The Worm principle

Lev D. Beklemishev*
Steklov Mathematical Institute, Moscow
and Utrecht University
e-mail: Lev.Beklemishev@phil.uu.nl

10th March 2003

Abstract

In [6] an approach to proof-theoretic analysis of Peano arithmetic based on the notion of graded provability algebra was suggested. Here we present a provability-algebraic version of the independent combinatorial Hydra battle principle. This allows for simple independence proofs of both principles based on provability-algebraic mathods.

1 Introduction

This paper is a companion to [6] where a proof-theoretic analysis of Peano arithmetic based on the concept of *graded provability algebra* is given. A particular feature of this approach is that a system of ordinal notation for ϵ_0 naturally emerges from the closed fragment of a certain decidable propositional modal logic. This unusual view of ϵ_0 suggests to have a closer look at some traditional applications of proof-theoretic analysis such as combinatorial independence results.

Here we present a simple statement of combinatorial nature that is independent of Peano Arithmetic and is motivated by the provability algebraic view of ϵ_0. The principle asserts the termination of a certain combinatorial game similar to the well-known *Hydra battle* of L. Kirby and J. Paris [12] which we call the *Worm battle*. In fact, modulo some details, the Hydra principle and the Worm principle turn out to be mutually translatable and one can easily infer the independence of the one from that of the other.[1] Thus, we essentially provide an alternative proof of the Kirby–Paris independence result. However, the Worm principle also has some independent interest because of the naturality of its provability algebraic interpretation.

*Supported by Russian Foundation for Basic Research.

[1] This direct translatability has been noticed in private correspondence independently by A. Weiermann, G.Lee and L. Carlucci.

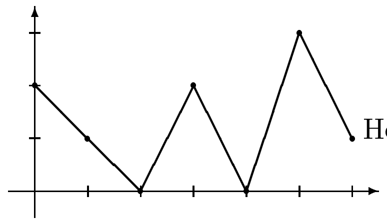

Figure 1: A Worm

Incidentally, L. Carlucci brought to our attention a paper by M. Hamano and M. Okada [11] where a very similar principle is derived from a restricted version of the much stronger *Buchholz hydra battle* principle [8]. The authors call it *one-dimentional version* of Buchholz hydra battle and also establish its intertranslatability with the usual Hydra battle. This might indicate some (as yet unclear) relationships between the provability algebraic approach and the much stronger systems of ordinal notations.

We tried to make the present paper possibly self-contained. So, we reproduce main ingredients of the graded provability algebra approach at the beginning of the paper. There is essentially only one result — the reduction property of graded provability algebras — for the proof of which we refer the reader to [6, 5]. The results of this paper were presented in tutorial lectures at the European Logic Colloquium in Münster, Germany, August 2002.

2 The Worm principle

The game deals with objects called *worms*. A worm is a just a finite function $f : [0, n] \to \mathbb{N}$. Worms can be specified as lists of natural numbers $w = (f(0), f(1), \dots, f(n))$. For example, $w = 2102031$ is a worm (where we omit commas assuming all elements are <10). $f(n)$ is called the *head* of the worm. The empty worm is denoted by $\varnothing$.

Now we describe the rules of the game. Informally, the battle starts with an arbitrary worm and at each step the head of the worm is being affected so that it decreases by 1. In response the worm grows according to the two simple rules below. Unlike the original Hydra battle, the Worm battle is fully deterministic.

Formally, we specify a function $\mathrm{next}(w, m)$, where $w = (f(0), f(1), \dots, f(n))$ is a worm and m is a step of the game:

1. If $f(n) = 0$ then $\mathrm{next}(w, m) := (f(0), \dots, f(n-1))$. In this case the head of the worm is cut away.

2. If $f(n) > 0$ let $k := \max_{i<n} f(i) < f(n)$.

   The worm w (with the head decreased by 1) is then the concatenation of two parts, the *good*[2] part $r := (f(0), \dots, f(k))$, and the *bad* part $s := (f(k+1), \dots, f(n-1), f(n)-1)$. We define

$$\text{next}(w, m) := r * \underbrace{s * s * \cdots * s}_{m+1 \text{ times}}.$$

Now let $w_0 := w$ and $w_{n+1} := \text{next}(w_n, n+1)$.

As a typical example consider the worm $w = 2102031$ depicted in Figure 1. At the first step we obtain $k = 4$; $r = 21020$; $s = 30$; $\text{next}(w, 1) = 210203030$. Then the game proceeds as follows:

$$\begin{aligned}
w_0 &= 2102031 \\
w_1 &= 210203030 \\
w_2 &= 21020303 \\
w_3 &= 21020302222 \\
w_4 &= 2102030222122212221222212221 \\
w_5 &= 2102030(22212221222122212220)^6 \\
&\dots
\end{aligned}$$

Notice that w_n is defined by primitive recursion. In fact, w_n is an elementary function of n and (the code of) w. This can be seen from the estimate

$$|w_n| \leq (n+2)! \cdot |w_0|$$

showing that the length of a worm grows only elementarily in the course of the game. Also notice that the maximal size of the elements of the worm can only decrease. This allows to write out a Δ_0-formula in three variables stating $w_n = u$.

The intended true PA-unprovable principle asserts that **E**very **W**orm eventually **D**ies:

$$\mathsf{EWD} :\Leftrightarrow \forall w \exists n\, w_n = \varnothing.$$

Theorem 1 EWD *is true but unprovable in* PA. *In fact,* EWD *is equivalent to 1-consistency of* PA *within* EA.

The notion of 1-consistency is introduced in the next section.

[2] This part can also be empty.

3 n-Provability and n-consistency

As our basic fragment of arithmetic we take *elementary arithmetic* EA. The precise formulation of EA is not important, for definiteness we specify the language of EA as that of Peano arithmetic augmented by a symbol exp for the function 2^x and a symbol $\leq$. Δ_0-formulas in the language of EA are those with all quantifier occurrences bounded by terms. Π_n- and Σ_n-formulas are obtained from Δ_0 by adding a quantifier prefix in the standard way. Axioms of EA consist of some minimal set of open defining axioms for all the symbols of the language and the induction schema for Δ_0-formulas. Peano arithmetic PA can be obtained from EA by adding the full induction schema. We shall also use an extension of EA by an axiom stating that the superexponentiation function $\lambda x. \exp^{(x)}(x)$ is total, denoted EA^+. EA and EA^+ are finitely axiomatizable fragments of primitive recursive arithmetic PRA.

Let $Th_{\Pi_n}(\mathbb{N})$ denote the set of all true arithmetical Π_n-sentences. A theory T is called *n-consistent* if $T + Th_{\Pi_n}(\mathbb{N})$ is consistent. Let $n\text{-}\mathsf{Con}(T)$ be the natural Π_{n+1}-formula expressing the n-consistency of T. $\langle n\rangle_T\varphi$ stands for $n\text{-}\mathsf{Con}(T+\varphi)$. These formulas are uniquely defined as soon as T is an *elementary presented* theory, that is, equipped with a Δ_0-formula defining the set of Gödel numbers of its axioms. In the following we shall always tacitly assume T to be elementary presented.

