difficult to understand (consider the difficulty of comprehending the Dialectica interpretation or no-counterexample interpretation of a formula with more than three alternations of quantifiers,

*Supported in part by NSF grants DMS-8902480 and INT-8914569.

for instance). On the other hand, the more direct and intuitive witness function method has been extremely valuable for the understanding of *why* the provably total functions of a theory are what they are and also for the formulation of new theories for desired classes of computational complexity and, conversely, for the formulation of conjectures about the provably total functions of extant theories. The main support for our favorable opinion of the witness function method is, firstly, its successes for bounded arithmetic and, secondly, the results of this paper showing its applicability to Peano arithmetic.

While checking references for this paper, the author read Mints [19] for the first time — it turns out that Mints's proof that the provably recursive functions of $I\Sigma_1$ are precisely the primitive recursive functions is based on what is essentially the witness function method. This theorem of Mints is, in essence, Theorem 9 below. Mints's use of the witness function method predates its independent development by this author for applications to bounded arithmetic. The present paper expands the applicability of the witness function method to all of Peano arithmetic.

The outline of this paper is as follows: section 2 develops the necessary background material on Peano arithmetic, the subtheories $I\Sigma_n$, transfinite induction axioms, least ordinal principle axioms, the sequent calculus and the correct notion of free-cut free proof for transfinite induction/least number principle axioms. In section 3, the central notions of the witness function method and witness oracles are developed and the Σ_n-definable functions of $I\Sigma_n$ and $I\Delta_0 + TI(\omega_m, \Pi_n)$ are characterized. This includes the definition of α-primitive recursive (in Σ_k) functions and normal forms for such functions. Then the provably recursive (i.e., Σ_1-defined) functions of $I\Sigma_n$ are characterized by proving a conservation theorem for $TI(\omega_m, \Pi_n)$ over $TI(\omega_{m+1}, \Pi_{n-1})$. Section 4 outlines a proof of Parsons's theorem on the conservativity of the Π_{n+1}-induction rule over the Σ_n-induction axiom. Section 5 contains a proof of the Π_{n+1}-conservativity of $B\Sigma_{n+1}$ over $I\Sigma_n$. Section 6 concludes with a discussion of the analogies between the methods of this paper and the methods used for bounded arithmetic.

2. Preliminaries

2.1. Arithmetic and ordinals

Peano arithmetic (PA) is formulated[2] in the language 0, S, $+$, $\cdot$ and $\leq$.

[2] Our formulation of PA is similar to the usual one in [21] except that it has different non-induction axioms and has $\leq$ instead of $<$. It is easily seen that our definition of $I\Sigma_n$ and PA is equivalent to the usual one apart from the inessential replacement of $<$ by $\leq$.

It has induction axioms

$$A(0) \wedge (\forall x)(A(x) \rightarrow A(S(x))) \rightarrow (\forall x)A(x)$$

for all formulas A, plus it has a finite base set of axioms, namely, Robinson's theory Q of seven axioms defining 0, S, $+$ and $\cdot$ and, in addition, the axiom

$$(\forall x)(\forall y)(x \leq y \leftrightarrow (\exists z)(x + z = y))$$

which defines $\leq$. A *bounded quantifier* is of the form $(\exists x \leq t)$ or $(\forall x \leq t)$ where t is any term not involving x. The usual quantifiers, $(\forall x)$ and $(\exists x)$, are called *unbounded quantifiers.* The Δ_0-formulas, or *bounded formulas*, are the formulas in which every quantifier is bounded. The classes Σ_n and Π_n of formulas are defined by induction on n, so that $\Sigma_0 = \Pi_0 = \Delta_0$ and so that Σ_{n+1} is the set of formulas of the form $(\exists \vec{x})B$ where $B \in \Pi_n$ and so that Π_{n+1} is defined dually. The theory $I\Sigma_n$ is defined to be the theory in the language of Peano arithmetic with the same eight non-induction axioms as PA and with induction axioms for all formulas $A \in \Sigma_n$.

The collection axioms provide an alternative way to define fragments of Peano arithmetic. A collection axiom is of the form

$$(\forall x \leq t)(\exists y)A(x,y) \rightarrow (\exists z)(\forall x \leq t)(\exists y \leq z)A(x,y).$$

We let $B\Sigma_n$ denote the set of collection axioms for all $A \in \Sigma_n$; $B\Pi_n$ is defined similarly. It is well-known that $I\Delta_0 + B\Sigma_{n+1} \vDash I\Sigma_n$ and $I\Sigma_n \vDash B\Sigma_n$. It is also well-known that $I\Delta_0 + B\Sigma_{n+1}$ is Π_{n+1}-conservative over $I\Sigma_n$ and we shall reprove this in section 5 below. An important feature of the collection axioms is that it provides a 'quantifier exchange' principle that allows moving bounded quantifiers inside the scope of unbounded quantifiers. The classes Σ_n and Π_n can be generalized to classes Σ_n^G and Π_n^G by allowing bounded quantifiers to appear anywhere in the formula (instead of only in the Δ_0 matrix) but counting only the alternations of unbounded quantifiers. For example, the hypothesis and conclusion of the collection axiom above are Σ_n^G-formulas if $A \in \Sigma_n$. The theory $I\Delta_0 + B\Sigma_n$, and hence $I\Sigma_n$, can prove that every Σ_n^G-formula is equivalent to a Σ_n-formula.

Remark: Some authors include function symbols for all primitive recursive functions in the language of PA. We do not adopt this convention; however, as is well-known, every primitive recursive function is provably recursive (Σ_1-definable, see below) in $I\Sigma_1$ and hence the theories $I\Sigma_n$, for $n \geq 1$ are not significantly affected by the addition of symbols for primitive recursive functions. Thus the theorems and proofs of this paper also apply to theories with symbols for primitive recursive functions.

Definition Let T be a subtheory of PA and $f : \mathbb{N}^k \to \mathbb{N}$. The function f is Σ_i-definable in T iff there is a formula $A(x_1, \ldots, x_k, y) \in \Sigma_i$ such that

(1) $T \vdash (\forall \vec{x})(\exists! y) A(\vec{x}, y)$, and

(2) $\{(\vec{n}, m) : \mathbb{N} \vDash A(\vec{n}, m)\}$ is the graph of f, i.e., $A(\vec{n}, m)$ holds iff $f(\vec{n}) = m$ for all integers $\vec{n}, m$.

The function f is *provably recursive in* T iff f is Σ_1-definable in T.

The intuitive idea of 'provably recursive' is that the theory T should prove that some Turing machine M, which computes f, halts on all appropriate inputs. Since $A(\vec{x}, y)$ can be taken to be a Σ_1-formula expressing "there is a w which codes a halting M-computation with input $\vec{x}$ and output y", it is clear that any function which is provably recursive in this intuitive sense is also Σ_1-definable. Conversely, if f is Σ_1-definable in T, then there is Turing machine M which computes f, provably in T. Namely, M performs a brute-force search for values of y and the unboundedly existentially quantified variables of A. Thus 'Σ_1-definable' coincides with the intuitive notion of 'provably recursive'.

One reason that the provably recursive functions of T are of particular significance is that if f is provably recursive in T, then T may be conservatively extended by adding f as a new function symbol with $f(\vec{x}) = y \leftrightarrow A(\vec{x}, y)$ as a new axiom. If T is a fragment $I\Sigma_n$ then f may be used freely in induction formulas (without affecting quantifier complexity). Similarly, if T can prove that a Π_1-formula and a Σ_1-formula are equivalent then T can be conservatively extended by adding a new predicate symbol with arguments including the free variables of the two formulas and adding a new axiom defining the predicate symbol to be equivalent to the formulas. The new predicate may also be used freely in induction formulas. Such new predicates are called Δ_1*-defined predicates of* T.

Recall that $I\Sigma_1$ (and even $I\Delta_0$) can formalize many metamathematical notions; of particular importance are the sequence coding functions $\langle x_0, \ldots, x_k \rangle$, $(\langle x_0, \ldots, x_k \rangle)_i = x_i$, and $Len(\langle x_0, \ldots, x_k \rangle) = k + 1$.

The ordinals are set-theoretically defined to be those sets which are transitive and well-founded by $\in$. We write $\prec$ for the ordering of ordinals, so $\alpha \prec \beta$ means $\alpha \in \beta$. It is well-known how to define ordinal addition, multiplication and exponentiation. The Cantor normal form for an ordinal α is the unique expression

$$\alpha \quad = \quad \omega^{\gamma_1} \cdot n_1 + \omega^{\gamma_2} \cdot n_2 + \cdots \omega^{\gamma_r} \cdot n_r$$

where $\gamma_1 \succ \gamma_2 \succ \cdots \succ \gamma_r$ are ordinals and $n_1, \ldots, n_r$ are positive integers (i.e., nonzero, finite ordinals). Here ω is the first infinite ordinal; we let

$\omega_0 = 1$, $\omega_1 = \omega$ and, generally, $\omega_{n+1} = \omega^{\omega_n}$. Thus ω_n is a stack of n ω's. The limit of ω_n as $n \to \omega$ is called ϵ_0; hence ϵ_0 is the least ordinal such that $\epsilon_0 = \omega^{\epsilon_0}$. For $\alpha \prec \epsilon_0$, the Cantor normal form can be extended so that the exponents γ_i are also written in Cantor normal form, and with exponents in the latter Cantor normal forms also in Cantor normal form, etc. (eventually the process must stop). For example,

$$\omega^{\omega^{\omega^0 \cdot 3} + \omega^{\omega^0 \cdot 2}} \cdot 4 + \omega^0$$

is a Cantor normal form; usually this is expressed more succinctly as $\omega^{\omega^3+\omega^2} \cdot 4 + 1$. In this paper, we shall always use ordinals $\preccurlyeq \epsilon_0$ and by Cantor normal form always means the extended version with exponents also in Cantor normal form. ϵ_0 is its own Cantor normal form.

By using Gödel numbering, integers can encode Cantor normal forms and this can be intensionally formalized[3] in $I\Sigma_1$; with care, these can even be formalized in $I\Delta_0$. In particular, $I\Delta_0$ can define the relation *IsOrdinal*(x) expressing that x is the Gödel number of an ordinal, the relation $x \prec y$, and the functions for ordinal addition, multiplication and exponentiation. To avoid excessive notation, we use the same notation for actual and for metamathematical operations; for example, $\omega + 1$ also denotes its own Gödel number. However, there will occasionally be situations where context is not sufficient to distinguish between ordinals and their Gödel numbers: this occurs when n may be either an integer or a finite ordinal; to resolve ambiguity, we write $\ulcorner n \urcorner$ for the Gödel number of the ordinal n and we write n for the integer n. To improve readability, we use $\alpha, \beta, \gamma, \ldots$ and $\rho, \sigma, \tau, \ldots$ as variables that range over Gödel numbers of ordinals. For example, the formula $(\forall \sigma \prec \beta)(\cdots)$ abbreviates the first-order formula

$$\mathit{IsOrdinal}(\beta) \land (\forall x)(\mathit{IsOrdinal}(x) \land x \prec \beta \to \cdots).$$

Note that $\forall \sigma \prec \beta$ corresponds to an *unbounded* quantifier unless β is known to code a finite ordinal.

Transfinite induction on ordinals may be used to provide alternate axiomatizations for fragments of Peano arithmetic:

Definition Let Ψ be a set of formulas and let $\kappa \preccurlyeq \epsilon_0$. Then $TI(\kappa, \Psi)$ is the set of axioms

$$(\forall \gamma \preccurlyeq \kappa)[(\forall \beta \prec \gamma)A(\beta) \to A(\gamma)] \to A(\kappa) \tag{1}$$

where A is a formula in Ψ, possibly with other free variables as parameters.

[3] 'Intensionally formalized' means that $I\Sigma_1$ can prove simple syntactic facts about ordinal encodings and about operations on encoded ordinals.

The *least ordinal principle* axioms $LOP(\kappa, \Psi)$ are

$$A(\kappa) \to (\exists\gamma \preccurlyeq \kappa)[A(\gamma) \wedge (\forall\beta \prec \gamma)(\neg A(\beta))] \tag{2}$$

where $A \in \Psi$ and A may have parameter variables. For a fixed formula A, the axioms (1) and (2) are called $TI(\kappa, A)$ and $LOP(\kappa, A)$, respectively.

$TI(\prec \kappa, \Psi)$ is the theory $\cup_{\mu \prec \kappa} TI(\mu, \Psi)$.

$LOP(\prec \kappa, \Psi)$ is the theory $\cup_{\mu \prec \kappa} LOP(\mu, \Psi)$.

A slight variation on the least ordinal principle and transfinite induction axioms is

$$TI^*(\kappa, \Psi): \qquad (\forall\gamma \preccurlyeq \kappa)[(\forall\beta \preccurlyeq \gamma)A(\beta) \to A(\gamma)] \to (\forall\gamma \preccurlyeq \kappa)A(\gamma)$$

$$LOP^*(\kappa, \Psi): \qquad (\exists\gamma \preccurlyeq \kappa)A(\gamma) \to (\exists\gamma \preccurlyeq \kappa)[A(\gamma) \wedge (\forall\beta \prec \gamma)(\neg A(\beta))].$$

For Ψ one of the classes Σ_n or Π_n, $TI^*(\kappa, \Psi)$ is equivalent to $TI(\kappa, \Psi)$ since the former obviously implies the latter and since $TI^*(\kappa, A)$ may be inferred from $TI(\kappa, B)$ where $B(\alpha)$ is $A(\alpha) \vee (\alpha \succ \gamma' \wedge A(\gamma'))$, where γ' is a new variable acting as a parameter. Similarly, LOP^* and LOP are equivalent for Ψ one of the classes Σ_n or Π_n.

This paper is concerned primarily with the axioms $TI(\prec \omega_m, \Sigma_n)$ and $LOP(\prec \omega_m, \Sigma_n)$ where $m \geq 2$ and $n \geq 0$. The next two propositions give equivalences among such axioms (see [26] for generalizations of these propositions).

PROPOSITION 1 *Let $m \geq 2$ and $n \geq 0$.*

(a) $I\Delta_0 + TI(\prec \omega_m, \Sigma_n) \equiv I\Delta_0 + LOP(\prec \omega_m, \Pi_n)$

(b) $I\Delta_0 + TI(\prec \omega_m, \Pi_n) \equiv I\Delta_0 + LOP(\prec \omega_m, \Sigma_n)$

(c) $I\Delta_0 + LOP(\prec \omega_m, \Pi_n) \equiv I\Delta_0 + LOP(\prec \omega_m, \Sigma_{n+1})$

(d) $I\Delta_0 + TI(\prec \omega_m, \Sigma_n) \equiv I\Delta_0 + TI(\prec \omega_m, \Pi_{n+1})$

Proof (a) and (b) are trivial since $TI(\kappa, A)$ and $LOP(\kappa, \neg A)$ are logically equivalent (essentially, contrapositives). For (c), if $A \in \Sigma_{n+1}$ then $A(\rho)$ must be $(\exists\vec{y})B(\rho, \vec{y})$ where $B \in \Pi_n$. Now, $LOP(\kappa, A)$ follows from $LOP^*(\omega \cdot \kappa + \omega, C)$ where $C(\rho)$ is the Π_n-formula expressing

> "ρ encodes an ordinal $\omega \cdot \kappa + \langle\vec{y}\rangle$, with $\vec{y}$ integers, such that $B(\kappa, \vec{y})$ holds."