The formula $[n]_T\varphi := \neg\langle n\rangle_T\neg\varphi$ formalizes the *n-provability* of φ in T. Thus, $[n]_T\varphi$ asserts that φ is provable from the axioms of T and some true Π_n-sentences. For $n = 0$ these concepts coincide with the usual Gödel's consistency assertion and provability predicate for T. We also write $\Box$ for $[0]$ and $\Diamond$ for $\langle 0\rangle$.

Properties of the n-provability are very similar to those of the usual provability predicate. First of all, the n-provability predicate $[n]_T$ satisfies Bernays–Löb derivability conditions.

Proposition 1

(i) $T \vdash \varphi \;\Rightarrow\; \mathsf{EA} \vdash [n]_T\varphi$;

(ii) $\mathsf{EA} \vdash [n]_T(\varphi \to \psi) \to ([n]_T\varphi \to [n]_T\psi)$;

(iii) $\mathsf{EA} \vdash [n]_T\varphi \to [n]_T[n]_T\varphi$.

The last condition is a consequence of a more general fact known as provable Σ_{n+1}-completeness.

Proposition 2 *For any Σ_{n+1}-formula $\sigma(x_1,\dots,x_k)$, with exactly the variables $x_1,\dots,x_k$ free,*

$$\mathsf{EA} \vdash \sigma(x_1,\dots,x_k) \to [n]_T\sigma(\dot{x}_1,\dots,\dot{x}_k).$$

Here $\sigma(\dot{x}_1, \ldots, \dot{x}_k)$ under $[n]_T$ denotes the definable Kalmar elementary term for the function that, given a tuple $n_1, \ldots, n_k$, outputs the code $\ulcorner\sigma(\bar{n}_1, \ldots, \bar{n}_k)\urcorner$ of the result of substitution of the numerals $\bar{n}_1, \ldots, \bar{n}_k$ for variables $x_1, \ldots, x_k$ in σ.

As a standard consequence of the derivability conditions and the arithmetical fixed point lemma we obtain formalized *Löb's Theorem.*

Proposition 3 *For any formula φ,*

$$\mathsf{EA} \vdash [n]_T([n]_T\varphi \to \varphi) \leftrightarrow [n]_T\varphi.$$

Another useful lemma shows that n-consistency assertions are equivalent to the uniform reflection principles for T. Let $\mathsf{RFN}_{\Pi_{n+1}}(T)$ denote the schema

$$\{\forall x(\Box_T\varphi(\dot{x}) \to \varphi(x)) : \varphi \in \Pi_{n+1}\}.$$

Proposition 4 *Over* EA,

$$n\text{-}\mathsf{Con}(T) \iff \mathsf{RFN}_{\Pi_{n+1}}(T).$$

Proof. ($\Rightarrow$) If $\varphi(x) \in \Pi_{n+1}$, then $\neg\varphi(x)$ implies $[n]_T\neg\varphi(\dot{x})$ by Σ_{n+1}-completeness. Therefore $\Box_T\varphi(\dot{x})$ implies $[n]_T(\varphi(\dot{x}) \wedge \neg\varphi(\dot{x}))$, that is, $[n]_T\bot$.

($\Leftarrow$) If $[n]_T\bot$, then for some true $\pi \in \Pi_n$, $\Box_T\neg\pi$ by formalized Deduction theorem. Let $\varphi(x) \in \Pi_n$ be a truth-definition for Π_n-formulas so that EA proves:

$$\text{For each } \psi \in \Pi_n, \quad \mathsf{EA} \vdash \psi \leftrightarrow \varphi(\ulcorner\psi\urcorner).$$

We have $\Box_T\neg\varphi(\ulcorner\pi\urcorner)$ but $\varphi(\ulcorner\pi\urcorner)$. $\boxtimes$

4 Graded provability algebras

Let T be a theory containing EA. Since the formulas $[0]_T, [1]_T, \ldots$ satisfy Bernays–Löb derivability conditions, all of them correctly define operators

$$\varphi \longmapsto [n]_T\varphi$$

acting on the Lindenbaum boolean algebra $\mathcal{B}_T$ of T. (Here and below we freely identify formulas of T and the corresponding elements of $\mathcal{B}_T$.) The enriched structure $\mathcal{M}_T^\infty = (\mathcal{B}_T, [0]_T, [1]_T, \ldots)$ is called the *graded provability algebra of T*.

Terms of this algebra correspond to propositional *polymodal formulas*, that is, the formulas built up from propositional variables and $\bot$, $\top$ by boolean connectives and $[0]_T, [1]_T, \ldots$. The identities of $\mathcal{M}_T^\infty$ are exactly characterized by the following system **GLP** due to G. Japaridze ([2, 7]).

Axioms: (i) Boolean tautologies;

(ii) $[n](\varphi \to \psi) \to ([n]\varphi \to [n]\psi)$;

(iii) $[n]([n]\varphi \to \varphi) \to [n]\varphi$;

(iv) $[m]\varphi \to [n]\varphi$, for $m \leq n$;

(v) $\langle m \rangle \varphi \to [n]\langle m \rangle \varphi$, for $m < n$.

Rules: modus ponens, $\varphi \vdash [n]\varphi$.

This is expressed by the arithmetical completeness theorem for **GLP**.

Proposition 5 (Japaridze) *For any sound theory T containing* EA*,*

$$\mathbf{GLP} \vdash \varphi(\vec{x}) \iff \mathcal{M}_T^\infty \vDash \forall \vec{x}\,(\varphi(\vec{x}) = \top).$$

We note that the soundness ($\Rightarrow$) follows immediately from Propositions 1–3. We will essentially only rely on the soundness part in this paper.

The graded provability algebra of T provides a kind of big, universal structure where all the extensions of T formulated in the arithmetical language 'live in'. Any arithmetical theory extending T is embeddable as a filter into the Lindenbaum algebra of T. In particular, fragments of PA above EA can be viewed as particular filters in $\mathcal{M}_{\mathsf{EA}}^\infty$. However, in order that the machinery of provability algebras be applicable to these theories, the structure $\mathcal{M}_{\mathsf{EA}}^\infty$ has to 'see' these filters, in other words, they have to be, in some sense, nicely definable in the structure $\mathcal{M}_{\mathsf{EA}}^\infty$.

This is what we have to know about PA (see [15, 16]):

Proposition 6 *The following relationships hold provably in* EA*:*

(i) $I\Sigma_n \equiv \mathsf{EA} + \langle n+1 \rangle_{\mathsf{EA}} \top$*, for* $n \geq 1$*;*

(ii) $\mathsf{PA} \equiv \mathsf{EA} + \{\langle n \rangle_{\mathsf{EA}} \top : n < \omega\}$.

When reasoning in provability algebras we shall often confuse extensions of T and filters in $\mathcal{M}_T^\infty$. $U \subseteq_n V$ denotes the Π_{n+1}-conservativity of U over V, i.e., for every $\pi \in \Pi_n$ such that $U \vdash \pi$ we have $V \vdash \pi$. $U \equiv_n V$ means $U \subseteq_n V$ and $V \subseteq_n U$. The same notation is also applied to arbitrary *sets* of elements of $\mathcal{M}_T^\infty$ and means the corresponding relation between theories/filters axiomatized by those sets.

The following crucial property of graded provability algebras is proved in [5, 6].

Proposition 7 (Reduction) *Assume T is a Π_{n+2}-axiomatized theory containing* EA*. Then for all $\varphi \in \mathcal{M}_T^\infty$ the following holds in $\mathcal{M}_T^\infty$ (provably in* EA^+*):*

$$\{\langle n+1 \rangle_T \varphi\} \equiv_n \{Q_k^n(\varphi) : k < \omega\},$$

where

$$Q_0^n(\varphi) = \langle n\rangle_T\varphi,$$
$$Q_{k+1}^n(\varphi) = \langle n\rangle_T(Q_k^n(\varphi)\wedge\varphi).$$

Thus, the filter generated by all Π_{n+1}-consequences of an element $\langle n+1\rangle_T\varphi\in\mathcal{M}_T^\infty$ of complexity Π_{n+2} can be generated by specific Π_{n+1}-elements $Q_k^n(\varphi)$. It is important that these elements are definable by terms in the language of $\mathcal{M}_T^\infty$. We call this property of $\mathcal{M}_T^\infty$ *reduction property.*

We conclude this section with a corollary of the reduction property concerning the n-consistency orderings. The *n-consistency ordering* $<_n$ on $\mathcal{M}_T^\infty$ is defined by

$$\psi <_n \varphi \iff T\vdash\varphi\rightarrow\langle n\rangle_T\psi.$$

Clearly, $<_n$ is transitive and, by Löb's theorem, irreflexive on $\mathcal{M}_T^\infty\setminus\{\bot\}$.

For $\alpha=\langle n+1\rangle_T\varphi$ we define $\alpha[\![k]\!]:=Q_k^n(\varphi)$. The following corollary tells that the limit of the sequence $\alpha[\![k]\!]$ (in the sense of the ordering $<_n$ on $\mathcal{M}_T^\infty$) is α.

Corollary 8 *Assume $\mathcal{M}_T^\infty$ satisfies the reduction property. If $\psi<_n\alpha$, then $\exists k:\psi<_n\alpha[\![k]\!]$. Hence $\alpha[\![0]\!]<_n\alpha[\![1]\!]<_n\ldots\longrightarrow\alpha$.*

Proof. It is obvious that $\alpha[\![k]\!]<_n\alpha[\![k+1]\!]$ for any k. Likewise, a simple induction on k shows $\alpha[\![k]\!]<_n\alpha$, for any k.

Now, if $T\vdash\alpha\rightarrow\langle n\rangle_T\psi$, then by the reduction property $\langle n\rangle_T\psi$ belongs to the filter generated by $\{\alpha[\![k]\!]:k<\omega\}$. Hence, $T\vdash\alpha[\![k]\!]\rightarrow\langle n\rangle_T\psi$, for some k. ⊠

As a word of caution we remark that the sequence $\alpha[\![k]\!]$ is not uniquely determined by the element $\alpha\in\mathcal{M}_T^\infty$. Different choices of φ such that $\alpha=\langle n+1\rangle_T\varphi$ can yield different sequences.

5 An ordinal notation system for ϵ_0

Work in the closed fragment of **GLP**. Recall that by Japaridze's theorem, for any closed modal formula φ,

$$\mathbf{GLP}\vdash\varphi \iff T\vdash\varphi^*, \qquad (*)$$

where φ^* denotes the interpretation of φ in $\mathcal{M}_T^\infty$. This means that the Lindenbaum algebra $\mathcal{M}_0^\infty$ of the closed fragment of **GLP** is canonically embeddable into $\mathcal{M}_T^\infty$, if T is sound. We shall consider a certain substructure of $\mathcal{M}_0^\infty$ as our ordinal notation system for ϵ_0.

Let S be the set of formulas generated from $\top$ by $\langle 0\rangle$, $\langle 1\rangle$, ... An element of S typically has the form

$$\alpha = \langle n_1\rangle\langle n_2\rangle \dots \langle n_k\rangle\top.$$

We identify such elements with words in the alphabet of natural numbers

$$\alpha = n_1 n_2 \dots n_k.$$

The empty word $\varnothing$ is identified with $\top$. S_n denotes the restriction of S to the alphabet $\{n, n+1, \dots\}$.

We define the relation $<_n$ on S in analogy with that on the algebra $\mathcal{M}_T^\infty$:

$$\beta <_n \alpha \iff \mathbf{GLP} \vdash \alpha \to \langle n\rangle\beta.$$

By $(*)$ we have, for sound T,

$$\beta <_n \alpha \iff \mathcal{M}_T^\infty \vDash \beta^* <_n \alpha^*.$$

Proposition 9 *$(S_n, <_n)$ is well-founded of height ϵ_0. Modulo provable equivalence in* **GLP** *the ordering is linear.*

We shall use the elements of S as our codes for the ordinals below ϵ_0. Recall that **GLP** is elementary decidable, so the ordering $(S_n, <_n)$ is elementary decidable, too.

The proof of this theorem is elaborated in [6], but it is not really needed for the treatment of the Worm principle below. To help the reader's intuition we only give the easy correspondence between S and the ordinals below ϵ_0.

Define $o(0^k) = k$. If $\alpha = \alpha_1 0 \alpha_2 0 \cdots 0 \alpha_n$, where all $\alpha_i \in S_1$ and not all of them empty, then

$$o(\alpha) = \omega^{o(\alpha_n^-)} + \cdots + \omega^{o(\alpha_1^-)},$$

where β^- is obtained from $\beta \in S_1$ by replacing every letter $m+1$ by m.

Notice that $o : S \to \epsilon_0$ is obviously onto. Proposition 9 (for the case $n = 0$) can now be more explicitly formulated as follows: For all $\alpha, \beta \in S$,

$$\mathbf{GLP} \vdash \alpha \leftrightarrow \beta \quad \text{iff} \quad o(\alpha) = o(\beta);$$
$$\mathbf{GLP} \vdash \beta \to \Diamond\alpha \quad \text{iff} \quad o(\alpha) < o(\beta).$$

Example 10 $o(2101) = \omega^{o(0)} + \omega^{o(10)} = \omega + \omega^{\omega^0 + \omega^1} = \omega^\omega$. Accordingly, we have

$$\mathbf{GLP} \vdash 2101 \leftrightarrow (21 \wedge 01) \leftrightarrow 21 \leftrightarrow 2.$$

The first equivalence here follows, e.g., from Lemma 11(ii) below.

6 Reading off the fundamental sequences

Reduction property provides the fundamental sequences for certain elements of $\mathcal{M}_T^\infty$. We want to use the same fundamental sequences in our ordinal notation system. We only have to establish that modulo **GLP** the set S is closed under the operation $\alpha \mapsto \alpha[\![n]\!]$.

In [6] it is shown that S is closed under conjunction. $\wedge$ together with the operators $\langle n\rangle$ is sufficient to build the formulas Q_k which describe the fundamental sequences. Here we prefer to take a shortcut which also allows to explicitly calculate the fundamental sequences.