Also, if $\kappa \prec \omega_m$, then $\omega \cdot \kappa + \omega \prec \omega_m$; so (c) is proved. Finally, (d) follows immediately from (a), (b) and (c). □

It is important to note that Proposition 1 holds for $n = 0$; it is easy to see that the proof of (c) is valid for $n = 0$ since C is a Δ_0-formula if B is. This has as consequence that $I\Delta_0 + TI(\prec \omega_m, \Sigma_0)$ is equivalent to $I\Delta_0 + TI(\prec \omega_m, \Pi_1)$ and since $I\Delta_0$ can express every primitive recursive predicate as a Π_1 formula, it follows that transfinite ($\prec \omega_m$) induction on Δ_0-formulas implies the same amount of transfinite induction on primitive recursive predicates. In addition, relative to $I\Delta_0$, $TI(\prec \omega_m, \Sigma_0)$ is equivalent to $LOP(\prec \omega_m, \Sigma_0)$, which in turn is equivalent to $LOP(\prec \omega_m, \Sigma_1)$. Since every primitive recursive predicate can be expressed as a Σ_1-formula, it follows that transfinite ($\prec \omega_m$) induction on Δ_0-formulas implies the $\prec \omega_m$ least ordinal principle for primitive recursive predicates. We shall, in section 3, frequently informally argue that various complicated metamathematical constructions can be formalized in theories $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$; since $m \geq 2$ always holds, these theories can prove the usual induction and least number principles for primitive recursive predicates, which is sufficient for formalizing all the metamathematical constructions in section 3.

PROPOSITION 2 *Let* $n \geq 1$.

$$\begin{aligned} I\Sigma_n \equiv I\Pi_n &\equiv I\Delta_0 + TI(\omega, \Sigma_n) \equiv I\Delta_0 + TI(\omega, \Pi_n) \\ &\equiv I\Delta_0 + LOP(\prec \omega_2, \Sigma_n) \\ &\equiv I\Delta_0 + TI(\prec \omega_2, \Sigma_{n-1}) \end{aligned}$$

Proof It is clear that $I\Sigma_n \equiv I\Delta_0 + TI(\omega, \Sigma_n)$ and by standard techniques these are equivalent to $I\Pi_n$ and $I\Delta_0 + TI(\omega, \Pi_n)$. In light of Proposition 1, it suffices to show that $LOP(\prec \omega_2, \Sigma_n)$ follows from $I\Delta_0 + TI(\omega, \Pi_n)$. To accomplish this, we show, by induction on k, that $LOP(\prec \omega^k, \Sigma_n)$ follows from the latter theory. For $k = 1$ this is proved by the kind of reasoning used to prove Proposition 1(a),(b). To show $LOP(\prec \omega^{k+1}, \Sigma_n)$; let $A(\alpha) \in \Sigma_n$, let $\alpha_0 \prec \omega^{k+1}$ and reason informally with the assumptions $TI(\omega, \Pi_n)$ and $LOP(\prec \omega^k, \Sigma_n)$: further set $C(\alpha)$ to be the formula $(\exists i)A(\omega \cdot \alpha + i)$, so $C(\alpha) \in \Sigma_n$. Now assume $A(\alpha_0)$ holds; since $\alpha_0 = \omega \cdot \alpha_1 + i_1$ for some $\alpha_1 \prec \omega^k$ and some finite i_1, $C(\alpha_1)$ holds also. By $LOP(\prec \omega^k, \Sigma_n)$, there is a least α_2 such that $C(\alpha_2)$ holds and now by $TI(\omega, \Pi_n)$, there is a least i_2 such that $A(\omega \cdot \alpha_2 + i_2)$. Clearly $\alpha = \omega \cdot \alpha_2 + i_2$ is the least ordinal such that $A(\alpha)$ holds. □

2.2. Arithmetic and the sequent calculus

This section describes how the sequent calculus and free cut elimination are applied to the fragments of arithmetic defined above. The reader is presumed to be familiar with the sequent calculus (refer to [27] or Chapter 4 of [2] for the necessary background material). We shall assume the language of first-order logic contains symbols $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\exists$ and $\forall$; this leads to a large number of rules of inference but we shall omit most cases from our proofs in any event. It will be assumed that bounded quantifiers are part of the syntax of first-order logic with the sequent calculus containing the four appropriate rules of inference for bounded quantifiers.[4] See [2] for the full definition of the sequent calculus LKB with bounded quantifier rules of inference.

To formalize the proof theory of arithmetic with the sequent calculus, it is customary to use special induction inferences in place of induction axioms. An *induction inference* is of the form

$$\frac{\Gamma, A(a) \longrightarrow A(Sa), \Delta}{\Gamma, A(0) \longrightarrow A(t), \Delta}$$

where t may be any term, a is a free variable called the *eigenvariable* and a must not appear in the lower sequent. The induction inference for A is equivalent to the induction axiom for A, because the side formulas Γ and Δ are allowed. Thus $I\Sigma_k$ is formalized in the sequent calculus with a finite set of axiom schemes plus the induction inferences for Σ_k formulas. The finite set of axiom schemes for $I\Sigma_k$ consists of the following initial sequents:

$$\begin{array}{ll}
Sr = St \longrightarrow r = t & \longrightarrow r \cdot 0 = 0 \\
St = 0 \longrightarrow & \longrightarrow r \cdot (St) = r \cdot t + r \\
\longrightarrow r + 0 = r & \longrightarrow r = 0, (\exists x \leq r)(Sx = r) \\
\longrightarrow r + St = S(r + t) & r \leq t \longrightarrow (\exists x \leq t)(r + x = t) \\
 & r + s = t \longrightarrow r \leq t
\end{array}$$

where r, s and t are allowed to be any terms. Of course the usual logical initial sequents $A \longrightarrow A$ with A atomic and the initial sequents for equality are also allowed. It is important for us that every initial sequent consists of only Δ_0 formulas.

The theory $I\Delta_0 + TI(\prec \omega_m, \Sigma_n)$ is formalized in the sequent calculus with the same initial sequents, with induction inferences for Δ_0-formulas and for transfinite induction, with the $LOP(\prec \omega_m, \Pi_n)$ inferences defined below.

Let τ be a **closed** term with value the Gödel number of an ordinal and let $B(\alpha)$ be a formula; the $LOP(\tau, B)$ inference is

$$LOP(\tau, B): \qquad \frac{\alpha \preccurlyeq \tau, B(\alpha), \Gamma \longrightarrow \Delta, (\exists \beta \prec \alpha) B(\beta)}{B(\tau), \Gamma \longrightarrow \Delta}$$

[4] This assumption is not absolutely necessary and the reader may prefer to think of the bounded quantifiers as abbreviations — in this case the proofs by induction on the number of inferences in a free-cut free proof must be slightly modified.

where α is an eigenvariable and may occur only as indicated. It is not hard to see that the inference rule $LOP(\tau, B)$ is equivalent to the axiom form of $LOP(\tau, B)$: to derive the inference rule from the axiom, recall that the axiom $LOP(\tau, B)$ is

$$B(\tau) \longrightarrow (\exists\alpha \preccurlyeq \tau)[B(\alpha) \wedge (\forall\beta \prec \alpha)(\neg B(\beta))], \tag{3}$$

and use the derivation

$$\dfrac{(3) \qquad \dfrac{\alpha \preccurlyeq \tau, B(\alpha), \Gamma \longrightarrow \Delta, (\exists\beta \prec \alpha)B(\beta)}{(\exists\alpha \preccurlyeq \tau)(B(\alpha) \wedge (\forall\beta \prec \alpha)(\neg B(\beta))), \Gamma \longrightarrow \Delta}}{B(\tau), \Gamma \longrightarrow \Delta}$$

where the double horizontal line indicates omitted inferences. Conversely, to see that the $LOP(\tau, B)$ follows from the inference rule, use

$$\dfrac{\alpha \preccurlyeq \tau, B(\alpha) \longrightarrow (\exists\gamma \preccurlyeq \tau)[B(\gamma) \wedge (\forall\beta \prec \gamma)(\neg B(\beta))], (\exists\beta \prec \alpha)B(\beta)}{B(\tau) \longrightarrow (\exists\gamma \preccurlyeq \tau)[B(\gamma) \wedge (\forall\beta \prec \gamma)(\neg B(\beta))]}$$

where the upper sequent is, of course, provable in $I\Delta_0$.

The $LOP(\prec \omega_m, \Psi)$ inferences are the set of inferences $LOP(\tau, B)$ for $\tau \prec \omega_m$ and $B \in \Psi$. The *principal* formula of an LOP inference is the formula $B(\tau)$ in the lower sequent; the *auxiliary* formulas are the three formulas in the upper sequent other than Γ and Δ. An important property of the $LOP(\prec \omega_m, \Pi_{n-1})$ inferences is that the principal formula and the auxiliary formulas are all in Σ_n.[5]

Below we shall extensively study the theory $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$, which is equivalent to $I\Delta_0 + LOP(\prec \omega_m, \Pi_{n-1})$ and henceforth is to be formalized in the sequent calculus with initial sequents given above, the $I\Delta_0$-induction rule and the $LOP(\prec \omega_m, \Pi_{n-1})$ inference rule. This theory enjoys the important property of *free-cut elimination.* We say that a cut in a sequent calculus proof is *free* unless one of its cut formulas is a direct descendent of a formula in an axiom (initial sequent) or of a principal formula of an $I\Delta_0$ inference or of a principal formula of an $LOP(\prec \omega_m, \Pi_{n-1})$ inference. The free-cut elimination theorem implies that if $I\Delta_0 + LOP(\prec \omega_m, \Pi_{n-1})$ proves a sequent then there is a proof (in the same theory and of the same sequent) which contains no free cuts. Such a proof is called *free-cut free.*

[5] This is the reason we use LOP inferences instead of TI inferences. The $TI(\tau, \Sigma_{n-1})$ inferences would be

$$\dfrac{\alpha \preccurlyeq \tau, (\forall\beta \prec \alpha)B(\beta), \Gamma \longrightarrow \Delta, B(\alpha)}{\Gamma \longrightarrow \Delta, B(\tau)}$$

where $B \in \Sigma_{n-1}$ and α is an eigenvariable. These inferences contain a Π_n auxiliary formula.

This free-cut elimination theorem is proved by a elementary triple induction argument (equivalently, induction to ω^3) by the same argument used for the cut elimination theorem for first-order logic. In particular, the free-cut elimination theorem can be proved in $I\Sigma_1$.

A formula A is a *subformula of* B *in the wide sense* if A can be obtained from some subformula C of B by substituting freely terms for variables in C. In a free-cut free proof, each formula A is either (1) a direct descendent of a formula in an axiom or of a principal formula of an $I\Delta_0$ or LOP inference, or (2) a subformula in the wide sense of such a formula, or (3) a subformula in the wide sense of an auxiliary formula of an $I\Delta_0$ inference or an LOP inference, or (4) a subformula in the wide sense of a formula in the endsequent of the proof. This is because each formula in the proof has a (not necessarily direct) descendent which is a cut formula (so (1) or (2) applies), or which is an auxiliary formula of an induction or LOP inference (so (3) applies), or which is in the endsequent (so (4) applies).

The above gives the following important proposition:

PROPOSITION 3 *($n \geq 1$) Let T be a theory $I\Sigma_n$ or $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$. Suppose $\Gamma \longrightarrow \Delta$ is a consequence of T and every formula in Γ and Δ is in Σ_n. Then there is a T-proof of $\Gamma \longrightarrow \Delta$ in which every formula is in Σ_n.*

3. Definable functions of $I\Sigma_n$

3.1. Witness functions and ordinal primitive recursion

A witness oracle for an existential property $(\exists x)A(x, \vec{z})$ is an oracle which when queried with values for $\vec{z}$ responds either with a value for x such that $A(x, \vec{z})$ or with the statement that there is no such value for x. If A is a decidable predicate then a witness oracle for A is clearly equivalent to an oracle for the function

$$U_{\exists x A}(\vec{z}) \quad = \quad \begin{cases} 1 + (\mu x)A(x, \vec{z}) & \text{if } (\exists x)A(x, \vec{z}) \\ 0 & \text{otherwise} \end{cases}$$

where $(\mu x)A(x, \vec{z})$ is the least value for x such that $A(x, \vec{z})$ holds. The advantage of viewing a witness oracle as a function is that it allows the definition of being primitive recursive relative to a witness oracle:

Definition Let $n \geq 1$. The set of functions which are *primitive recursive in* Σ_n is defined inductively by:

(1) The constant function 0, the successor function $S(x) = x + 1$, and the projection functions $\pi_i^n(x_1, \ldots, x_n) = x_i$ are primitive recursive in Σ_n.

(2) The set of functions primitive recursive in Σ_n is closed under composition.

(3) If $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^{k+2} \to \mathbb{N}$ are primitive recursive in Σ_n then so is the function f defined by

$$\begin{aligned} f(0, \vec{z}) &= g(\vec{z}) \\ f(m+1, \vec{z}) &= h(m, \vec{z}, f(m, \vec{z})). \end{aligned}$$

(4) If $A(\vec{z})$ is a formula $(\exists x)B(x, \vec{z})$ where $B \in \Pi_{n-1}$ then U_A is primitive recursive in Σ_n.

The set of functions primitive recursive in Σ_0 is just the set of primitive recursive functions, and is defined, as usual, by (1), (2) and (3).

It is important for the definition of primitive recursive in Σ_n that the functions U_A are included instead of just the characteristic functions of A. For example, if $n = 1$, these two functions are Turing equivalent; however, for primitive recursive processes these are not equivalent since even if $(\exists x)B$ is guaranteed to be true and if B is primitive recursive, a primitive recursive process can not find a value for x making B true without knowing (at least implicitly) an upper bound on the least value for x.

A primitive recursive in Σ_n function may ask any (usual) query to a Π_n or a Σ_n oracle. This is because, for example, if $A(\vec{z}) \in \Sigma_n$, then A is equivalent to a formula $(\exists x)B$ where $B \in \Pi_{n-1}$ and a witness oracle $U_{(\exists x)B}$ can be used to determine if $A(\vec{z})$ is true.

Definition Let α be (the Gödel number of) an ordinal. The set of α-*primitive recursive functions* is defined inductively by the closure properties of (1), (2) and (3) above and by

(5) If $g : \mathbb{N}^k \to \mathbb{N}$, $h : \mathbb{N}^{k+1} \to \mathbb{N}$ and $\kappa : \mathbb{N}^k \to \mathbb{N}$ are α-primitive recursive then so is the function f defined by

$$f(\beta, \vec{z}) = \begin{cases} h(\beta, \vec{z}, f(\kappa(\beta, \vec{z}), \vec{z})) & \text{if } \kappa(\beta, \vec{z}) \prec \beta \preccurlyeq \alpha \\ g(\beta, \vec{z}) & \text{otherwise} \end{cases}$$

where $\kappa(\beta, \vec{z}) \prec \beta \preccurlyeq \alpha$ means that β and $\kappa(\beta, \vec{z})$ are the Gödel numbers of ordinals obeying the inequalities.

A function is said to be $\prec \alpha$-*primitive recursive* iff it is γ-primitive recursive for some $\gamma \prec \alpha$.

Combining the notions of witness oracles and ordinal primitive recursion gives:

Definition Let $n \geq 0$ and α be (the Gödel number of) an ordinal. The set of functions which are *α-primitive recursive in Σ_n* is defined inductively by the closure properties of (1)-(5) above (omitting (4) if $n = 0$).

A function is said to be *$\prec \alpha$-primitive recursive in Σ_n* iff it is γ-primitive recursive in Σ_n for some $\gamma \prec \alpha$.

It is well-known, and not too hard to show, that a function is primitive recursive in Σ_n iff it is ω-primitive recursive and iff it is $\prec \omega^\omega$-primitive recursive in Σ_n.

3.2. Normal forms for ordinal primitive recursive functions

This section presents three normal forms for the definitions of $\prec \omega_m$-primitive recursive functions. These are called the zeroth, first and second normal forms and will be helpful for the proofs of the characterization of provably total functions of various fragments of Peano arithmetic.

Recall that that the set of functions $\prec \omega_m$-primitive recursive in Σ_n is, by definition, the smallest set of functions satisfying the closure properties (1)-(5): the Zeroth Normal Form Theorem states that the closure (3) under primitive recursion may be dropped at the expense of adding more base functions.