Lemma 11 *Some derivations in* **GLP***:*

(i) If $m < n$, then $\vdash \langle n\rangle\varphi \wedge \langle m\rangle\psi \leftrightarrow \langle n\rangle(\varphi \wedge \langle m\rangle\psi)$;

(ii) If $\alpha \in S_{n+1}$, then $\vdash \alpha \wedge n\beta \leftrightarrow \alpha n\beta$.

(iii) If $m \leq n$, then $\vdash nm\alpha \to m\alpha$.

Proof. Statement (i):

$$\begin{aligned} \mathbf{GLP} \vdash \langle n\rangle\varphi \wedge \langle m\rangle\psi &\to [n]\langle m\rangle\psi \quad \text{by Axiom (v)} \\ &\to \langle n\rangle(\varphi \wedge \langle m\rangle\psi). \end{aligned}$$

Statement (ii) follows by repeated application of (i). Statement (iii) follows from theorem $[m]\varphi \to [m][m]\varphi$ of **GLP**. ⊠

Lemma 12 *(i) If $\alpha = \langle n+1\rangle\gamma$ with $\gamma \in S_{n+1}$, then for all k,*
GLP $\vdash \alpha[\![k]\!] \leftrightarrow (n\gamma)^{k+1}$.

(ii) If $\alpha = \langle n+1\rangle\gamma m\beta$, where $\gamma \in S_{n+1}$ and $m \leq n$, then for any k,
GLP $\vdash \alpha[\![k]\!] \leftrightarrow (n\gamma)^{k+1}m\beta$.

Proof. (i) We argue by induction on k. For $k = 0$ we have $\alpha[\![0]\!] = \langle n\rangle\gamma$. For the induction step we have

$$\begin{aligned} \mathbf{GLP} \vdash \alpha[\![k+1]\!] &\leftrightarrow \langle n\rangle(\gamma \wedge (n\gamma)^{k+1}) \\ &\leftrightarrow \langle n\rangle(\gamma(n\gamma)^{k+1}) \quad \text{by Lemma 11(ii)} \\ &\leftrightarrow (n\gamma)^{k+2}. \end{aligned}$$

(ii) Similarly, for the induction step we have

$$\begin{aligned} \mathbf{GLP} \vdash \alpha[\![k+1]\!] &\leftrightarrow \langle n\rangle(\gamma m\beta \wedge (n\gamma)^{k+1}m\beta) \\ &\leftrightarrow \langle n\rangle(\gamma(m\beta \wedge (n\gamma)^{k+1}m\beta)) \quad \text{by Lemma 11(i)} \\ &\leftrightarrow (n\gamma)^{k+2}m\beta \quad \text{by Lemma 11(iii)}. \end{aligned}$$

⊠

7 Two soundness proofs

In this section we give two proofs of truth of EWD. The first proof is a standard one and is based on ordinal assignments and transfinite induction on ϵ_0 as the only principle that goes beyond EA.

The second proof is more interesting in that it does not use the well-foundedness of ϵ_0. Instead, it relies directly on the 1-consistency assumption for PA and uses the reasoning in graded provability algebras.

7.1 First proof

For any worm w define an element $i(w) \in S$ by writing the word w in the reverse order. Observe that by Lemma 12 we always have $i(\text{next}(w,n)) = i(w)[\![n]\!]$, if w ends with $m > 0$. After all, the definition of $\text{next}(w,n)$ was read off from that of $\alpha[\![n]\!]$ in this way.

Recall the ordinal assignment $o : S \to \epsilon_0$ defined in Section 5. It induces an assignment of ordinals to worms by $o(w) := o(i(w))$.

Let w_n be the worm battle sequence starting from w and let $\alpha_n := i(w_n)$ be the corresponding sequence of elements of S. If w_n ends with 0 we obviously have $o(w_{n+1}) < o(w_n)$. Otherwise we have:

$$o(w_{n+1}) = o(\text{next}(w_n, n+1)) = o(\alpha_n[\![n+1]\!]) < o(\alpha_n) = o(w_n).$$

This proves $o(w_n)$ to be a strictly decreasing sequence of ordinals, which contradicts the well-foundedness of ϵ_0.

Notice that this proof uses Proposition 9 to ensure that $o(\alpha[\![n]\!]) < o(\alpha)$. Alternatively, one can check this directly on the basis of the definition of $o(\alpha)$. We omit the details.

In contrast, our second proof does not rely on ordinals. In a sense, the use of transfinite induction is replaced by the use of Löb's theorem (and the 1-consistency assumption for PA).

7.2 Second proof

We prove $\mathsf{EA}+1\text{-}\mathsf{Con}(\mathsf{PA}) \vdash \mathsf{EWD}$. Now we shall interpret worms as elements of a graded provability algebra.

We work in $\mathcal{M}^{\infty}_{\mathsf{EA}}$. For any $\alpha \in S$ we denote by α^* its arithmetical interpretation in $\mathcal{M}^{\infty}_{\mathsf{EA}}$. Define $w^\star := (i(w)^+)^*$, where α^+ means increasing every element of α by 1.

Thus, for example, $(103)^\star = \langle 4\rangle_{\mathsf{EA}}\langle 1\rangle_{\mathsf{EA}}\langle 2\rangle_{\mathsf{EA}}\top$. In the following reasoning we omit the subscript $_{\mathsf{EA}}$ everywhere without causing confusion.

Lemma 13 *For any w, $\mathsf{PA} \vdash w^\star$.*

Proof. We argue by induction on $|w|$. If $w = vn$ and $m >$ any letter in w, then

$$\begin{aligned} \mathsf{EA} \vdash v^\star \wedge \langle m+1\rangle\top &\rightarrow \langle m+1\rangle v^\star \quad \text{by Lemma 11} \\ &\rightarrow \langle n+1\rangle v^\star. \end{aligned}$$

By Proposition 6 and the induction hypothesis

$$\mathsf{PA} \vdash v^\star \wedge \langle m+1\rangle\top,$$

so $\mathsf{PA} \vdash \langle n+1\rangle v^\star$, which yields the induction step. ⊠

Lemma 14 *For any* w,

$$\mathsf{EA} \vdash \forall n\, (w_n \neq \varnothing \rightarrow \Box(w_n^\star \rightarrow \langle 1\rangle w_{n+1}^\star)).$$

Proof. It is sufficient to prove

$$\forall w \neq \varnothing\ \forall n\ \mathsf{EA} \vdash w^\star \rightarrow \langle 1\rangle \mathrm{next}(w,n)^\star \tag{1}$$

by an argument formalizable in EA.

Let $\alpha = i(w)$. If α begins with 0, the claim is obvious. If α begins with $k+1$, by Lemma 12 $\alpha[\![n]\!] = i(\mathrm{next}(w,n))$. An easy induction on n yields:

$$\forall n\ \mathbf{GLP} \vdash \alpha \rightarrow \Diamond\alpha[\![n]\!].$$

The axioms of $\mathbf{GLP}$ are stable under $(\cdot)^+$, that is, if $\mathbf{GLP} \vdash \varphi$, then $\mathbf{GLP} \vdash \varphi^+$. Hence we obtain

$$\forall n\ \mathbf{GLP} \vdash \alpha^+ \rightarrow \langle 1\rangle\alpha[\![n]\!]^+.$$

This yields (1) by the soundness part of Japaridze's theorem. ⊠

The following argument uses the same idea as Solovay's proof of the fact that there do not exist provably uniformly descending hierarchies of consistency assertions.

Lemma 15 $\mathsf{EA} \vdash \langle 1\rangle w_0^\star \rightarrow \exists n\, w_n = \varnothing$.

Proof. We prove $\forall n\, w_n \neq \varnothing \rightarrow \forall n\, [1]\neg w_n^\star$ relying on Löb's theorem.

$$\begin{aligned} \mathsf{EA} \vdash \forall n\, w_n \neq \varnothing \wedge [1]\forall n[1]\neg w_n^\star &\rightarrow [1]\forall n[1]\neg w_{n+1}^\star \\ &\rightarrow \forall n[1][1]\neg w_{n+1}^\star \\ &\rightarrow \forall n[1]\neg w_n^\star \quad \text{by Lemma 14.} \end{aligned}$$

$$\begin{aligned} \mathsf{EA} \vdash [1]\forall n\, w_n \neq \varnothing &\rightarrow [1]([1]\forall n[1]\neg w_n^\star \rightarrow \forall n[1]\neg w_n^\star) \\ &\rightarrow [1]\forall n[1]\neg w_n^\star \quad \text{by Löb.} \end{aligned}$$

$$
\begin{aligned}
\mathsf{EA} \vdash \forall n\, w_n \neq \varnothing \ &\to\ [1]\forall n\, w_n \neq \varnothing \quad \text{by } \Sigma_2\text{-completeness}\\
&\to\ [1]\forall n [1]\neg w_n^\star\\
&\to\ \forall n[1]\neg w_n^\star\\
&\to\ [1]\neg w_0^\star,
\end{aligned}
$$

as required. ⊠

We conclude the proof of Theorem 1. From Lemmas 13 and 15 we obtain

$$
\begin{aligned}
\mathsf{PA} &\vdash \langle 1\rangle w^\star,\\
\mathsf{EA} &\vdash \langle 1\rangle w^\star \to \exists n\, w_n = \varnothing.
\end{aligned}
$$

Hence, $\forall w\ \mathsf{PA} \vdash \exists n\, w_n = \varnothing$. This proof is formalizable in EA, so 1-$\mathsf{Con}(\mathsf{PA})$ implies $\forall w \exists n\, w_n = \varnothing$ by Σ_1-reflection. ⊠

8 Provably total computable functions

For the independence proof of the Worm principle we need to know a few non-PA-specific facts concerning provably total computable functions. Essentially, we will need Proposition 20 below. The material of this section is mostly folklore. The reader can find some additional details in [4].

Recall that a function $f : \mathbb{N}^k \to \mathbb{N}$ is called *provably total computable in* T, if for some Σ_1-formula $\varphi(\vec{x}, y)$ there holds:

(i) $f(\vec{x}) = y \iff \mathbb{N} \vDash \varphi(\vec{x}, y)$;

(ii) $T \vdash \forall \vec{x} \exists y \varphi(\vec{x}, y)$.

$\mathcal{F}(T)$ denotes the class of all provably total computable functions in T. $\mathcal{F}(\mathsf{EA})$ is known to coincide with the *(Kalmar) elementary functions* $\mathcal{E}$. The class $\mathcal{E}$ is defined as the closure of $0, 1, +, \cdot, 2^x$, projection functions and the characteristic function of $\leq$ by composition and bounded recursion, that is, primitive recursion with the restriction that the resulting function is bounded by some previously generated function. Thus, it is easy to see that any elementary function is bounded by some fixed iterate of 2^x.

For T containing EA, the class $\mathcal{F}(T)$ contains $\mathcal{E}$ and is closed under composition, but generally not under the bounded recursion. Also notice that $\mathcal{F}(T)$ only depends on the set of Π_2-consequences of T. Hence, if T is Π_2-conservative over U, then $\mathcal{F}(T) \subseteq \mathcal{F}(U)$.

For many natural theories T the classes $\mathcal{F}(T)$ have been characterized recursion-theoretically. For example, by a well-known result of C. Parsons [17] and independently of G. Mints [1], $\mathcal{F}(I\Sigma_1)$ coincides with the class of primitive recursive functions. On the other hand, already W. Ackermann [3] and G. Kreisel [13] established that the class $\mathcal{F}(\mathsf{PA})$ coincides with the class of $<\epsilon_0$-recursive functions. Later some other characterizations of this class have been obtained. In particular, H. Schwichtenberg and S. Wainer (see [18, 9]) characterized $\mathcal{F}(\mathsf{PA})$ by a hierarchy of functions very close to those introduced below.

The notion of provably total computable function is tightly related to that of 1-consistency. In order to explain this relationship we consider the corresponding *programs*, or *indices* of such functions. Fix some natural coding of Turing machines and a Σ_1-formula $\varphi_e(x) = y$ expressing the statement that the Turing machine coded by e on input x halts and outputs y. Usually, one represents φ using Kleene's T-predicate as follows:

$$\varphi_e(x) = y \leftrightarrow \exists z\, (\mathsf{T}(e, x, z) \wedge \mathsf{U}(z) = y),$$

where formula $\mathsf{T} \in \Delta_0$ and the function U is elementary. Recall that $\mathsf{T}(e, x, z)$ expresses that z is a full protocol of a terminating computation of the machine e on input x.

Definition 16 Let T be an elementary presented theory. A number e is a *T-index*, if $e = \langle e_1, e_2\rangle$ where

- e_1 codes a Turing machine;
- e_2 codes a T-proof of $\forall x \exists y \varphi_{e_1}(x) = y$.

With this indexing of provably total computable functions a universal function ψ^T is associated:

$$\psi^T_e(x) := \begin{cases} \varphi_{e_1}(x), & \text{if } e = \langle e_1, e_2\rangle \text{ is a } T\text{-index;} \\ 0, & \text{otherwise.} \end{cases}$$

The usual diagonalization argument shows that ψ^T, as a function of arguments e and x, does not belong to $\mathcal{F}(T)$. Therefore, the statement of its totality delivers an independent principle for T.

Lemma 17 $\mathsf{EA} \vdash \forall e, x \exists y\, \psi_e(x) = y \leftrightarrow \mathsf{RFN}_{\Pi_2}(T)$.

Proof. The totality of ψ is expressed by the formula:

$$\forall e_1, e_2, x\, (\mathsf{Prf}_T(e_2, \ulcorner \forall x \exists y \varphi_{\dot{e}_1}(x) = y \urcorner) \rightarrow \exists y \varphi_{e_1}(x) = y). \qquad (2)$$

Any Π_2-sentence is equivalent to the one of the form $\forall x \exists y \varphi_{\bar{e}_1}(x) = y$ for a suitable index e_1, so (2) is equivalent to $\mathsf{RFN}_{\Pi_2}(T)$. ⊠

If $f(\vec{x})$ is a function whose graph is definable, let $f\!\downarrow$ denote the formula $\forall \vec{x}\, \exists y f(\vec{x}) = y$. The following basic result almost immediately follows from the Herbrand theorem (cf. [4] for details).