THEOREM 4 (ZEROTH NORMAL FORM) *Let $m \geq 2$ and $n \geq 0$. The functions $\prec \omega_m$-primitive recursive in Σ_n can be inductively defined by*

(0.1) *Every primitive recursive function is $\prec \omega_m$-primitive recursive in Σ_n.*

(0.2) *The set of functions $\prec \omega_m$-primitive recursive in Σ_n is closed under composition.*

(0.3) *If $n \geq 1$ and $A(\vec{z})$ is $(\exists x)B(x, \vec{z})$ where $B \in \Pi_{n-1}$, then U_A is $\prec \omega_m$-primitive recursive in Σ_n.*

(0.4) *If $\kappa_0 \prec \omega_m$ and if $g : \mathbb{N}^k \to \mathbb{N}$, $h : \mathbb{N}^{k+1} \to \mathbb{N}$ and $\kappa : \mathbb{N}^k \to \mathbb{N}$ are $\prec \omega_m$-primitive recursive in Σ_n then so is the function f defined by*

$$f(\beta, \vec{z}) = \begin{cases} h(\beta, \vec{z}, f(\kappa(\beta, \vec{z}), \vec{z})) & \text{if } \kappa(\beta, \vec{z}) \prec \beta \preccurlyeq \kappa_0 \\ g(\beta, \vec{z}) & \text{otherwise.} \end{cases}$$

Proof The fact that $\prec \omega_m$-primitive recursive in Σ_n functions satisfy conditions (0,1)-(0.4) is obvious. The idea for the other direction is quite simple; namely, that ω-primitive recursion may be used to simulate ordinary primitive recursion. For example, if f is defined by primitive recursion from g and h by

$$\begin{aligned} f(0,\vec{z}) &= g(\vec{z}) \\ f(m+1,\vec{z}) &= h(m,\vec{z},f(m,\vec{z})) \end{aligned}$$

then f can also be defined via ω-primitive recursion as follows. For $n \in \mathbb{N}$, let $\ulcorner n \urcorner$ denote the Gödel number of the finite ordinal n. Define

$$F(\alpha,\vec{z}) = \begin{cases} g(\vec{z}) & \text{if } \alpha = \ulcorner 0 \urcorner \\ H(\alpha,\vec{z},F(Pred(\alpha),\vec{z})) & \text{otherwise} \end{cases}$$

where

$$Pred(\alpha) = \begin{cases} \alpha - 1 & \text{if } \alpha \text{ is (the Gödel number of)} \\ & \quad \text{a successor ordinal} \\ \alpha & \text{otherwise} \end{cases}$$

and

$$H(\alpha,\vec{z},w) = \begin{cases} h(m,\vec{z},w) & \text{if } \alpha = \ulcorner m+1 \urcorner \text{ with } m \in \mathbb{N} \\ \text{arbitrary} & \text{otherwise.} \end{cases}$$

Now $Pred$ is primitive recursive and H is definable by composition from h and primitive recursive functions; furthermore, $f(m,\vec{z}) = F(\ulcorner m \urcorner,\vec{z})$. Thus f is defined from g and h and some primitive recursive functions using composition and ω-primitive recursion. □

Note that the proof of Theorem 4 shows that (0.1) could be weakened to include only the usual base functions (1) and a few specific primitive recursive functions for manipulating Gödel numbers of finite ordinals.

THEOREM 5 (FIRST NORMAL FORM) *Let $m \geq 2$ and $n \geq 0$. The set of functions $\prec \omega_m$-primitive recursive in Σ_n is the smallest set of functions satisfying the four conditions (1.1)-(1.4):*

(1.1)-(1.3): *same as (0.1)-(0.3).*

(1.4) *If $\kappa_0 \prec \omega_m$ and if g and κ are unary functions which are $\prec \omega_m$-primitive recursive in Σ_n then so is the function f defined by*

$$f(\alpha) = \begin{cases} f(\kappa(\alpha)) & \text{if } \kappa(\alpha) \prec \alpha \preccurlyeq \kappa_0 \\ g(\alpha) & \text{otherwise.} \end{cases}$$

In (1.4), we say that f *is defined by parameter-free* κ_0*-primitive recursion from* g *and* κ.

Proof For this proof only, let $\mathcal{F}$ denote the smallest set of functions which satisfies the closure conditions of (1.1)-(1.4). Obviously, the Zeroth Normal Form implies that every function in $\mathcal{F}$ is $\prec \omega_m$-primitive recursive in Σ_n. To show that $\mathcal{F}$ contains every function $\prec \omega_m$-primitive recursive in Σ_n, it will suffice to show that $\mathcal{F}$ is closed under the $\prec \omega_m$-primitive recursion of (0.4). For this, suppose f is defined by

$$f(\beta, \vec{z}) = \begin{cases} h(\beta, \vec{z}, f(\kappa(\beta, \vec{z}), \vec{z})) & \text{if } \kappa(\beta, \vec{z}) \prec \beta \preccurlyeq \kappa_0 \\ g(\beta, \vec{z}) & \text{otherwise.} \end{cases}$$

To give a definition of f using parameter-free $\prec \omega_m$-primitive recursion, we shall use ordinals that code the parameters $\vec{z}$ and which code a history of the computation of $f(\beta)$ with $\beta \preccurlyeq \kappa_0$. In order to code the history of the computation of f, we need ordinals $\beta_0, \beta_1, \ldots, \beta_s$ so that $\beta_0 = \beta$ and $\beta_{i+1} = \kappa(\beta_i, \vec{z}) \prec \beta_i$ and so that $\kappa(\beta_s, \vec{z}) \not\prec \beta_s$; also we need values $a_s, \ldots, a_0$ so that $a_s = g(\beta_s, \vec{z})$ and $a_i = h(\beta_i, \vec{z}, a_{i+1})$ for all $i < s$; it will follow that $f(\beta, \vec{z})$ is equal to a_0. We shall code and index this computation by the following scheme. We use ordinals of the form $\omega^2 \cdot \beta_i + \langle \vec{z}, \beta_0, \ldots, \beta_{i-1} \rangle$ to code the first phase of the computation of f, where $\langle \vec{z}, \beta_0, \ldots, \beta_{i-1} \rangle$ denotes the finite ordinal equal to the Gödel number of the sequence containing the entries $\vec{z}$ and the Gödel numbers $\beta_0, \ldots, \beta_{i-1}$. To code the second phase of the computation we use ordinals of the form $\omega \cdot i + \langle \vec{z}, \beta_0, \ldots, \beta_{i-1}, a_i \rangle$. Since $\kappa_0 \prec \omega_m$ there is an ordinal $\sigma_0 \prec \omega_{m-1}$ such that $\kappa_0 \prec \omega^{\sigma_0}$. Define

$$F(\alpha) = \begin{cases} F(K(\alpha)) & \text{if } K(\alpha) \prec \alpha \preccurlyeq \omega^{2+\sigma_0} \\ G(\alpha) & \text{otherwise} \end{cases}$$

where K and G are defined so that

$$K(\omega^2 \cdot \beta_i + \langle \vec{z}, \beta_0, \ldots, \beta_{i-1} \rangle) = \omega^2 \cdot \kappa(\beta_i, \vec{z}) + \langle \vec{z}, \beta_0, \ldots, \beta_i \rangle$$
$$\text{if } i \geq 0 \text{ and } \kappa(\beta_i, \vec{z}) \prec \beta_i$$

$$K(\omega^2 \cdot \beta_i + \langle \vec{z}, \beta_0, \ldots, \beta_{i-1} \rangle) = \omega \cdot i + \langle \vec{z}, \beta_0, \ldots, \beta_{i-1}, g(\beta_i, \vec{z}) \rangle$$
$$\text{where } 0 \leq i \in \mathbb{N} \text{ and } \kappa(\beta_i, \langle \vec{z} \rangle) \not\prec \beta_i$$

$$K(\omega \cdot (i+1) + \langle \vec{z}, \beta_0, \ldots, \beta_i, a \rangle) = \omega \cdot i + \langle \vec{z}, \beta_0, \ldots, \beta_{i-1}, h(\beta_i, \vec{z}, a) \rangle$$
$$\text{for } i \in \mathbb{N}$$

$$K(\ulcorner \langle \vec{z}, a \rangle \urcorner) = \ulcorner \langle \vec{z}, a \rangle \urcorner$$

$$G(\ulcorner \langle \vec{z}, a \rangle \urcorner) = a$$

where, in the last two equations, $\ulcorner\langle\vec{z},a\rangle\urcorner$ denotes the Gödel number of the finite ordinal $\langle\vec{z},a\rangle$. K and G may be arbitrarily defined for other inputs. Clearly F is defined by $\omega^{2+\sigma_0}$-primitive recursion from G and K. And f is definable in terms of F and g using composition:

$$f(\beta,\vec{z}) \quad = \quad \begin{cases} F(\omega^2\cdot\beta+\langle\vec{z}\rangle) & \text{if } \beta \preccurlyeq \kappa_0 \\ g(\beta,\vec{z}) & \text{otherwise} \end{cases}$$

We have used only $\prec \omega_m$-primitive recursion (since $\omega^{2+\sigma_0} \prec \omega_m$) and composition to define f from g, h, κ and primitive recursive functions. Hence $f \in \mathcal{F}$.
Q.E.D. Theorem 5

The final and best normal form for $\prec \omega_m$-primitive recursive in Σ_n functions is not an inductive definition, but is a true normal form.

THEOREM 6 (SECOND NORMAL FORM)

(a) *Let $m \geq 2$ and $n \geq 1$. A function $F(\vec{z})$ is $\prec \omega_m$-primitive recursive in Σ_n iff there are a $\kappa_0 \prec \omega_m$, a $A(\vec{y})$ of the form $(\exists x)B(x,y)$ with $B \in \Pi_{n-1}$, and primitive recursive functions τ, g and κ so that $F(\vec{z}) = f(\tau(\vec{z}))$ where $f(\beta)$ is defined by*

$$f(\beta) \quad = \quad \begin{cases} f(\kappa(\beta,U_A(\beta))) & \text{if } \kappa(\beta,U_A(\beta)) \prec \beta \preccurlyeq \kappa_0 \\ g(\beta) & \text{otherwise} \end{cases}$$

(b) *Let $m \geq 2$. A function $F(\vec{z})$ is $\prec \omega_m$-primitive recursive iff there are a $\kappa_0 \prec \omega_m$ and primitive recursive functions τ, g and κ so that $F(\vec{z}) = f(\tau(\vec{z}))$ where*

$$f(\beta) \quad = \quad \begin{cases} f(\kappa(\beta)) & \text{if } \kappa(\beta) \prec \beta \preccurlyeq \kappa_0 \\ g(\beta) & \text{otherwise} \end{cases}$$

An important feature of the second normal form theorem is that κ is now required to be primitive recursive, instead of merely $\prec \omega_m$-primitive recursive in Σ_n.

Proof We shall prove (a); the proof of (b) is essentially identical. First, every primitive recursive function can be expressed in the form (a): to prove this, if F is primitive recursive, let $\kappa_0 = 0$, let $\tau(\vec{z}) = \ulcorner\langle\vec{z}\rangle\urcorner$, let $\kappa(\beta,a) = 0$ and $g(\ulcorner\langle\vec{z}\rangle\urcorner) = F(\vec{z})$. The functions τ and κ are clearly primitive recursive and g is primitive recursive since F is. Second, if $A(y)$ is $(\exists x)B(x,y)$ where $B \in \Pi_{n-1}$, then the function U_A can be expressed in the form (a) by letting

$\kappa_0 = \omega \cdot 2$, letting $\tau(y) = \omega + y$, letting $\kappa(\omega + y, i) = \ulcorner i \urcorner$ and $\kappa(\ulcorner i \urcorner, a) = \ulcorner i \urcorner$ and letting $g(\ulcorner i \urcorner) = i$.

Next we show that the set of functions definable in the form (a) is closed under composition. Suppose F_1 and F_2 are defined by $F_1(v, \vec{z}) = f_1(\tau_1(v, \vec{z}))$ and $F_2(\vec{z}) = f_2(\tau_2(\vec{z}))$ where

$$f_i(\beta) \quad = \quad \begin{cases} f_i(\kappa_i(\beta, U_{A_i}(\beta))) & \text{if } \kappa_i(\beta, U_{A_i}(\beta)) \prec \beta \preccurlyeq \kappa_{0,i} \\ g_i(\beta) & \text{otherwise} \end{cases}$$

for $i = 1, 2$. By assumption, τ_i, κ_i and g_i are primitive recursive functions. We must show $F(\vec{z}) = F_1(F_2(\vec{z}), \vec{z})$ is also definable in this way. Pick $\sigma \prec \omega_{m-1}$ to be an ordinal such that $\kappa_{0,1}, \kappa_{0,2} \prec \omega^\sigma$. We set $F(\vec{z}) = f(\omega^{1+\sigma} \cdot 2 + \langle \vec{z} \rangle)$ and define $f(\beta)$ as in (a) with $\kappa_0 = \omega^{1+\sigma} \cdot 3$ and with κ defined so that, if $\beta \prec \omega^\sigma$,

$$\kappa(\omega^{1+\sigma} \cdot 2 + \langle \vec{z} \rangle) \;=\; \begin{cases} \omega^{1+\sigma} + \omega \cdot \tau_2(\vec{z}) + \langle \vec{z} \rangle & \text{if } \tau_2(\vec{z}) \preccurlyeq \kappa_{0,2} \\ \tau_1(g_2(\tau_2(\vec{z}))) & \text{if } \tau_2(\vec{z}) \not\preccurlyeq \kappa_{0,2} \text{ and} \\ & \quad \tau_1(g_2(\tau_2(\vec{z}))) \preccurlyeq \kappa_{0,1} \\ \omega^{1+\sigma} \cdot 3 & \text{otherwise} \end{cases}$$

$$\kappa(\omega^{1+\sigma} + \omega \cdot \beta + \langle \vec{z} \rangle) \;=\; \begin{cases} \omega^{1+\sigma} + \omega \cdot \kappa_2(\beta, U_{A_2}(\beta)) + \langle \vec{z} \rangle & \\ & \text{if } \kappa_2(\beta, U_{A_2}(\beta)) \prec \beta \preccurlyeq \kappa_{0,2} \\ \tau_1(g_2(\beta), \vec{z}) & \text{if not } \kappa_2(\beta, U_{A_2}(\beta)) \prec \beta \preccurlyeq \kappa_{0,2} \\ & \quad \text{and } \tau_1(g_2(\beta), \vec{z}) \preccurlyeq \kappa_{0,1} \\ \omega^{1+\sigma} \cdot 3 & \text{otherwise} \end{cases}$$

and, if $\beta \prec \kappa_{0,1}$, $\kappa(\beta) = \kappa_1(\beta, U_{A_1}(\beta))$. Also define g so that, for all $\beta \prec \omega^\sigma$,

$$\begin{aligned} g(\omega^{1+\sigma} \cdot 2 + \langle \vec{z} \rangle) &= g_1(\tau_1(g_2(\tau_2(\vec{z})))) \\ g(\omega^{1+\sigma} + \omega \cdot \beta + \langle \vec{z} \rangle) &= g_1(\tau_1(g_2(\beta))) \\ g(\beta) &= g_1(\beta) \end{aligned}$$

This almost defines $f(\vec{z})$ in the desired form (a); however, there is a problem since $\kappa(\alpha)$ is defined using both U_{A_1} and U_{A_2} (and not using them in correct manner either). To fix this, we define a new $A(y) = (\exists x)B(x, y)$ so that $\kappa(\alpha)$ is a primitive recursive function of only α and $U_A(\alpha)$. For this, suppose $A_i = (\exists x)B_i(x, y)$ where $B_i \in \Pi_{n-1}$. Define B by

$$B(x, \alpha) \quad \Leftrightarrow \quad \begin{cases} B_2(x, \beta) & \text{if } \alpha = \omega^{1+\sigma} + \omega \cdot \beta + m \\ B_1(x, \alpha) & \text{if } \alpha \prec \omega^{1+\sigma} \\ \text{arbitrary} & \text{otherwise.} \end{cases}$$

Since $B_1, B_2 \in \Pi_{n-1}$, so is B. That completes the proof that the set of functions definable in the form (a) are closed under composition.