Proposition 18 *Suppose the graph of f is elementary. Then $g \in \mathcal{F}(\mathsf{EA} + f\!\downarrow)$ iff g can be obtained from elementary functions and f by composition.*

We denote by $\mathbf{C}(f)$ the closure of $\mathcal{E} \cup \{f\}$ under composition. We can define the *jump* $\mathcal{F}(T)'$ of the class of provably total computable functions of T as $\mathbf{C}(\psi^T)$. From Lemma 17 we now obtain

Corollary 19 *If T is a Σ_1-sound theory, then $\mathcal{F}(\mathsf{EA} + \langle 1 \rangle_T \top) = \mathcal{F}(T)'$.*

Proof. The graph of ψ^T is not elementary. Consider the function $\tilde{\psi}^T$ such that $\tilde{\psi}^T_e(x)$ encodes the full protocol of the computation of $\psi_e(x)$, in other words

$$\tilde{\psi}^T_e(x) := \begin{cases} \mu z.\mathsf{T}(e_1, x, z), & \text{if } e = \langle e_1, e_2 \rangle \text{ is a } T\text{-index;} \\ 0, & \text{otherwise.} \end{cases}$$

It is easy to see that $\tilde{\psi}^T$ has an elementary graph, $\mathbf{C}(\psi^T) = \mathbf{C}(\tilde{\psi}^T)$ and

$$\mathsf{EA} \vdash \tilde{\psi}^T\!\downarrow \leftrightarrow \psi^T\!\downarrow.$$

Now apply Proposition 18 to $f = \tilde{\psi}^T$. ⊠

Proposition 18 leads to an alternative 'proofs-free' indexing of functions in $\mathcal{F}(T)$ for $T = \mathsf{EA} + f\!\downarrow$. Terms composed of elementary functions and a function symbol f have a natural Gödel numbering. These numbers can be considered as codes of provably total functions. So, with this Gödel numbering we can associate another universal function $\theta^T_e(x)$ that computes the value of the term with index e on x:

$$\theta^T_e(x) := \begin{cases} t[f, x], & \text{if } e = \ulcorner t \urcorner; \\ 0, & \text{otherwise.} \end{cases}$$

The two kinds of indexing are equivalent provably in EA^+, because the Herbrand theorem is verifiable in EA^+ and allows to extract an explicit term from a proof of totality of a computable function. The converse is also true: for any $\mathbf{C}(f)$-term t one can elementarily construct a Kleene index e_1 of the function $\lambda x.t[f, x]$ and a T-proof e_2 of its totality.

Lemma 20 *Suppose f has an elementary graph and*

(i) $\mathsf{EA} \vdash \forall x \; f(x) > 2^x$*;*

(ii) $\mathsf{EA} \vdash \forall x, y \, (x \leq y \to f(x) \leq f(y))$.

Then $\mathsf{EA} \vdash \lambda x.f^{(x)}(x)\!\downarrow \leftrightarrow \langle 1 \rangle_{\mathsf{EA}} f\!\downarrow$.

Here and below we assume that the Δ_0-definition of the graph of $\lambda x.f^{(x)}(x)$ is constructed from the Δ_0-definition of the graph of f in a natural way. (Using provable monotonicity of f this is easy.)

Proof. Let $T := \mathsf{EA} + f\!\downarrow$. By Lemma 17, $\langle 1 \rangle_{\mathsf{EA}} f\!\downarrow$ is EA-equivalent to $\psi^T\!\downarrow$. The formula $\psi^T\!\downarrow$, in particular, implies EA^+ and hence $\theta^T\!\downarrow$. Vice versa, $\theta^T\!\downarrow$

also implies EA^+ and hence $\psi^T\!\downarrow$. So, it is sufficient to show that $\lambda x.f^{(x)}(x)\!\downarrow$ is equivalent to the totality of θ^T.

Clearly, if θ is total, then for every k the function $f^{(k)}$ is also total. Indeed, $f^{(k)} \in \mathbf{C}(f)$ and the Gödel number of $f^{(k)}$ is obtained elementarily from k. We can evaluate it using θ, so $\lambda x.f^{(x)}(x)$ is total.

In the other direction, we use the monotonicity of f. Under the given assumptions, every term $g \in \mathbf{C}(f)$ can be majorized by a fixed iterate of the function f:

$$\mathsf{EA} \vdash \forall x\ (g(x) \leq f^{(k)}(x)).$$

The number k can be computed elementarily from the Gödel number of g, say, by a function $j(e)$.

Assume $\lambda x.f^{(x)}(x)$ is total. To show that, for any e and x, the value $\theta^T_e(x)$ is defined, consider the value $f^{(j(e))}(x)$. This value is smaller than $f^{(z)}(z)$, where $z := \max(j(e), x)$, hence it is defined. Therefore, the yet smaller value $\theta^T_e(x)$ is also defined. ⊠

Example 21 The classes $\mathcal{E} \subseteq \mathcal{E}' \subseteq \mathcal{E}'' \subseteq \dots$ form the so-called *Grzegorczyk hierarchy* [10]. It is well-known that the union of this hierarchy coincides with the class of primitive recursive functions (see also [18]). From the previous proposition we conclude that the class $\mathcal{E}^{(n)}$ coincides with $\mathbf{C}(F_n)$, where

$$F_0(x) := 2^x + 1; \quad F_{n+1}(x) := F_n^{(x)}(x).$$

The functions F_n are all primitive recursive and their graphs are elementary definable. The extension of EA by the axioms $F_n\!\downarrow$ for all $n \geq 1$ is an alternative axiomatization of the *primitive recursive arithmetic* PRA.

Define $T^n_\omega := T + \{\langle n\rangle^k_T\top : k < \omega\}$. Repeated application of Lemma 20 yields the following well-known fact.

Proposition 22 *(i)* $\mathsf{EA}^1_\omega \equiv \mathsf{PRA}$.

(ii) $\mathcal{F}(\mathsf{EA}^1_\omega)$ *is the class of primitive recursive functions.*

9 Independence of the Worm principle

In this section we let $w[\![n]\!] := \mathrm{next}(w, n)$ and

$$w[\![n \dots n+k]\!] := w[\![n]\!][\![n+1]\!]\dots[\![n+k]\!].$$

We introduce an analogue of the Hardy functions as follows. Let $h_w(n)$ be the smallest k such that $w[\![n \dots n+k]\!] = \varnothing$.

We need some nice properties of h established within EA. We notice that the function

$$W(w, n, k) := w[\![n \dots n+k]\!]$$

is elementary, because it can be defined by bounded recursion on k, similarly to the worm sequence w_n. This gives a natural elementary representation of the relation $h_w(n) = k$ in EA.

The following notion will be used to establish the monotonicity of the h functions. Let $v \trianglelefteq u$ iff $v = u[\![0]\!][\![0]\!]\dots[\![0]\!]$. This essentially means that v is an initial segment of u except possibly for the last letter, which should be not larger than the corresponding letter in u.

Lemma 23 *If $h_w(m)$ is defined and $u \trianglelefteq w$, then*

$$\exists k\ w[\![m \dots m+k]\!] = u.$$

Proof. The n-th letter in w can only change if all letters to the right of it are deleted. So, if w rewrites to $\varnothing$, it cannot possibly miss the u state. ⊠

Here and below the assumption *'$h_w(n)$ is defined'* is needed to formalize the argument inside EA, because EA may not be able to verify that h_w is a total function. In the standard model of arithmetic this assumption is, of course, superfluous, as we know that EWD is true.

Corollary 24 *If $h_w(n)$ is defined, then $\forall m \leq n\, \exists k\ w[\![n \dots n+k]\!] = w[\![m]\!]$.*

Lemma 25 *If $v \trianglelefteq u$ and $x \leq y$ then $h_v(x) \leq h_u(y)$.*

Proof. Repeating Corollary 24 obtain $s_0, s_1, \dots$ such that

$$\begin{array}{rcl} u[\![y \dots y+s_0]\!] & = & v[\![x]\!] \\ u[\![y \dots y+s_0+s_1]\!] & = & v[\![x]\!][\![x+1]\!] \\ & \dots & \end{array}$$

Therefore, all the steps of the rewrite sequence for v occur in the rewrite sequence for u. ⊠

Lemma 26 $h_{u0v}(n) = h_u(n + h_v(n) + 2) + h_v(n) + 1 > h_u(h_v(n))$.

Proof. Nothing can happen to the 0 between u and v until the v part is eliminated. So, the worm $u0v$ first rewrites to $u0$ in $h_v(n)$ steps and then to $\varnothing$. ⊠

Corollary 27 *If $w \in S_1$, then $h_{w1}(n) > h_w^{(n)}(n)$.*

Proof. Observe that $w1[\![n]\!] = w0w0\dots w0$. ⊠

Now we can formulate the main lemma. As usual, $h_w\!\downarrow$ denotes the formula $\forall x \exists y\, h_w(x) = y$. We also let $w^* := \alpha^*$, where $\alpha = i(w)$.

Lemma 28 $\mathsf{EA} \vdash \forall w \in S_1\ (h_{1111w}\!\downarrow \to \langle 1 \rangle w^*)$.

Using this lemma we can easily give

Proof of the independence of EWD:

$$\begin{array}{rcl} \mathsf{EA} \vdash \forall w \exists n\, w_n = \varnothing & \to & \forall w \in S_1\, h_w{\downarrow} \\ & \to & \forall n\, \langle 1 \rangle \langle n \rangle \top \\ & \to & 1\text{-}\mathsf{Con}(\mathsf{PA}). \end{array}$$

Here, there first implication holds, because for every worm w and a number x we can find another worm $w' := w0^x$ such that $w'[\![0 \dots x-1]\!] = w$. So, w' dies iff $h_w(x)$ is defined.

The third implication holds by the formalization of Proposition 6. ⊠

Remark 29 In the proof below we essentially use Proposition 20. Notice that by Corollary 27 we have $h_{111}(x) > 2^x$, therefore the same inequality holds for the function $h_{111w}(x)$, where w is any worm. This is the only reason why we inserted 1111 in front of w in the formulation of the main lemma. In fact, a somewhat sharper statement is obtained if one defines

$$w" := \begin{cases} w, & \text{if } w \text{ begins with } m > 1; \\ 1111w, & \text{otherwise.} \end{cases}$$

Then one can prove in EA that $\forall w \in S_1\, (h_{w"}{\downarrow} \to \langle 1 \rangle w^*)$.

Proof of Lemma 28. By Löb we can use as an additional assumption

$$A := \forall w \in S_1\, \Box (h_{1111w}{\downarrow} \to \langle 1 \rangle w^*).$$

Indeed, if we prove that $\mathsf{EA} \vdash A \to \forall w \in S_1\, (h_{1111w}{\downarrow} \to \langle 1 \rangle w^*)$, then by Löb's theorem the statement of the lemma will also be provable in EA.

The proof relies on the reduction property of $\mathcal{M}^\infty_{\mathsf{EA}}$. More precisely, we shall use the following corollary.

Corollary 30 *Suppose $\alpha \in S_1$ begins with $m > 1$. Then*

$$\mathsf{EA}^+ \vdash \langle 1 \rangle \alpha^* \leftrightarrow \forall n \langle 1 \rangle \alpha[\![n]\!]^*.$$

Proof. In $\mathcal{M}^\infty_{\mathsf{EA}}$, by the reduction property, $\alpha^* \equiv_1 \{\alpha[\![n]\!]^* : n < \omega\}$. Therefore, formalizably in EA^+, α^* proves a false Σ_1-sentence iff $\alpha[\![n]\!]^*$ does, for some n. The contraposition of this yields the statement of the corollary. ⊠

To prove Lemma 28 we reason in EA and consider two cases according to the last symbol in $1111w$.

If $1111w = v1$, then $h_{v1}{\downarrow}$ implies $\lambda x. h_v^{(x)}(x){\downarrow}$, by Lemma 27.

The function h_v is increasing, has an elementary graph and grows at least exponentially. So, if $w = \varnothing$, the claim is obvious: $h_{1111}{\downarrow}$ implies the totality of superexponentiation and hence $\langle 1\rangle\top$. If w is nonempty, $v = 1111v_0$ and we reason as follows:

$$\begin{array}{rcll} \lambda x.h_v^{(x)}(x)\downarrow & \to & \langle 1\rangle h_v\downarrow & \text{by Proposition 20} \\ & \to & \langle 1\rangle\langle 1\rangle v_0^* & \text{by the assumption } A \\ & \to & \langle 1\rangle w^*. & \end{array}$$

If $1111w = v$ ends with $m > 1$, then $v[\![n]\!] = 1111(w[\![n]\!])$. We have

$$\begin{array}{rcl} h_v\downarrow & \to & \lambda x.h_{v[\![x]\!]}(x+1)\downarrow \\ & \to & \forall n\, h_{v[\![n]\!]}\downarrow. \end{array}$$

Argument: Consider any n and x. We have to show that $h_{v[\![n]\!]}(x)$ is defined. If $x \leq n$, then $h_{v[\![n]\!]}(x) \leq h_{v[\![n]\!]}(n+1)$. If $x \geq n$, then $h_{v[\![n]\!]}(x) \leq h_{v[\![x]\!]}(x+1)$. In both cases we know that the larger value is defined.

Further we obtain

$$\begin{array}{rcll} \forall n\, h_{v[\![n+1]\!]}\downarrow & \to & \forall n\, h_{v[\![n]\!]1}\downarrow & \text{as } v[\![n]\!]1 \trianglelefteq v[\![n+1]\!] \\ & \to & \forall n\, \langle 1\rangle h_{v[\![n]\!]}\downarrow & \text{as before} \\ & \to & \forall n\, \langle 1\rangle\langle 1\rangle w[\![n]\!]^* & \text{by } A \\ & \to & \forall n\, \langle 1\rangle w[\![n]\!]^* & \text{by } \Sigma_2\text{-completeness} \\ & \to & \langle 1\rangle w^* \text{ by Corollary 30.} & \end{array}$$

This ends the proof of Lemma 28 and Theorem 1. ⊠

From Lemma 28 we also obtain that the growth rate of the provably total computable functions of PA is bounded by the functions h_n, where n are just the single letter worms. (This, in a somewhat different manner, also implies the independence of the Worm principle.)