Finally, we must show that the functions definable in the form (a) are closed under parameter-free $\prec \omega_m$-primitive recursion. For this, suppose f is defined from functions g and κ, which are defined in form (a), and from an ordinal $\kappa_0 \prec \omega_m$ as in (1.4) and further suppose that κ is defined in the normal form (a) by

$$\begin{aligned} \kappa(\alpha) &= f_1(\tau_1(\alpha)) \\ f_1(\beta) &= \begin{cases} f_1(\kappa_1(\beta, U_{A_1}(\beta))) & \text{if } \kappa_1(\beta, U_{A_1}(\beta)) \prec \beta \preccurlyeq \kappa_{0,1} \\ g_1(\beta) & \text{otherwise} \end{cases} \end{aligned}$$

where $\kappa_{0,1} \prec \omega_m$ and τ_1, κ_1 and g_1 are primitive recursive functions. Pick σ_0, σ_1 to be the least ordinals such that $\kappa_0 \prec \omega^{\sigma_0}$ and $\kappa_{0,1} \prec \omega^{\sigma_1}$; hence $\sigma_0, \sigma_1 \prec \omega_{m-1}$. We now define $F(\alpha) = f'(\omega^{1+\sigma_1+\sigma_0} + \ulcorner\alpha\urcorner)$ where f' will be defined in the second normal form (a) with primitive recursive functions κ', g' and ordinal κ_0' where κ' is defined by

$$\kappa'(\omega^{1+\sigma_1+\sigma_0} + \ulcorner\alpha\urcorner) = \begin{cases} \omega^{1+\sigma_1} \cdot \alpha + \omega^{\sigma_1} & \text{if } \alpha \preccurlyeq \kappa_0 \\ \omega^{1+\sigma_1+\sigma_0} + \omega & \text{otherwise} \end{cases}$$

$$\kappa'(\omega^{1+\sigma_1} \cdot \beta + \omega^{\sigma_1}) = \begin{cases} \omega^{1+\sigma_1} \cdot \beta + \tau_1(\beta) & \text{if } \tau_1(\beta) \preccurlyeq \kappa_{0,1} \\ \omega^{1+\sigma_1} \cdot g_1(\tau_1(\beta)) & \text{if } \tau_1(\beta) \not\preccurlyeq \kappa_{0,1} \\ & \text{and } g_1(\tau_1(\beta)) \prec \beta \\ \omega^{1+\sigma_1+\sigma_0} & \text{otherwise} \end{cases}$$

$$\kappa'(\omega^{1+\sigma_1} \cdot \beta + \gamma) = \begin{cases} \omega^{1+\sigma_1} \cdot \beta + \kappa_1(\gamma, U_{A_1}(\gamma)) \\ \qquad \text{if } \kappa_1(\gamma, U_{A_1}(\gamma)) \prec \gamma \preccurlyeq \kappa_{0,1} \\ \omega^{1+\sigma_1} \cdot g_1(\gamma) + \omega^{\sigma_1} \\ \qquad \text{if } \kappa_1(\gamma, U_{A_1}(\gamma)) \not\prec \gamma \text{ and } g_1(\gamma) \prec \beta \\ \omega^{1+\sigma_1+\sigma_0} \quad \text{if } \kappa_1(\gamma, U_{A_1}(\gamma)) \not\prec \gamma \text{ and } g_1(\gamma) \not\prec \beta \end{cases}$$

(provided $\gamma \preccurlyeq \kappa_{0,1}$), and g' is defined by

$$\begin{aligned} g'(\omega^{1+\sigma_1+\sigma_0} + \ulcorner\alpha\urcorner) &= \alpha \\ g'(\omega^{1+\sigma_1} \cdot \beta + \gamma) &= \beta \qquad \text{if } \beta \preccurlyeq \kappa_0 \text{ and } \gamma \preccurlyeq \omega^{\sigma_1} \end{aligned}$$

and $\kappa_0' = \omega^{1+\sigma_1+\sigma_0} + \omega$. Any values of κ' and g' left unspecified may be arbitrary. Now, inspection shows that

$$F(\alpha) = \begin{cases} F(\kappa(\alpha)) & \text{if } \kappa(\alpha) \prec \alpha \preccurlyeq \kappa_0 \\ \alpha & \text{otherwise} \end{cases}$$

and, by construction, F is definable in form (a). Now the function f is definable by $f(\alpha) = g(F(\alpha))$ and since g and F are expressible in form (a) it follows by the earlier part of this proof that their composition f is too.
Q.E.D. Theorem 6

One further refinement can be made to the second normal form theorem: instead of allowing arbitrary U_A's with $A \in \Sigma_n$, it is possible to allow only a single, fixed, suitably chosen U_A. Of course, such an A is many-one complete for Σ_n. It is necessary to modify the ordinal coding methods in the above proof to establish this refinement — the details are left to the reader.

3.3. Some definability theorems

The next theorems characterize the Σ_n definable functions of $I\Sigma_n$; their proof will be a straightforward use of the witness function method.

THEOREM 7 *Let $m \geq 2$ and $n \geq 1$. The Σ_n-definable functions of the theory $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ are precisely the functions which are $\prec \omega_m$-primitive recursive in Σ_{n-1}.*

THEOREM 8 *Let $n \geq 1$. The Σ_n-definable functions of the theory $I\Sigma_n$ are precisely the functions which are primitive recursive in Σ_{n-1}.*

THEOREM 9 *The Σ_1-definable (provably recursive) functions of $I\Sigma_1$ are precisely the primitive recursive functions.*

There are (at least) three prior prooftheoretic proofs of Theorem 9. Parsons [22] gave a proof based on the Gödel Dialectica interpretation, Mints [19] gave a proof which uses a method very close to the witness function method except presented with a functional language, and Takeuti [27] gives a proof based on Gentzen-style assignment of ordinals to proofs.

Proof Theorems 8 and 9 are corollaries of Theorem 7 since $I\Sigma_n$ and $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ are the same theory. Although only the proof of Theorem 7 is given below, it should be remarked that the other two theorems can be proved directly by a similar and easier argument.

The easier half of the proof is to show that every $\prec \omega_m$-primitive recursive in Σ_{n-1} function is Σ_n-definable in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$. Recall that every primitive recursive function is Σ_1-definable in $I\Sigma_1$ so this half of the $m = 2$ and $n = 1$ case of Theorem 7 follows. For other values of m and n, suppose F is $\prec \omega_m$-primitive recursive in Σ_{n-1} and that F is defined by $F(\vec{z}) = f(\tau(\vec{z}))$ where

$$f(\beta) = \begin{cases} f(\kappa(\beta, U_A(\beta))) & \text{if } \kappa(\beta, U_A(\beta)) \prec \beta \preccurlyeq \kappa_0 \\ g(\beta) & \text{otherwise} \end{cases}$$

in accordance with the Second Normal Form, so g, κ and τ are primitive recursive functions, $\kappa_0 \prec \omega_m$ and $A(y)$ is $(\exists x)B(x,y)$ where $B \in \Pi_{n-2}$ (in the simpler case where $n = 1$, $\kappa(\beta, U_A(\beta))$ is replaced by $\kappa(\beta)$ and U_A is not used at all). Obviously it will suffice to show that f is Σ_n-definable by $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$.

A sequence of ordinals $\beta_0, \ldots, \beta_k$ is an *f-computation series* if $\beta_{i+1} \prec \kappa_0$, $\beta_{i+1} = \kappa(\beta_i, U_A(\beta_i))$ and $\beta_{i+1} \prec \beta_i$, for all $0 \le i < k$. To metamathematically define an f-computation series, we use (if $n > 1$),

$$\begin{aligned}
&\text{“}w \text{ codes an } f\text{-computation series”} \;\Leftrightarrow \\
&\quad w \text{ is a sequence of Gödel numbers of ordinals of length } k+1 \\
&\quad \text{and } (\forall i < k)\Big[\Big((\exists y)[B((w)_i, y) \wedge (\forall y' < y)(\neg B((w)_i, y)) \\
&\qquad\qquad\qquad \wedge (w)_{i+1} = \kappa((w)_i, y+1)]\Big) \\
&\qquad\qquad \vee \Big((\forall y)(\neg B((w)_i, y)) \wedge (w)_{i+1} = \kappa((w)_i, 0)\Big)\Big] \\
&\quad \text{and } (\forall i < k)((w)_{i+1} \prec (w)_i \wedge (w)_{i+1} \prec \kappa_0).
\end{aligned}$$

(Recall that if $w = \langle \beta_0, \ldots, \beta_k \rangle$, then $(w)_i = \beta_i$.) Since $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ contains $I\Sigma_n$, it also contains the collection axiom $B\Sigma_n$. Thus the subformula $(\forall y' < y)(\cdots)$ above is equivalent to a Σ_{n-2} formula, and by applying prenex operations, the formula “w codes an f-computation series” is equivalent to a Π_n formula. By applying prenex operations in a different order, and using $B\Sigma_n$, this formula is also equivalent to a Σ_n-formula. If $n = 1$, then instead define

$$\begin{aligned}
&\text{“}w \text{ codes an } f\text{-computation series”} \;\Leftrightarrow \\
&\quad w \text{ is a sequence of Gödel numbers of ordinals of length } k+1 \\
&\quad \text{and } (\forall i < k)(\beta_{i+1} = \kappa(\beta_i) \prec \beta_i \wedge \beta_{i+1} \prec \kappa_0),
\end{aligned}$$

so, in this case, it is a primitive recursive property.[6]

The graph of the function $f(\beta)$ can now be defined by using the fact that $y = f(\beta)$ iff $y = g(\beta')$ where β' is the least ordinal such that there is an f-computation series $\langle \beta, \ldots, \beta' \rangle$. More formally, letting $fCS(w)$ be the formula “w is an f-computation series”,

$$\begin{aligned}
y = f(\beta) \;\Leftrightarrow\; (\exists \langle \beta, \ldots, \beta' \rangle)\big[&y = g(\beta') \wedge fCS(\langle \beta, \ldots, \beta' \rangle) \wedge \\
&\wedge \neg(\kappa(\beta', U_A(\beta')) \prec \beta' \wedge \beta' \preccurlyeq \kappa_0)\big].
\end{aligned}$$

Since $fCS(\cdots)$ is equivalent to a Σ_n-formula and since $z = U_A(\beta')$ can be expressed as a Π_{n-1}-formula, the relation $y = f(\beta)$ is a Σ_n-property,

[6] It is possible to strengthen the second normal form theorem to make this a Δ_0-formula.

provably in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$. The theory also proves

$$\forall\beta\ \exists \text{ a least } \beta' \text{ s.t. } \exists\langle\beta,\dots,\beta'\rangle(fCS(\langle\beta,\dots,\beta'\rangle))$$

since $fCS(\langle\beta\rangle)$ and by $LOP(\prec \omega_m, \Sigma_n)$ since $\kappa_0 \prec \omega_m$.[7] Thus $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ can Σ_n-define the function f as it proves $(\forall\beta)(\exists! y)(y = f(\beta))$ where $y = f(\beta)$ denotes the Σ_n-formula defining the graph of f. Likewise,

$$(\forall\vec{z})(\exists! y)(\exists\beta)(\beta = \tau(\vec{z}) \wedge y = f(\beta))$$

is also provable and Σ_n-defines the function F. That completes the first half of the proof of Theorem 7.

To prove the rest of Theorem 7, assume that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves $(\forall x)(\exists! y)A(x,y)$, with $A \in \Sigma_n$ — we must show that $x \mapsto y$ is a $\prec \omega_m$-primitive recursive in Σ_{n-1} function. Since $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves $(\forall x)(\exists y)A$, there must be a free-cut free proof in the theory $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ of the sequent

$$\longrightarrow (\exists y)A(c,y)$$

where c is a new free variable. Only Σ_n formulas can appear in this free-cut free proof. The general idea of the proof is to show that this free-cut free proof embodies an algorithm for computing y from c. Indeed, the free-cut free proof can be interpreted as explicitly containing a $\prec \omega_m$-primitive recursive in Σ_{n-1} algorithm. Since the proofs of the normal form theorems were constructive, the free-cut free proof also contains an implicit description of a $\prec \omega_m$-primitive recursive in Σ_{n-1} algorithm in the second normal form. Our proof below that an algorithm can be extracted from the free-cut free proof is quite constructive and can be formalized in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ — the upshot is that there is a $\prec \omega_m$-primitive recursive in Σ_{n-1} function f which is Σ_n-defined by $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ in the form given by the Second Normal Form Theorem such that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1}) \vdash (\forall x)A(x, f(x))$. As a corollary to the proof method, if $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves $(\forall x)(\exists y)B(x,y)$ with $B \in \Sigma_n$ then there is a $B^*(x,y) \in \Sigma_n$ such that $(\forall x)(\exists! y)B^*(x,y)$ and $B^*(x,y) \to B(x,y)$ are provable.[8]

We shall see later that the proof is formalizable, not only in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$, but also in $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$, provided $n > 1$.

[7] $LOP(\prec \omega_m, \Sigma_n)$ is a consequence of $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ by Proposition 1.

[8] This fact is readily proved directly anyway. If $B \in \Pi_{n-1}$ then let B^* be the formula $B(x,y) \wedge (\forall y' < y)(\neg B(x,y'))$, which is equivalent to a Σ_n formula by $B\Sigma_n$. For general $B \in \Sigma_n$, incorporate outermost existential quantifiers of B into the the $(\exists y)$ and proceed similarly.

Rather than just considering the free-cut free proof of $\longrightarrow(\exists y)A$, we more generally consider proofs of sequents $\Gamma\longrightarrow\Delta$ of Σ_n-formulas. Since every principal and auxiliary formula of a $LOP(\prec\omega_m, \Pi_{n-1})$ inference is in Σ_n and every formula in the endsequent is in Σ_n, it follows that every formula in the free-cut free proof is in Σ_n. For convenience, assume also that the proof is in free variable normal form (so free variables are not reused).

Definition Let $i \geq 1$ and $A(\vec{x}) \in \Sigma_i$. If $A \in \Pi_{i-1}$ then Wit^i_A is defined to be the formula A. Otherwise, A is uniquely expressible in the form $(\exists y_0)\cdots(\exists y_k)B(\vec{x},\vec{y})$ where $B \in \Pi_{i-1}$. Then $Wit^i_A(w,\vec{x})$ is the formula

$$B(\vec{x},(w)_0,\ldots,(w)_k).$$

Note that $Wit^i_A \in \Pi_{i-1}$. If $Wit^i_A(w,\vec{x})$ holds, we say w *witnesses* the truth of $A(\vec{x})$.

MAIN LEMMA 10 *($n \geq 1$, $m \geq 2$) Suppose $I\Delta_0 + TI(\prec\omega_m,\Sigma_{n-1})$ proves the sequent $A_1,\ldots,A_k\longrightarrow B_1,\ldots,B_\ell$ and that each A_i and B_j is in Σ_n and that $\vec{c}$ are all the variables free in the sequent. Then there are functions $f_1,\ldots,f_\ell$ which are $\prec\omega_m$-primitive recursive in Σ_{n-1} and are Σ_n-definable in $I\Delta_0 + TI(\prec\omega_m,\Sigma_{n-1})$ such that $I\Delta_0 + TI(\prec\omega_m,\Sigma_{n-1})$ proves*

$$Wit^n_{A_1}(w_1,\vec{c}),\ldots,Wit^n_{A_k}(w_k,\vec{c})\longrightarrow Wit^n_{B_1}(f_1(\vec{w},\vec{c}),\vec{c}),\ldots,Wit^n_{B_\ell}(f_\ell(\vec{w},\vec{c}),\vec{c}).$$

Informally, the $f_1,\ldots,f_\ell$ will, given witnesses for all of $A_1,\ldots,A_k$, produce a witness for at least one of $B_1,\ldots,B_\ell$.

The proof of the Main Lemma is by induction on the number of inferences in a free-cut free proof of the sequent. In the base case, there are zero inferences, so the sequent is an axiom and consists of Δ_0-formulas — for these axioms, the lemma is trivial. For the induction step, the proof splits into cases depending in the final inference of the proof. Most of the cases are straightforward; for example, if the last inference is an $\exists$*:left* inference then the proof ends with

$$\frac{A_1,\ldots,A_k \longrightarrow B_0(\vec{c},s),B_2,\ldots,B_\ell}{A_1,\ldots,A_k \longrightarrow (\exists z_0)B_0(\vec{c},z_0),B_2,\ldots,B_\ell}$$

where $s = s(\vec{c})$ is a term with free variables from $\vec{c}$ only and where B_1 is $(\exists z_0)B_0$ and is of the form $(\exists z_0)\cdots(\exists z_r)B'(\vec{z},\vec{c})$ with $B' \in \Pi_{n-1}$ (possibly $r = 0$). The induction hypothesis is that

$$\begin{aligned} &Wit^n_{A_1}(w_1,\vec{c}),\ldots,Wit^n_{A_k}(w_k,\vec{c}) \\ &\qquad\longrightarrow Wit^n_{B_0(\vec{c},s)}(f_0(\vec{w},\vec{c}),\vec{c}),\ldots,Wit^n_{B_\ell}(f_\ell(\vec{w},\vec{c}),\vec{c}) \end{aligned} \qquad (4)$$

is provable in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ for appropriate functions $f_0, f_2, \ldots, f_\ell$. If $B_1 \in \Sigma_{n-2}$ then $Wit^n_{B_0}$ is just B_0 and $Wit^n_{B_1}$ is just B_1; and a single $\exists$*:right* inference applied to (4) gives

$$Wit^n_{A_1}(w_1, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \longrightarrow Wit^n_{B_1}(f_1(\vec{w}, \vec{c}), \vec{c}), \ldots, Wit^n_{B_\ell}(f_\ell(\vec{w}, \vec{c}), \vec{c}) \quad (5)$$

where f_1 is arbitrary. Otherwise, let $f_1(\vec{w}, \vec{c})$ be defined so that

$$f_1(\vec{w}, \vec{c}) = \langle s(\vec{c}), a_1, \ldots, a_r \rangle \quad \text{where} \quad f_0(\vec{w}, \vec{c}) = \langle a_1, \ldots, a_r \rangle$$

if $r > 0$, and $f(\vec{w}, \vec{c}) = \langle s(\vec{c}) \rangle$ if $r = 0$. Clearly f_1 is $\prec \omega_m$-primitive recursive in Σ_{n-1} since f_0 is and, also clearly, $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves (5) for this f_1.

We leave the rest of the simpler cases to the reader and consider only the two substantial cases of $\forall$*:right* and $LOP(\prec \omega_m, \Pi_{n-1})$ as last inference. (Part of the $\exists$*:left* case is also substantial, but is very similar to $\forall$*:right.*)

($\forall$*:right*) Suppose the last inference is

$$\frac{A_1, \ldots, A_k \longrightarrow B_0(b, \vec{c}), B_2, \ldots, B_\ell}{A_1, \ldots, A_k \longrightarrow (\forall z_0) B_0(z_0, \vec{c}), B_2, \ldots, B_\ell}$$

where the free variable b does not occur except as indicated and B_1 is $(\forall z_0) B_0(\vec{z}, \vec{c})$. Since B_1 is in Σ_n and has outermost quantifier universal, it must therefore actually be in Π_{n-1} and be of the form $(\forall z_0) \cdots (\forall z_r) B'(\vec{z}, \vec{c})$ where $B' \in \Sigma_{n-2}$. Also $Wit^n_{B_0}$ and $Wit^n_{B_1}$ are just B_0 and B_1, respectively. The induction hypothesis is that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves

$$Wit^n_{A_1}(w_1, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \longrightarrow B_0(b, \vec{c}), Wit^n_{B_2}(g_2(\vec{w}, b, \vec{c}), \vec{c}), \ldots, Wit^n_{B_\ell}(g_\ell(\vec{w}, b, \vec{c}), \vec{c})$$

for functions $g_2, \ldots, g_\ell$ which are $\prec \omega_m$-primitive recursive in Σ_{n-1}. The difficulty is that these functions take b as an argument, but b is not free in the endsequent so we can not just set $f_i = g_i$. The solution to this difficulty is to let $C(v, \vec{c})$ be the Π_{n-2}-formula $\neg B'((v)_0, \ldots, (v)_r, \vec{c})$ and use the function $U_{\exists v C}$ to find a value, if any, for b such that $B_0(b, \vec{c})$ holds: define

$$f_i(\vec{w}, \vec{c}) \quad = \quad g_i(\vec{w}, (U_{\exists v C}(\vec{c}) - 1)_0, \vec{c}).$$

When $B_1(\vec{c})$ is false, $U_{\exists v C}(\vec{c}) - 1$ codes a sequence $\langle b_0, \ldots, b_r \rangle$ such that $\neg B_0(b_0, \ldots, b_r)$ and $(U_{\exists v C}(\vec{c}) - 1)_0$ equals b_0. Thus $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves

$$Wit^n_{A_1}(w_1, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \longrightarrow B_1(\vec{c}), Wit^n_{B_2}(f_2(\vec{w}, \vec{c}), \vec{c}), \ldots, Wit^n_{B_\ell}(f_\ell(\vec{w}, \vec{c}), \vec{c})$$

and $f_2, \ldots, f_k$ are $\prec \omega_m$-primitive recursive in Σ_{n-1} since $g_2, \ldots, g_k$ are and since $(\exists v)C$ is in Σ_{n-1}.

LOP$(\prec \omega_m, \Pi_{n-1})$: Suppose the last inference is

$$\frac{\alpha \preccurlyeq \kappa_0, A_1(\alpha, \vec{c}), A_2, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell, (\exists \beta \prec \alpha) A_1(\beta, \vec{c})}{A_1(\kappa_0, \vec{c}), A_2, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell}$$

where $A_1 \in \Pi_{n-1}$, where κ_0 is a closed term with value a Gödel number of an ordinal $\prec \omega_m$, where α is a free variable, which appears only as indicated, and where $(\exists \beta \prec \alpha) A_1(\beta)$ is an abbreviation for the formula $(\exists \beta)(\beta \prec \alpha \wedge A_1(\beta))$. The induction hypothesis states that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves

$$\begin{aligned} &\alpha \preccurlyeq \kappa_0, A_1(\alpha, \vec{c}), Wit^n_{A_2}(w_2, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \\ &\qquad \longrightarrow Wit^n_{B_1}(g_1(\vec{w}, \alpha, \vec{c}), \vec{c}), \ldots, Wit^n_{B_\ell}(g_\ell(\vec{w}, \alpha, \vec{c}), \vec{c}), \\ &\qquad\qquad g_{\ell+1}(\vec{w}, \alpha, \vec{c}) \prec \alpha \wedge A_1(g_{\ell+1}(\vec{w}, \alpha, \vec{c}), \vec{c}) \end{aligned}$$

for appropriate functions $g_1, \ldots, g_{\ell+1}$. Define

$$H(\beta, \vec{c}) = \begin{cases} \beta & \text{if } A_1(\beta, \vec{c}) \\ \kappa_0 & \text{otherwise} \end{cases}$$

H is $\prec \omega_m$-primitive recursive in Σ_{n-1} since $A_1 \in \Pi_{n-1}$. Now define

$$F(\vec{w}, \beta, \vec{c}) = \begin{cases} F(\vec{w}, H(g_{\ell+1}(\vec{w}, \beta, \vec{c}), \vec{c}), \vec{c}) & \text{if } H(g_{\ell+1}(\vec{w}, \beta, \vec{c}), \vec{c}) \prec \beta \preccurlyeq \kappa_0 \\ \beta & \text{otherwise.} \end{cases}$$

Clearly F is also $\prec \omega_m$-primitive recursive in Σ_{n-1}. Finally set

$$f_i(\vec{w}, \vec{c}) = g_i(\vec{w}, F(\vec{w}, \kappa_0, \vec{c}), \vec{c});$$

it is easy to check that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves

$$\begin{aligned} &A_1(\kappa_0, \vec{c}), Wit^n_{A_2}(w_2, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \\ &\qquad \longrightarrow B_1(\vec{c}), Wit^n_{B_2}(f_2(\vec{w}, \vec{c}), \vec{c}), \ldots, Wit^n_{B_\ell}(f_\ell(\vec{w}, \vec{c}), \vec{c}) \end{aligned}$$

since $F(\vec{w}, \kappa_0, \vec{c})$ gives the ordinal at which $g_{\ell+1}$ fails to give a smaller ordinal satisfying A_1 and with this ordinal, one of $g_1, \ldots, g_\ell$ must produce a witness for the corresponding $B_1, \ldots, B_\ell$.

Q.E.D. Lemma 10 and Theorems 7, 8 and 9

The above proof did not consider the case where the last inference of the proof is an induction inference: since induction is restricted to Δ_0-formulas and the witness formula for a Δ_0-formula is just the formula itself, that case is completely trivial. However, $I\Sigma_n$ is, by Proposition 2 a consequence of $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ and it must, a priori, be possible to handle $I\Sigma_n$ induction inferences by the witness function method as above. In fact, it is quite simple — an $I\Sigma_n$-induction inference is handled by primitive recursion in Σ_{n-1}. This leads to a direct proof of Theorems 8 and 9; we leave the details of this direct proof to the reader.

We have now finished the characterization of the Σ_n-definable functions of $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ and of $I\Sigma_n$. It remains to characterize the Σ_k-definable functions of these theories when $k < n$. (In section 6, we discuss the case $k > n$ too). The central result needed for this characterization is that the theory $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ is Π_{n+1}-conservative over $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$:

THEOREM 11 *Let $m \geq 2$ and $n \geq 1$.*

(a) $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1}) \vdash TI(\prec \omega_{m+1}, \Sigma_{n-2})$.

(b) *If $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1}) \vdash A$ where $A \in \Pi_{n+1}$, then $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2}) \vdash A$.*

Part (a) of this theorem is due to Gentzen [10]; the proof can be found in Lemma 3.4 of [26] or Theorem 12.3 of [27] and is also repeated below. Part (b) extends the prior result of Schmerl [24] that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ is Π_{n-1}-conservative over $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$; Schmerl's proof was based on reflection principles. A weaker version of (b) with Π_2-conservativity in place of Π_{n+1}-conservativity can be found in [26].

Proof (a) By Proposition 1, it will suffice to show that the theory $I\Delta_0 + TI(\prec \omega_m, \Pi_n)$ can prove $TI(\prec \omega_{m+1}, \Pi_{n-1})$. Let $A(\alpha) \in \Pi_{n-1}$ and let HYP_A be the formula $(\forall\beta)[(\forall\gamma \prec \beta)A(\gamma) \rightarrow A(\beta)]$ and let $\kappa \prec \omega_{m+1}$. We reason inside $I\Delta_0 + TI(\prec \omega_m, \Pi_n)$ to prove $A(\kappa)$ assuming HYP_A. Let $A^*(\alpha)$ be the formula $(\forall\gamma \prec \alpha)A(\gamma)$; by HYP_A, $A^*(\alpha) \rightarrow A^*(\alpha+1)$. Let $J(\beta)$ be the formula

$$(\forall\alpha)\left(A^*(\alpha) \rightarrow A^*(\alpha + \omega^\beta)\right).$$

Clearly, $J \in \Pi_n$. We shall use transfinite induction on J to prove $J(\kappa_0)$ for some fixed $\kappa_0 \prec \omega_m$ such that $\kappa \prec \omega^{\kappa_0}$. Since $A^*(0)$ holds trivially, $J(\kappa_0)$ implies $A^*(\omega^{\kappa_0})$ which, in turn implies $A(\kappa)$. Thus it suffices to prove HYP_J:

$$(\forall\beta)[(\forall\gamma \prec \beta)J(\gamma) \rightarrow J(\beta)]$$

since, using $TI(\prec \omega_m, \Pi_n)$, this implies $J(\kappa_0)$ holds for this particular κ_0. First note that $J(0)$ holds by our observation that $A^*(\alpha) \rightarrow A^*(\alpha+1)$.

Now let β be an arbitrary non-zero ordinal and suppose $(\forall\gamma \prec \beta)J(\beta)$: we must prove $J(\beta)$. If β is a successor ordinal, $\beta = \beta' + 1$, it suffices to show $J(\beta') \to J(\beta' + 1)$, i.e.,

$$(\forall\alpha)\left(A^*(\alpha) \to A^*(\alpha + \omega^{\beta'})\right) \to (\forall\alpha')\left(A^*(\alpha') \to A^*(\alpha' + \omega^{\beta'+1})\right).$$

Assume $J(\beta')$ holds and let α' be arbitrary such that $A^*(\alpha')$ and let $\gamma \prec \alpha' + \omega^{\beta'+1}$; we must show $A^*(\gamma)$. By consideration of Cantor normal forms, $\gamma \prec \alpha' + \omega^{\beta'} \cdot n$ for some finite n. From $J(\beta')$, it follows that

$$(\forall\alpha)\left(A^*(\alpha) \to A^*(\alpha + \omega^{\beta'} \cdot k)\right) \to (\forall\alpha)\left(A^*(\alpha) \to A^*(\alpha + \omega^{\beta'} \cdot (k+1))\right)$$

holds for all (finite) k. By ordinary Π_n-induction, this implies that

$$(\forall\alpha)\left(A^*(\alpha) \to A^*(\alpha + \omega^{\beta'} \cdot k)\right)$$

holds for all finite k. Thus $A^*(\gamma)$ holds. Finally, suppose β is a limit ordinal and assume $(\forall\delta \prec \beta)J(\delta)$ and assume $A^*(\alpha)$. If $\gamma \prec \alpha+\omega^{\beta}$ then $\gamma \prec \alpha+\omega^{\delta}$ for some $\delta \prec \beta$ so $A(\gamma)$ holds by $J(\delta)$. Since γ was arbitrary, $J(\beta)$ follows. That completes the proof of (a).

The proof of (b) consists of a partial formalization of the Main Lemma 10 in the theory $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$. First an important lemma is necessary:

LEMMA 12 *Let $m \geq 2$ and $n \geq 2$. $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ can Σ_n-define precisely the $\prec \omega_m$-primitive recursive in Σ_{n-1} functions.*

Proof By the just established part (a) of Theorem 11, every Σ_n-definable function of $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ is also Σ_n-defined by $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ and hence, by Theorem 7, is $\prec \omega_m$-primitive recursive in Σ_{n-1}. To show the converse, suppose $F(\vec{z})$ is defined from primitive recursive functions g, τ, and κ, from $A(y) = (\exists x)B(x)$ with $B \in \Pi_{n-2}$, and from an ordinal $\kappa_0 \prec \omega_m$ as in the Second Normal From Theorem; so $F(\vec{z}) = f(\tau(\vec{z}))$ where

$$f(\beta) = \begin{cases} f(\kappa(\beta, U_A(\beta))) & \text{if } \kappa(\beta, U_A(\beta)) \prec \beta \preccurlyeq \kappa_0 \\ g(\beta) & \text{otherwise.} \end{cases}$$

Recall the definition of an f-computation series $\beta_0, \ldots, \beta_k$ used in the proof of Theorem 7 to code a partial computation of f. In the proof of Theorem 7, the existence of a maximal length f-computation series beginning with $\beta_0 = \tau(\vec{z})$ was proved by finding the least β_k such that there exists an f-computation series from β_0 to β_k. The existence of β_k was proved via $LOP(\prec \omega_m, \Sigma_n)$: this was the key step in Σ_n-defining F in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$.

To Σ_n-define f and F in $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ requires a more subtle argument. The basic motivation for this argument is that one could try to minimize the ordinals of the form

$$\omega^{\beta_0} + \omega^{\beta_1} + \cdots + \omega^{\beta_{k-1}} + \omega^{\beta_k} \cdot 2$$

with $\beta_0, \ldots, \beta_k$ an f-computation series — but this is too simplistic because of the presence of the U_A function. Instead, we encode partial computations of f by a sequence of ordinals

$$\beta_0, \alpha_0, \beta_1, \alpha_1, \ldots, \beta_k, \alpha_k$$

where $\beta_0, \ldots, \beta_k$ is an f-computation series and where each $\alpha_i \preccurlyeq \omega$ and encodes the value of $U_A(\beta_i)$:

Definition Let α be the Gödel number of an ordinal $\preccurlyeq \omega$. Then $D(\alpha)$ is the integer defined by

$$D(\alpha) \quad = \quad \begin{cases} 0 & \text{if } \alpha = \omega \\ n+1 & \text{if } \alpha = \ulcorner n \urcorner \end{cases}$$

Definition An *f-computation ordinal (fCO)* is (the Gödel number of) an ordinal of the form

$$\omega^{\omega^2 \cdot \beta_0 + \alpha_0} + \omega^{\omega^2 \cdot \beta_1 + \alpha_1} + \cdots \omega^{\omega^2 \cdot \beta_{k-1} + \alpha_{k-1}} + \omega^{\omega^2 \cdot \beta_k + \alpha_k} + \omega^{\omega^2 \cdot \beta_k + \alpha_k}$$

(only the final summand is repeated), where

(*i*) $\beta_{i+1} \prec \beta_i \preccurlyeq \kappa_0$, for $0 \le i < k$,

(*ii*) $\alpha_i \preccurlyeq \omega$, for $0 \le i < k$,

(*iii*) $\beta_{i+1} = \kappa(\beta_i, D(\alpha_i))$, for $0 \le i < k$,

(*iv*) For $0 \le i \le k$,

- if $\alpha_i = \ulcorner n \urcorner$, then $B(\beta_i, n)$ and for all $m < n$, $\neg B(\beta_i, m)$
- if $\alpha_i = \omega$, then $(\forall m) \neg B(\beta_i, m)$,

(*v*) It is not the case that $\kappa(\beta_k, D(\alpha_k)) \prec \beta_k \preccurlyeq \kappa_0$.

A *psuedo-f-computation ordinal (PfCO)* is defined exactly like an f-computation ordinal except that (*v*) is omitted and (*iv*) is replaced by

(*iv'*) For $0 \le i \le k$, if $\alpha_i = \ulcorner n \urcorner$ then $B(\beta_i, n)$.

We write $fCO(\alpha,\vec{z})$ and $PfCO(\alpha,\vec{z})$ for formulas expressing the condition that α is an fCO or PfCO, respectively, with $\beta_0=\tau(\vec{z})$.

The quantifier complexity of $PfCO$ is easily analyzed since (i)-(iii) are primitive recursive and (iv') is Π_{n-2} since $B\in\Pi_{n-2}$ and by $B\Pi_{n-2}$-collection (which is a consequence of $I\Delta_0+TI(\prec\omega_{m+1},\Sigma_{n-2})$ since this theory contains $I\Sigma_{n-1}$). Thus $PfCO$ is a Π_{n-2} formula. Letting $\kappa_1=\omega^{\omega^{\omega^2\cdot\kappa_0+\omega+1}}$ we have that $\kappa_1\prec\omega_{m+1}$ and, therefore, if $\tau(\vec{z})\preccurlyeq\kappa_0$ and $PfCO(\alpha,\vec{z})$, then $\alpha\prec\kappa_1$. We henceforth assume w.l.o.g. that $\tau(\vec{z})\preccurlyeq\kappa_0$. Now, there exists α such that $PfCO(\alpha,\vec{z})$; namely, $\omega^{\omega^{\omega^2\cdot\tau(\vec{x})+\omega}}\cdot 2$. Hence, by $LOP(\prec\omega_{m+1},\Pi_{n-2})$, there is a minimum ordinal denoted α_{min} such that $PfCO(\alpha_{min},\vec{z})$. We claim that $fCO(\alpha_{min},\vec{z})$ also holds. To prove this, suppose

$$\alpha_{min} \;=\; \omega^{\omega^{\omega^2\cdot\beta_0+\alpha_0}}+\cdots+\omega^{\omega^{\omega^2\cdot\beta_k+\alpha_k}}+\omega^{\omega^{\omega^2\cdot\beta_k+\alpha_k}};$$

the only way $fCO(\alpha_{min})$ can fail is if condition (iv) or (v) is violated. First suppose (iv) fails for some value of i. Then, if $\alpha_i=\omega$ but $B(\beta_i,m)$ holds, then

$$\omega^{\omega^{\omega^2\cdot\beta_0+\alpha_0}}+\cdots+\omega^{\omega^{\omega^2\cdot\beta_{i-1}+\alpha_{i-1}}}+\omega^{\omega^{\omega^2\cdot\beta_i+m}}+\omega^{\omega^{\omega^2\cdot\beta_i+m}} \tag{6}$$

is a psuedo f-computation ordinal $\prec\alpha_{min}$ violating the choice of α_{min}. Likewise, if $\alpha_i=\ulcorner n\urcorner$ but $B(\beta_i,m)$ holds with $m<n$, then the same ordinal (6) is a psuedo f-computation ordinal $\prec\alpha_{min}$. Hence (iv) must hold. Now suppose (v) fails. Then,

$$\omega^{\omega^{\omega^2\cdot\beta_0+\alpha_0}}+\cdots+\omega^{\omega^{\omega^2\cdot\beta_{k-1}+\alpha_{k-1}}}+\omega^{\omega^{\omega^2\cdot\beta_k+\alpha_k}}+\omega^{\omega^{\omega^2\cdot\beta_{k+1}+\omega}}+\omega^{\omega^{\omega^2\cdot\beta_{k+1}+\omega}}$$

where $\beta_{k+1}=\kappa(\beta_k,D(\alpha_k))$ is a psuedo f-computation ordinal $\prec\alpha_{min}$, which is again a contradiction. Hence (v) must also hold and α_{min} is an fCO.

Thus $I\Delta_0+TI(\prec\omega_{m+1},\Sigma_{n-2})$ can define $F(\vec{z})$ by proving

$$\begin{aligned}(\forall\vec{z})(\exists!y)\Big[(\exists\alpha)\Big\{&PfCO(\alpha,\vec{z})\wedge(\forall\alpha')(\alpha'\prec\alpha\rightarrow\neg PfCO(\alpha',\vec{z}))\wedge\\ &\alpha=\omega^{\omega^{\omega^2\cdot\beta_0+\alpha_0}}+\cdots+\omega^{\omega^{\omega^2\cdot\beta_k+\alpha_k}}\cdot 2\wedge y=g(\beta_k)\Big\}\Big].\end{aligned} \tag{7}$$

$PfCO$ is a Π_{n-2}-formula so the subformula $(\forall\alpha')(\cdots)$ is in Π_{n-1} and the subformula $(\exists\alpha)(\cdots)$ is a Σ_n-formula; thus this is a Σ_n-definition of $F(\vec{z})$ in $I\Delta_0+TI(\prec\omega_{m+1},\Sigma_{n-2})$.

Q.E.D. Lemma 12

Lemma 12 stated that the Σ_n-definable functions of $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ are precisely the $\prec \omega_m$-primitive recursive in Σ_{n-1} functions; the lemma was proved using the second normal form for such functions. However, this use of the second normal form was not essential for the proof: $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ can also prove that the $\prec \omega_m$-primitive recursive in Σ_{n-1} functions are closed under composition and under $\prec \omega_m$-primitive recursion. These closure properties are proved in $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ by formalizing the proofs of the three normal form theorems. Since the proofs of the normal form theorem were completely constructive, this formalization is straightforward (and left to the reader).

We are now ready to return to the proof of part (b) of Theorem 11, for which it suffices to prove that if $B(\vec{c})$ is a Σ_n-formula and $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves the sequent $\longrightarrow B(\vec{c})$, then so does $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$. In fact, more than this is true: a sequent $\Gamma \longrightarrow \Delta$ of Σ_n-formulas is a consequence of $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ if and only if it is a consequence of $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ — this is a corollary of the next lemma.

MAIN LEMMA 13 *($n \geq 2$, $m \geq 2$) Suppose $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves the sequent $A_1, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell$ and that each A_i and B_j is in Σ_n and that $\vec{c}$ are all the variables free in the sequent. Then there are functions $f_1, \ldots, f_\ell$ which are $\prec \omega_m$-primitive recursive in Σ_{n-1} and are Σ_n-definable in $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ such that $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ proves*

$$Wit^n_{A_1}(w_1, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \longrightarrow Wit^n_{B_1}(f_1(\vec{w}, \vec{c}), \vec{c}), \ldots, Wit^n_{B_\ell}(f_\ell(\vec{w}, \vec{c}), \vec{c}).$$

The proof of Lemma 13 is exactly like the proof of Lemma 10 except that now the definitions of the functions $f_1, \ldots, f_k$ and the proofs that they produce the correct witnesses are now carried out in $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ — the reader should refer back to the earlier proof to verify that it works out as claimed. □

Now suppose $A_1, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell$ is a sequent of Σ_n-formulas which is provable in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$. By the just stated lemma and from the definition of Wit, $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proves

$$Wit^n_{A_1}(w_1, \vec{c}), \ldots, Wit^n_{A_k}(w_k, \vec{c}) \longrightarrow B_1(\vec{c}), \ldots, B_\ell(\vec{c})$$

which, via $\exists$*:left* inferences gives

$$A_1(\vec{c}), \ldots, A_k(\vec{c}) \longrightarrow B_1(\vec{c}), \ldots, B_\ell(\vec{c}).$$

Q.E.D. Theorem 11

THEOREM 14 *Let* $m \geq 2$ *and* $n \geq 1$ *and* $1 \leq k \leq n-1$. *Then* $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1}) \vdash TI(\prec \omega_{m+k}, \Sigma_{n-1-k})$ *and* $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ *is conservative over the theory* $I\Delta_0 + TI(\prec \omega_{m+k}, \Sigma_{n-1-k})$ *with respect to* Π_{n+2-k}*-consequences.*

Proof Apply Theorem 11 k times. □

COROLLARY 15 *Let* $n \geq 1$. *The theory* $I\Sigma_n$ *contains and is* Π_3*-conservative over the theory* $I\Delta_0 + TI(\prec \omega_{n+1}, \Delta_0)$.

Proof Take $m = 2$; since $I\Sigma_n$ is equal to $I\Delta_0 + TI(\prec \omega_2, \Sigma_{n-1})$ the previous theorem with $k = n-1$ yields the corollary. □

Now we are ready to prove the theorem characterizing the Σ_j-definable functions of $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ and of $I\Sigma_n$ for all $1 \leq j \leq n$.

THEOREM 16 *Let* $m \geq 2$ *and* $1 \leq j \leq n$.

(a) *If* $j > 1$ *then the* Σ_j*-definable functions of* $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ *are precisely the functions which are* $\prec \omega_{m+n-j}$*-primitive recursive in* Σ_{j-1}.

(b) *(For* $j = 1$.*) The* Σ_1*-definable functions (i.e., the provably recursive functions) of* $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ *are precisely the functions which are* $\prec \omega_{m+n-1}$*-primitive recursive.*

THEOREM 17 *Suppose* $1 \leq j \leq n$. *The functions which are* Σ_j*-definable in* $I\Sigma_n$ *are precisely the functions which are* $\prec \omega_{n-j+2}$*-primitive recursive in* Σ_{j-1}.

THEOREM 18 *Let* $n \geq 1$. *The provably total functions of* $I\Sigma_n$ *are precisely the* $\prec \omega_{n+1}$*-primitive recursive functions.*

Proof The proof of Theorem 16 is phrased for $j > 1$, but applies equally well to the $j = 1$ case. Suppose $F(\vec{z})$ is Σ_j-defined by $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ proving $(\forall \vec{z})(\exists! y)A(y, \vec{z})$ where $A \in \Sigma_j$. By Theorem 14 with $k = n - j$, $I\Delta_0 + TI(\prec \omega_{m+n-j}, \Sigma_{j-1})$ also proves the Π_{j+1}-sentence $(\forall \vec{z})(\exists! y)A$; that is, it also Σ_j-defines f. Hence, by Theorem 7, $F(\vec{z})$ is $\prec \omega_{m+n-j}$-primitive recursive in Σ_{j-1}. Conversely, every $\prec \omega_{m+n-j}$-primitive recursive in Σ_{j-1} function is Σ_j-definable in $I\Delta_0 + TI(\prec \omega_{m+n-j}, \Sigma_{j-1})$, and hence in $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$, by Theorems 7 and 14. That proves Theorem 16. Theorems 17 and 18 are corollaries of Theorem 16, since $I\Sigma_n$ is the same theory as $I\Delta_0 + TI(\prec \omega_2, \Sigma_{n-1})$. □

Theorem 18 immediately implies the well-known fact that the provably total functions of Peano arithmetic are precisely the $\prec \epsilon_0$-primitive recursive functions.

4. Π_{n+1}-induction rule versus Σ_n induction axiom

This section presents a sketch for a proof of Parsons's theorem on the conservativity of a restricted Π_{n+1}-induction rule over the usual Σ_n-induction axiom — this proof is based on the witness function method. For reasons of length we omit the details of the proof.

The Π_{n+1}-*strict induction rule* allows inferences of the form

$$\frac{\longrightarrow A(0) \qquad A(b) \longrightarrow A(b+1)}{\longrightarrow A(t)}$$

where b is the eigenvariable and occurs only as indicated, t is any term and A is in Π_{n+1}. Note that no side formulas are allowed (otherwise it would be equivalent to the Π_{n+1}-induction axiom). The strict induction rule is equivalent to what Parsons calls the "induction rule" modified only slightly to fit in the framework of the sequent calculus. By free-cut elimination any sequent of Π_{n+1}-formulas which is provable in $I\Delta_0$ plus the Π_{n+1}-strict induction rule has a proof in which every formula is in Π_{n+1}.

Notation Π_{n+1}-*IR* denotes the theory of arithmetic $I\Delta_0$ plus the Π_{n+1}-strict induction rule. This system is always presumed to be formalized in the sequent calculus.

It is not too difficult to see that Π_{n+2}-*IR* proves the Σ_n induction axioms, for all $n \geq 0$. To prove this, if $A(b) \in \Sigma_n$, use the strict induction rule on the formula

$$[A(0) \land (\forall x)(A(x) \to A(x+1))] \to A(b)$$

with respect to the variable b.

THEOREM 19 *(Parsons [22]) Let $n \geq 1$. A Π_{n+1}-sentence is a theorem of $I\Sigma_n$ iff it is a consequence of Π_{n+1}-IR.*

Parsons's proof of Theorem 19 was based on the Gödel Dialectica interpretation; other proof-theoretic proofs of Theorem 19 have been given in [19, 25]. The main novelty of our proof outlined below is that it uses the witness function method directly.

Proof (Outline): The easy direction is that if $I\Sigma_n \vdash A$ where $A \in \Pi_{n+1}$, then Π_{n+1}-*IR* also proves A. Since $A \in \Pi_{n+1}$, A is expressible as $(\forall\vec{x})B(\vec{x})$ where $B \in \Sigma_n$; it suffices to show that Π_{n+1}-*IR* $\vdash B(\vec{c})$. By free-cut elimination, there is a $I\Sigma_n$-proof P of $B(\vec{c})$ such that every formula occuring in P is a Σ_n-formula. We now can prove by induction on the number of inferences in this proof that every sequent in P is a consequence of Π_{n+1}-IR. The only difficult case is the induction inferences, which are of the form

$$\frac{\Gamma, A(b) \longrightarrow A(b+1), \Delta}{\Gamma, A(0) \longrightarrow A(t), \Delta}$$

Letting $D(b)$ be the formula $(\bigwedge \Gamma \wedge A(b)) \vee (\bigvee \Delta)$, the upper sequent is logically equivalent to $D(b) \rightarrow D(b+1)$ and the lower sequent is logically equivalent to $D(0) \rightarrow D(t)$. And if Π_{n+1}-IR proves the upper sequent, then it also proves the lower sequent by use of the strict induction rule on the formula $D(0) \rightarrow D(b)$, which, as a Boolean combination of Σ_n-formulas is logically equivalent to a Π_{n+1}-formula.

For the hard direction of Theorem 19, we need the next lemma. We let PRA_n be a set of function symbols for the functions which are primitive recursive in Σ_n. By Theorem 8, each function symbol in PRA_{n-1} represents a function which is Σ_n-definable in $I\Sigma_n$ — we may augment the language of $I\Sigma_n$ with these function symbols, provided we are careful not to use them in induction formulas. In the next lemma, the notation $\vec{x}_i$ denotes a vector of variables and $||\vec{x}_i||$ denotes the number (possibly zero) of variables in the vector.

LEMMA 20 *Suppose $A_i(\vec{x}_i, \vec{c})$ and $B_j(\vec{y}_j, \vec{c})$ are Σ_n-formulas, for $1 \le i \le k$ and $1 \le j \le \ell$, and that Π_{n+1}-IR proves the sequent*

$$(\forall \vec{x}_1)A_1(\vec{x}_1, \vec{c}), \ldots, (\forall \vec{x}_k)A_k(\vec{x}_k, \vec{c}) \longrightarrow (\forall \vec{y}_1)B_1(\vec{y}_1, \vec{c}), \ldots, (\forall \vec{y}_\ell)B_\ell(\vec{y}_\ell, \vec{c}). \quad (8)$$

Let $f_1, \ldots, f_k$ be new function symbols so that f_i has arity $||\vec{x}_i|| + ||c||$. Then there are terms $t_i(\vec{y}_1, \ldots, \vec{y}_\ell, \vec{c})$ in the language $PRA_{n-1} \cup \{f_1, \ldots, f_k\}$, for $1 \le i \le \ell$, such that $I\Sigma_n$ proves

$$\begin{aligned}(\forall \vec{x}_1)Wit^n_{A_1}(f_1(\vec{x}_1, \vec{c}), \vec{x}, \vec{c}), \ldots, (\forall \vec{x}_k)Wit^n_{A_k}(f_k(\vec{x}_k, \vec{c}), \vec{x}, \vec{c})& \\ \longrightarrow Wit^n_{B_1}(t_1, \vec{y}_1, \vec{c}), \ldots, Wit^n_{B_\ell}(t_\ell, \vec{y}_\ell, \vec{c}).& \quad (9)\end{aligned}$$

Theorem 19 follows immediately from Lemma 20 with $k = 0$ and $\ell = 1$ and from the fact that every PRA_{n-1}-function is definable in $I\Sigma_n$. For reasons of length, we omit the proof of Lemma 20: the general idea of the proof is a relatively straightforward use of the witness function method; however, it requires the development of some deep facts about primitive recursive (in Σ_n) functions. An important feature of the lemma is that each term t_i may involve all of $\vec{y}_1, \ldots, \vec{y}_\ell$.

A second theorem of Parsons is that Theorem 19 also holds with the addition of the $B\Sigma_n$-collection axiom:

THEOREM 21 *(Parsons [22]) Let $n \geq 1$. The Π_{n+1}-consequences of Π_{n+1}-$IR + B\Sigma_n$ are the same as the Π_{n+1}-consequences of $I\Sigma_n$.*

Proof (Outline) Recall that $B\Pi_{n-1}$ is equivalent to $B\Sigma_n$, relative to the base theory $I\Delta_0$. The $B\Pi_{n-1}$ axioms contain unbounded quantifiers in the scope of bounded quantifiers, so it is not possible to use free-cut elimination to force a proof in Π_{n+1}-$IR + B\Sigma_n$ to contain only Π_{n+1}-formulas. We let Π_n^+ denote the set of formulas which have n blocks of like unbounded quantifiers, starting with a block of universal quantifiers, allowing arbitrary bounded quantifiers to be included in the first block of unbounded quantifiers (see the next section for a careful definition of the analogous class Σ_n^+). Now, temporarily define the set of Σ_n^* formulas to be the formulas which are of one of the following forms: (1) $(\exists\vec{y})B(\vec{x})$ where $B \in \Pi_{n-1}^+$ or (2) $(\forall z \leq t)(\exists y_1)B(y_1, z, \vec{c})$ where $B \in \Pi_{n-1}$. We also define the Π_{n+1}^* formulas to be the formulas which are either Π_{n+1} or Σ_n^*. Since the $B\Pi_{n-1}$ axioms can be formulated in the form $A \longrightarrow A'$ with A and A' both in Σ_n^*, the free-cut elimination theorem implies that if $\Gamma \longrightarrow \Delta$ is a sequent of Π_{n+1}^*-formulas provable in Π_{n+1}-$IR + B\Pi_n$, then this sequent has a proof in which every formula is a Π_{n+1}^*-formula. The notion of "witness" can be generalized as follows: if $A(\vec{c})$ is a Σ_n^*-formula in one of the above forms; then, if A is of form (1), $Wit_A^{*n}(w, \vec{c})$ is defined just like $Wit_A^n(w, \vec{c})$ was and, if A is of form (2) then $Wit_A^{*n}(w, \vec{c})$ is defined to be the formula

$$(\forall z \leq t)Wit_{(\exists y_1)B}^n((w)_z, z, \vec{c}).$$

LEMMA 22 *Suppose $A_i(\vec{x}_i, \vec{c})$ and $B_j(\vec{y}_j, \vec{c})$ are Σ_n^*-formulas, for $1 \leq i \leq k$ and $1 \leq j \leq \ell$, and that Π_{n+1}-$IR + B\Sigma_n$ proves the sequent*

$$(\forall\vec{x}_1)A_1(\vec{x}_1, \vec{c}), \ldots, (\forall\vec{x}_k)A_k(\vec{x}_k, \vec{c}) \longrightarrow (\forall\vec{y}_1)B_1(\vec{y}_1, \vec{c}), \ldots, (\forall\vec{y}_\ell)B_\ell(\vec{y}_\ell, \vec{c}).$$

Let $f_1, \ldots, f_k$ be new function symbols so that f_i has arity $||\vec{x}_i|| + ||c||$. Then there are terms $t_i(\vec{y}_1, \ldots, \vec{y}_\ell, \vec{c})$ in the language $PRA_{n-1} \cup \{f_1, \ldots, f_k\}$, for $1 \leq i \leq \ell$, such that $I\Sigma_n$ proves

$$(\forall\vec{x}_1)Wit_{A_1}^{*n}(f_1(\vec{x}_1, \vec{c}), \vec{x}, \vec{c}), \ldots, (\forall\vec{x}_k)Wit_{A_k}^{*n}(f_k(\vec{x}_k, \vec{c}), \vec{x}, \vec{c}) \longrightarrow Wit_{B_1}^{*n}(t_1, \vec{y}_1, \vec{c}), \ldots, Wit_{B_\ell}^{*n}(t_\ell, \vec{y}_\ell, \vec{c}). \quad (10)$$

We omit the proof of the lemma and the rest of Theorem 21.

Finally, it should be remarked that Π_{n+1}-$IR + B\Sigma_n$ does not contain $I\Sigma_n$. This can be proved by noting that Π_{n+1}-$IR + I\Sigma_n$ is not Π_{n+2}-conservative over $I\Sigma_n$. For example, with $n = 1$, let $A(k, m)$ be the Ackermann function so that the functions $f_k(m) = A(k, m)$ are all primitive recursive and so that each primitive recursive function is eventually dominated by f_k for sufficiently large k. Let $A^*(k,m,y)$ be the graph of the Ackermann function; it is well-known that $A^*(k,m,y)$ is Δ_0 (for us it is sufficient that it is Σ_1). Now, it is easy to see that $I\Sigma_1$ proves $(\forall x)(\exists y)A^*(0,x,y)$ and

$$(\forall x)(\exists y)A^*(b,x,y) \longrightarrow (\forall x)(\exists y)A^*(b+1,x,y).$$

Thus $\Pi_2\text{-}IR + I\Sigma_1 \vdash (\forall k)(\forall x)(\exists y)A^*(k,x,y)$. But the Ackermann function is not primitive recursive, hence not Σ_1-definable in $I\Sigma_1$. Thus $\Pi_2\text{-}IR + I\Sigma_1$ is not Π_2-conservative over $I\Sigma_1$ and thus not equal to $\Pi_2\text{-}IR$ and not a subtheory of $\Pi_2\text{-}IR + B\Sigma_1$.

To show $\Pi_{n+1}\text{-}IR + B\Sigma_n \nvdash I\Sigma_n$ for $n > 1$, use essentially the same argument, but use 'primitive recursive in Σ_{n-1}' in place of 'primitive recursive' and use a suitable replacement of the Ackermann function that dominates the functions primitive recursive in Σ_{n-1}.

5. Conservativity of collection over induction

In this section we prove the well-known theorem that the $B\Sigma_{n+1}$-collection axioms are Π_{n+2}-conservative over $I\Sigma_n$. The proof method does not use the witness function method per se, but it involves an induction on the length of free-cut free proofs similar to the methods of earlier sections. Earlier proofs of this theorem include Parsons [22] and Paris-Kirby [21]; see in addition, [3, 25]. The advantage of our proof below is that it gives a direct and elementary proof-theoretic proof.

Recall that the $B\Sigma_{n+1}$-collection axioms are equivalent to the $B\Pi_n$-collection axioms. In the sequent calculus, the $B\Pi_n$-collection axioms are of the form

$$(\forall x \leq a)(\exists y)A(x,y) \longrightarrow (\exists z)(\forall x \leq a)(\exists y \leq z)A(x,y)$$

where $A \in \Pi_n$ and may contain free variables besides x, y. In the above sequent there are bounded quantifiers outside of unbounded quantifiers so the formulas are not, strictly speaking, Σ_{n+1}-formulas. Accordingly, we define a generalized form of Σ_{n+1}-formulas that will be allowed to appear in free-cut free proofs.

Definition The class Σ_{n+1}^+ of formulas is defined inductively by

(1) $\Pi_n \subseteq \Sigma_{n+1}^+$,

(2) If $A \in \Sigma_{n+1}^+$, then $(\exists x)A$, $(\exists x \leq t)A$ and $(\forall x \leq t)A$ are in Σ_{n+1}^+, where t is any term not involving x.

If s is a term and A is a Σ_{n+1}^{+}-formula, then $A^{\leqslant s}$ is the formula obtained by bounding unbounded existential quantifiers in the outermost block of quantifiers of A by the term s; namely,

Definition Fix n and suppose $A \in \Sigma_{n+1}^{+}$.

(1) If $A \in \Pi_n$, then $A^{\leqslant s}$ is A.

(2) If A is $(\exists x)B$ and $A \notin \Pi_n$, then $A^{\leqslant s}$ is $(\exists x \leq s)B$.

(3) If A is $(Qx \leq t)B$ then $A^{\leqslant s}$ is $(Qx \leq t)(B^{\leqslant s})$.

Let $\Gamma \longrightarrow \Delta$ be a sequent $A_1, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell$ of Σ_{n+1}^{+}-formulas. Then $\Gamma^{\leqslant s}$ is the formula $\bigwedge_{i=1}^{k} A_i^{\leqslant s}$ and $\Delta^{\leqslant s}$ is the formula $\bigvee_{j=1}^{\ell} B_j^{\leqslant s}$. This notation should cause no confusion since antecedents and succedents are always clearly distinguished.

If $\vec{c} = c_1, \ldots c_s$ is a vector of free variables, then $\vec{c} \leq u$ abbreviates the formula $c_1 \leq s \wedge \cdots \wedge c_s \leq u$. $(\forall \vec{c} \leq u)$ and $(\exists \vec{c} \leq u)$ abbreviate the corresponding vectors of bounded quantifiers.

THEOREM 23 *$(n \geq 1)$ Suppose $\Gamma \longrightarrow \Delta$ is a sequent of Σ_{n+1}^{+}-formulas that is provable in $I\Delta_0 + B\Sigma_{n+1}$. Let $\vec{c}$ include all the free variables occurring in $\Gamma \longrightarrow \Delta$. Then*

$$I\Sigma_n \vdash (\forall u)(\exists v)(\forall \vec{c} \leq u)\Big(\Gamma^{\leqslant u} \rightarrow \Delta^{\leqslant v}\Big).$$

Intuitively, the theorem is saying that given a bound u on the sizes of the free variables and on the sizes of the witness for the formulas in Γ, there is a bound v for the values of a witness for a formula in Δ.

Theorem 23 immediately implies the main theorem of this section:

THEOREM 24 *$I\Delta_0 + B\Sigma_{n+1}$ is Π_{n+2}-conservative over $I\Sigma_n$.*

Recall that $I\Delta_0 + B\Sigma_{n+1} \vdash I\Sigma_n$. Before proving Theorem 23, we establish the following lemma (due to Clote and Hájek).

LEMMA 25 *$(n \geq 1)$ Let $B(\vec{c}, d) \in \Pi_n$. Then*

$$I\Sigma_n \vdash (\forall u)(\exists v)(\forall \vec{c} \leq u)[(\forall x)B(\vec{c}, x) \leftrightarrow (\forall x \leq v)B(\vec{c}, x)].$$

The formula of Lemma 25 is called the Σ_n-strong replacement principle.

Proof Let s be the length of the vector $\vec{c}$. We reason inside $I\Sigma_n$. Let $C(\vec{c}, d)$ be the Σ_n-formula $\neg B(\vec{c}, d)$. Let $Num(u, \ell)$ be the formula expressing

$\exists\langle\vec{c}_1, d_1, \ldots, \vec{c}_\ell, d_\ell\rangle$ s.t. $\vec{c}_1, \ldots, \vec{c}_\ell$ are distinct s-tuples $\leq u$ and $C(\vec{c}_i, d_i)$ holds for all $1 \leq i \leq \ell$.

Of course, this asserts that there are $\geq \ell$ distinct values of $\vec{c} \leq u$ for which $(\exists x)C(\vec{c}, x)$ holds. Now Num is a Σ_n-formula and $Num(\vec{c}, (u+1)^s + 1)$ is clearly false; so by $I\Sigma_n$, there is a value ℓ_0 such that $Num(\vec{c}, \ell_0)$ but not $Num(\vec{c}, \ell_0 + 1)$. Given $\vec{c}_1, d_1, \ldots, \vec{c}_{\ell_0}, d_{\ell_0}$ witnessing $Num(\vec{c}, \ell_0)$, let $v = \max\{d_1, \ldots, d_{\ell_0}\}$. It follows that

$$(\forall \vec{c} \leq u)\Big((\exists x)C(\vec{c}, x) \leftrightarrow (\exists x \leq v)C(\vec{c}, x)\Big)$$

which is what we needed to prove. □

Proof of Theorem 23: By free-cut elimination, $\Gamma \longrightarrow \Delta$ has a sequent calculus proof P in which every formula is a Σ_{n+1}^+-formula. (Since we allow bounded quantifiers in Σ_{n+1}^+-formulas, it is convenient to work in the sequent calculus LKB with inference rules for bounded quantifiers [2].) We prove the theorem by induction on the number of inferences in P. The proof splits into cases depending on the last inference of P. The hardest case, $\forall$*:right* is saved for last.

Case (1): If P has no inferences and $\Gamma \longrightarrow \Delta$ is an initial sequent, then either $\Gamma \longrightarrow \Delta$ is a logical, equality or arithmetic axiom, containing only Δ_0-formulas, and the theorem is trivial, or $\Gamma \longrightarrow \Delta$ is a $B\Sigma_{n+1}$ axiom. In the latter case, taking $v = u$, it is immediate that $I\Sigma_n$ proves

$$(\forall x \leq a)(\exists y \leq u)A(x, y) \rightarrow (\exists z \leq u)(\forall x \leq a)(\exists y \leq z)A(x, y)$$

and the theorem holds.

Case(2): Suppose the last inference of P is a structural inference, a propositional inference or a $\forall$*:left* or $\forall \leq$*:left* inference. The inference may have either one or two premisses:

$$\frac{\Pi \longrightarrow \Lambda}{\Gamma \longrightarrow \Delta} \qquad \text{or} \qquad \frac{\Pi_1 \longrightarrow \Lambda_1 \quad \Pi_2 \longrightarrow \Lambda_2}{\Gamma \longrightarrow \Delta}$$

It is easily checked that, in the first case we have that $I\Sigma_n$ proves $\Gamma^{\leqslant u} \rightarrow \Pi^{\leqslant u}$ and $\Lambda^{\leqslant v} \rightarrow \Delta^{\leqslant v}$ and, in the second case we have that $I\Sigma_n$ proves $\Gamma^{\leqslant u} \rightarrow \Pi_1^{\leqslant u} \wedge \Pi_2^{\leqslant u}$ and $\Lambda_1^{\leqslant v} \wedge \Lambda_2^{\leqslant v} \rightarrow \Delta^{\leqslant v}$. In the first case, the induction hypothesis states that $I\Sigma_n$ proves

$$(\exists v)(\forall \vec{c} \leq u)\Big(\Pi^{\leqslant u} \rightarrow \Lambda^{\leqslant v}\Big)$$

from which $(\exists v)(\forall \vec{c} \leq u)(\Gamma^{\leqslant u} \to \Delta^{\leqslant v})$ follows. In the second case, by the induction hypothesis, $I\Sigma_n$ proves

$$(\exists v_i)(\forall \vec{c} \leq u)\left(\Pi_i^{\leqslant u} \to \Lambda_i^{\leqslant v_i}\right)$$

for $i = 1, 2$. Taking $v = \max\{v_1, v_2\}$ and noting that $I\Sigma_n$ proves $v_i \leq v \land \Lambda_i^{\leqslant v_i} \to \Lambda_i^{\leqslant v}$, we get that $I\Sigma_n$ proves $(\exists v)(\forall \vec{c} \leq u)(\Gamma^{\leqslant u} \to \Delta^{\leqslant v})$.

Case (3): Suppose the final inference of P is an $\exists$*:right* inference:

$$\frac{\Gamma \longrightarrow B(\vec{c}, t(\vec{c})), \Lambda}{\Gamma \longrightarrow (\exists x)B(\vec{c}, x), \Lambda}$$

We reason inside $I\Sigma_n$ as follows: given arbitrary u, there is (by the induction hypothesis) a v' such that

$$(\forall \vec{c} \leq u)\left(\Gamma^{\leqslant u} \to B^{\leqslant v'}(\vec{c}, t(\vec{c})) \lor \Lambda^{\leqslant v'}\right).$$

Letting $v = \max\{v', t(u, \ldots, u)\}$ we have that $t(\vec{c}) \leq v$ for all $\vec{c} \leq u$ (since the language has 0, S, $+$ and $\cdot$ as the only function symbols). This v makes the theorem true. The case where the last inference of P is a $\exists \leq$*:right* is similar.

Case (4): Suppose the last inference of P is an $\exists$*:left*:

$$\frac{A(\vec{c}, d), \Gamma \longrightarrow \Delta}{(\exists x)A(\vec{c}, x), \Gamma \longrightarrow \Delta}$$

where d is the eigenvariable occuring only where indicated. The induction hypothesis is that $I\Sigma_n$ proves

$$(\forall u)(\exists v)(\forall \vec{c}, d \leq u)\left(A^{\leqslant u}(\vec{c}, d) \land \Gamma^{\leqslant u} \to \Delta^{\leqslant v}\right).$$

This is equivalent to

$$(\forall u)(\exists v)(\forall \vec{c} \leq u)\left((\exists d \leq u)A^{\leqslant u}(\vec{c}, d) \land \Gamma^{\leqslant u} \to \Delta^{\leqslant v}\right)$$

which is what we needed to prove.

Case (5): The $\exists \leq$*:left* inference is a little more subtle. If the final inference of P is

$$\frac{d \leq t(\vec{c}), A(\vec{c}, d), \Gamma \longrightarrow \Delta}{(\exists x \leq t(\vec{c}))A(\vec{c}, x), \Gamma \longrightarrow \Delta}$$

we reason inside $I\Sigma_n$ as follows. Let u be arbitrary, there is a v' such that

$$(\forall \vec{c}, d \leq u)\left(d \leq t(\vec{c}) \land A^{\leqslant u}(\vec{c}, d) \land \Gamma^{\leqslant u} \to \Delta^{\leqslant v'}\right). \tag{11}$$

Let $u' = \max\{u, t(\vec{u})\}$; by the induction hypothesis, there is a v such that (11) holds with u', v in place of u, v'. Now let $\vec{c} \leq u$ and suppose $(\exists x \leq t)A^{\leqslant u}(\vec{c}, x) \wedge \Gamma^{\leqslant u}$. Clearly, this implies $(\exists x \leq u')(x \leq t \wedge A^{\leqslant u'} \wedge \Gamma^{\leqslant u'})$. Taking d to be this x, we have $\Delta^{\leqslant v}$ holds.

Case (6): Suppose the last inference of P is a *Cut*:

$$\frac{\Gamma_1 \longrightarrow \Delta_1, A \qquad A, \Gamma_2 \longrightarrow \Delta_2}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}$$

We reason inside $I\Sigma_n$. Suppose u is arbitrary and $\Gamma_1^{\leqslant u} \wedge \Gamma_2^{\leqslant u}$. Pick v_1, depending only on u by the induction hypothesis, so that $\Delta^{\leqslant v_1} \vee A^{\leqslant v_1}$. Let $u_2 = \max\{v_1, u\}$. By the induction hypothesis, there is a $v \geq v_1$ depending only on u_2 so that if $A^{\leqslant v_1}$ holds, then $\Delta_2^{\leqslant v}$ holds. Now clearly either $\Delta_1^{\leqslant v}$ or $\Delta_2^{\leqslant v}$ holds. Since v depends only on u, this proves this case.

Case (7): Suppose the final inference of P is a $\forall$*:right*:

$$\frac{\Gamma \longrightarrow B(\vec{c}, d), \Lambda}{\Gamma \longrightarrow (\forall x)B(\vec{c}, x), \Lambda}$$

Note $B \in \Pi_n$ since $(\forall x)B$ must be a Σ^+_{n+1}-formula. We reason inside $I\Sigma_n$. Let u be arbitrary. By Σ_n-strong replacement (Lemma 25) there is a $u' \geq u$ such that

$$(\forall \vec{c} \leq u)\Big((\forall x)B(\vec{c}, x) \leftrightarrow (\forall x \leq u')B(\vec{c}, u')\Big).$$

Let $v \geq u'$ be given by the induction hypothesis so that

$$(\forall \vec{c}, d \leq u')\Big(\Gamma^{\leqslant u'} \rightarrow B(\vec{c}, d) \vee \Delta^{\leqslant v}\Big). \tag{12}$$

Now let $\vec{c} \leq u$ be arbitrary such that $\Gamma^{\leqslant u}$. We need to show $(\forall x)B(\vec{c}, x) \vee \Delta^{\leqslant v}$. Suppose not, then there is a $d \leq u'$ such that $\neg B(\vec{c}, d)$, and by (12), $\Delta^{\leqslant v}$ holds, which is a contradiction.

The case where the final inference of P is a $\forall \leq$*:left* inference is similar, although Lemma 25 is not needed.

Q.E.D. Theorem 23

It would be interesting to give a similar proof that Π_{n+1}-$IR + B\Sigma_n$ is Π_{n+1}-conservative over Π_{n+1}-IR, in place of the more complicated and omitted proof of Theorem 21 above.

6. Analogies between bounded and Peano arithmetic

The witness function method has been extensively used characterizing definable functions of fragments of bounded arithmetic — the work in section 3 above gives an approach to Peano arithmetic which is very similar to some of the proofs used earlier in bounded arithmetic.

First, Theorem 8, which characterized the Σ_n-definable functions of $I\Sigma_n$ is analogous to the main theorem of Buss [2] which characterized the Σ_n^b-definable functions of S_2^n (which is axiomatized with Σ_n^b-PIND axioms). In $I\Sigma_n$, the Σ_n-definable functions are precisely the functions primitive recursive in Σ_{n-1}; whereas, in S_2^n, the Σ_n^b-definable functions are precisely the functions polynomial time computable with respect to a (usual) Σ_{n-1}^p-oracle. It should be noted that a usual Σ_{n-1}^p-oracle is equivalent to a witness oracle for Σ_{n-1}^p with respect to polynomial time computation, since there is an a-priori bound on the size of a witness and a witness value may be queried bit-by-bit. The proofs of these two theorems are analogous as well.

Second, Theorem 11, which stated that $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ is Π_{n+1}-conservative over $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ is analogous to the result of [4] that S_2^n is $\forall\Sigma_n^b$-conservative over T_2^{n-1}. To see the analogy more sharply, note on one hand $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ and $I\Delta_0 + TI(\prec \omega_{m+1}, \Sigma_{n-2})$ are equivalent to $I\Delta_0 + TI(\prec \omega_m, \Pi_n)$ and $I\Delta_0 + TI(\prec \omega_{m+1}, \Pi_{n-1})$ (respectively), which are axiomatized with transfinite induction on Π_n-formulas up to ordinals $\prec \omega_m$ and on Π_{n-1} formulas up to ordinals $\prec \omega^{\omega_m}$; and on the other hand, S_2^n may be axiomatized by induction (PIND) on Π_n^b-formula up to lengths $|x|$ and T_2^{n-1} may be axiomatized by induction on Π_n^b-formulas up to $2^{|x|}$. So both conservation theorems give situations where the complexity of induction formulas may be reduced by one block of quantifier alternation in exchange for "exponentiating" the length of induction. Another theorem of this type is the result of [6] that R_3^n is $\forall\Sigma_n^b$-conservative over S_3^{n-1}.

Witness oracles have been applied to bounded arithmetic in [18] and in [6]. Another area of contact between bounded arithmetic and Peano arithmetic may be found in Kaye [14] who gives a proof that $I\Sigma_n \neq B\Sigma_{n+1}$ based on methods used earlier by [18] to show that if $T_2^{n+1} = S_2^{n+1}$ then the polynomial time hierarchy collapses.

We conclude with a partial characterization of the Σ_j-definable functions of $I\Sigma_n$ when $j > n$:

Definition Let A be a formula; w.l.o.g. all negations in A are on atomic formulas. The *counterexample oracles of* A are the witness oracles $U_{(\exists x)\neg B}$ for $(\forall x)B$ a subformula of A.

THEOREM 26 *Let $j > n \geq 1$. Suppose $I\Sigma_n \vdash (\forall x)(\exists! y)A(x,y)$ where $A \in \Sigma_j$. Then the function $f : x \mapsto y$, such that $(\forall x)A(x, f(x))$, is primitive recursive in Σ_{n-1} and in the counterexample oracles for A.*

The same holds for $I\Delta_0 + TI(\prec \omega_m, \Sigma_{n-1})$ with "primitive recursive" replaced by "$\prec \omega_m$-primitive recursive".

The proof of this theorem is analogous to the proof of Theorems 7 and 8 except that the $\forall$*:right* cases of the proof now have to accommodate the fact that a $\forall$*:right* quantifier may be an ancestor of a quantifier in $(\exists y)A(c,y)$. Of course a counterexample oracle for A is exactly what is needed for this case.

Theorem 26 can be extended to partially characterize the Σ_j^b-definable functions of T_2^{n-1} or S_2^n when $j > n$; namely,

THEOREM 27 *(See [18, 23, 17]) Let* $j > n \geq 1$.

(a) *Suppose* $A \in \Sigma_j^b$ *and* $S_2^n \vdash (\forall x)(\exists! y)A(x,y)$. *Then the function* f *such that* $(\forall x)A(x, f(x))$ *can be computed by a polynomial time Turing machine with an oracle for* Σ_{n-1}^p *and with the counterexample oracles of* A.

(b) *Suppose* $A \in \Sigma_j^b$ *and* $T_2^{n-1} \vdash (\forall x)(\exists! y)A(x,y)$. *Then the function* f *such that* $(\forall x)A(x, f(x))$ *can be computed by a polynomial time Turing machine which makes a constant number of queries to an oracle for* Σ_{n-1}^p *and to the counterexample oracles of* A.

References

[1] B. ALLEN, *Arithmetizing uniform NC.* Ph.D. thesis, University of Hawaii, 1989.

[2] S. R. BUSS, *Bounded Arithmetic*, Bibliopolis, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[3] ——, *A conservation result concerning bounded theories and the collection axiom*, Proceedings of the American Mathematical Society, 100 (1987), pp. 709–716.

[4] ——, *Axiomatizations and conservation results for fragments of bounded arithmetic*, in Logic and Computation, proceedings of a Workshop held Carnegie-Mellon University, 1987, vol. 106 of Contemporary Mathematics, American Mathematical Society, 1990, pp. 57–84.

[5] S. R. BUSS AND J. KRAJÍČEK, *An application of Boolean complexity to separation problems in bounded arithmetic.* in preparation.

[6] S. R. BUSS, J. KRAJÍČEK, AND G. TAKEUTI, *Provably total functions in bounded arithmetic theories* R_3^i, U_2^i *and* V_2^i. To appear in Arithmetic, Proof theory and Computational Complexity, ed. P. Clote and J. Krajíček, Oxford University Press.

[7] P. CLOTE, *A first-order theory for the parallel complexity class NC*, Tech. Rep. BCCS-89-01, Boston College, Jan. 1989. To be published in expanded form jointly with G. Takeuti.

[8] P. CLOTE AND G. TAKEUTI, *Exponential time and bounded arithmetic (extended abstract)*, in Structure in Complexity, Lecture Notes in Computer Science #223, Springer Verlag, 1986, pp. 77–103.

[9] G. GENTZEN, *Neue Fassung des Widerspruchsfreiheitbeweis für der reinen Zahlentheorie*, Forschungen zur Logik end zur Grundlegung der exacten Wissenschaften, New Series, 4 (1938), pp. 19–44. English translation in [11], pp. 252-286.

[10] ——, *Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie*, Mathematische Annalen, 119 (1943), pp. 140–161. English translation in [11], pp. 287-308.

[11] ——, *Collected Papers of Gerhard Gentzen*, North-Holland, 1969. Edited by M. E. Szabo.

[12] K. GÖDEL, *Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes*, Dialectica, 12 (1958), pp. 280–287.

[13] W. A. HOWARD, *Assignment of ordinals to terms for primitive recursive functionals of finite type*, in Intuitionism and Proof Theory, North-Holland, 1970, pp. 443–458.

[14] R. KAYE, *Using Herbrand-type theorems to separate strong fragments of arithmetic.* Typeset manuscript, August 1991.

[15] J. KETONEN AND R. SOLOVAY, *Rapidly growing Ramsey functions*, Annals of Mathematics, 113 (1981), pp. 267–314.

[16] J. KRAJÍČEK, *Fragments of bounded arithmetic and bounded query classes.* To appear in Transactions of the A.M.S.

[17] ——, *No counter-example interpretation and interactive computation.* In Logic From Computer Science, Proc. of a Workshop held Nov. 13-17, 1989, Springer-Verlag, 1992, pp. 287-293.

[18] J. KRAJÍČEK, P. PUDLÁK, and G. TAKEUTI, *Bounded arithmetic and the polynomial hierarchy*, Annals of Pure and Applied Logic, 52 (1991), pp. 143–153.

[19] G. E. MINTS, *Quantifier-free and one-quantifier systems*, Journal of Soviet Mathematics, 1 (1973), pp. 71–84.

[20] J. PARIS AND L. HARRINGTON, *A Mathematical Incompleteness in Peano Arithmetic* in Handbook of Mathematical Logic, North-Holland, 1977, pp. 1133–1142.

[21] J. B. PARIS AND L. A. S. KIRBY, *Σ_n-collection schemes in arithmetic*, in Logic Colloquium '77, North-Holland, 1978, pp. 199–210.

[22] C. PARSONS, *On a number-theoretic choice schema and its relation to induction*, in Intuitionism and Proof Theory: proceedings of the summer conference at Buffalo N.Y. 1968, North-Holland, 1970, pp. 459–473.

[23] P. PUDLÁK, *Some relations between subsystems of arithmetic and the complexity of computations.* In Logic From Computer Science, Proc. of a Workshop held Nov. 13-17, 1989, Springer-Verlag, 1992, pp. 499-519.

[24] U. R. SCHMERL, *A fine structure generated by reflection formulas over primitive recursive arithmetic*, in Logic Colloquium 78, North-Holland, 1979, pp. 335–350.

[25] W. SIEG, *Fragments of arithmetic*, Annals of Pure and Applied Logic, 28 (1985), pp. 33–71.

[26] R. SOMMER, *Transfinite Induction and Hierarchies Generated by Transfinite Recursion within Peano Arithmetic*, PhD thesis, U.C. Berkeley, 1990.

[27] G. TAKEUTI, *Proof Theory*, North-Holland, 2nd ed., 1987.