Theorem 2 *If $f \in \mathcal{F}(\mathsf{PA})$ then for some n and almost all x, $f(x) \leq h_n(x)$.*

Proof. First of all, we prove that

$$\mathsf{PA} \equiv_1 \mathsf{EA} + \{\langle 1\rangle_{\mathsf{EA}}\langle n\rangle_{\mathsf{EA}}\top : n < \omega\}.$$

The inclusion $\supseteq$ follows from Lemma 13. For the opposite inclusion assume $\mathsf{PA} \vdash \pi$ with $\pi \in \Pi_2$. Then for some n we have $\mathsf{EA} + \langle n\rangle_{\mathsf{EA}}\top \vdash \pi$. Hence,

$$\begin{array}{rcll} \mathsf{EA} \vdash \langle 1\rangle_{\mathsf{EA}}\langle n\rangle_{\mathsf{EA}}\top & \to & \langle 1\rangle_{\mathsf{EA}}\pi & \\ & \to & \pi, & \text{by } \Sigma_2\text{-completeness.} \end{array}$$

This proves the claim. We conclude that if $f \in \mathcal{F}(\mathsf{PA})$ then

$$\mathsf{EA} + \langle 1\rangle_{\mathsf{EA}}\langle n\rangle_{\mathsf{EA}}\top \vdash f\downarrow,$$

for some n. By Lemma 28 it follows that

$$\mathsf{EA} + h_{1111n}{\downarrow} \vdash f{\downarrow}.$$

Lemma 18 now implies that f can be obtained by composition from elementary functions and h_{1111n}. Hence, by monotonicity, it is majorized by a fixed iterate of h_{1111n}, ergo by h_{1111n1} for almost all x.

Using a sharper version of Lemma 28 (see Remark 29) we can in the same way conclude that f is majorized by h_{n1} for almost all x, assuming $n > 1$. By Lemma 25 one also estimates $h_{n1}(x)$ by $h_{n+1}(x)$ from above. ⊠

10 Comparing ordinal notation systems

It is interesting to compare the ordinal notation system for ϵ_0 studied in this paper and [6] with the standard one based on Cantor normal forms. Are they essentially the same?

An answer to this question is a matter of degree of precision. From a sufficiently general point of view they are equivalent. Certainly, the order relations are EA-provably elementary isomorphic.

However, in the proof-theoretic literature starting perhaps from [14] it has been argued that natural systems of ordinal notation should be perceived as orderings equipped with some additional operations. For the standard ordinal notation system one considers the operations $(0, +, \omega^x)$ as basic.[3] These operations are sufficient to generate all ordinal notations up to ϵ_0 as closed terms.

The ordinal notation system considered here can also be perceived as an ordered structure together with some additional operations. This is a many-one notation system, as different (**GLP**-equivalent) words from S can denote the same ordinal. It is possible to restrict the attention to the words in normal form (see [6]). Then one obtains a one-one ordinal notation system.

The operations come from the graded provability algebra and are essentially $\top$ (interpreted as 0) and $\langle n \rangle$, for each n. An additional operation that was used is conjunction $\wedge$. It is not, strictly speaking, needed to generate all necessary ordinal notations, but it is a natural operation of the Lindenbaum algebra and was useful in constructing the fundamental sequences. We notice that all these operations respect **GLP**-equivalence, so they correctly define operations on ordinals (not just on their representations).

Let us examine how to express the operations of the two ordinal notation systems in terms of one another. The ordinal sum can be expressed as follows: for $\alpha, \beta \in S$,

$$\alpha + \beta = \begin{cases} \beta\alpha, & \exists k\, \beta = 0^k \\ \beta 0 \alpha, & \forall k\, \beta \neq 0^k. \end{cases}$$

[3]Sometimes one also adds ordinal multiplication and/or suitable inverse operations to the basic list. Sometimes one also considers the single basic function $x + \omega^y$.

The function ω^x corresponds to α^+ if $o(\alpha) = x$. Thus, the function $x + \omega^y$ is nicely expressible by $\alpha^+ 0\beta$, if $o(\alpha) = y$ and $o(\beta) = x$.

However, notice that $(\cdot)^+$ is, officially, not an operation of the structure. It is also easily seen that it is not expressible by any particular term. For that matter, the same problem is with $+$, because a function of two arguments cannot be expressed as a composition of unary functions. (Concatenation is *not* an operation of the structure!)

The opposite translation is also not quite straightforward. We have $o(\langle 0\rangle\alpha) = o(\alpha) + 1$. However, for $n > 0$ the expressions become more complicated, e.g., if $o(\alpha) = \omega^{\alpha_k} \cdot n_k + \cdots + \omega^{\alpha_0} \cdot n_0$ in Cantor normal form, then

$$o(\langle 1\rangle\alpha) = \omega^{\alpha_k} \cdot n_k + \cdots + \omega^{\alpha_1} \cdot n_1 + \omega^{\alpha_0 + 1}. \tag{3}$$

(The latter expression is not in Cantor normal form in case $\alpha_1 = \alpha_0 + 1$.) The operation $\langle 2\rangle$ works similarly but on the 'second floor' of the Cantor normal form expression, that is, in this case on the normal form of the ordinal α_0:

$$o(\langle 2\rangle\alpha) = \omega^{\alpha_k} \cdot n_k + \cdots + \omega^{\alpha_1} \cdot n_1 + \omega^{\langle 1\rangle(\alpha_0)},$$

where the operation $\langle 1\rangle$ on ordinals is computed by the right hand side of (3). The effect of $\langle n\rangle$ for $n > 2$ can be calculated similarly.

Conjunction $\wedge$ considered as an operation on ordinals is a bit puzzling. Of course, this operation satisfies all the identities of $\wedge$: it is symmetric, associative, idempotent. However, $x \wedge y$ does not always equal $\max(x, y)$, as one naturally expects. E.g.,

$$\omega \wedge (\omega + 1) = o(1 \wedge 01) = o(101) = \omega + \omega.$$

By Corollary 10 from [6] we know that, if both α and β are words from S_n and begin with n, then one of α and β implies the other. This means that in this case, indeed, $o(\alpha \wedge \beta) = \max(o(\alpha), o(\beta))$. We do not have a very nice expression for $o(\alpha) \wedge o(\beta)$, in general. There is a simple recursive algorithm of calculating it with Cantor normal forms, though (see Lemma 11 in [6]).

Now we consider fundamental sequences. It turns out that the fundamental sequences $\alpha[\![n]\!]$ used in this paper are almost the same as those for the standard system of ordinal notation, which may even be a bit surprising taking into account all the differences discussed above. This was observed by A. Weiermann, G. Lee and L. Carlucci.

Let $\alpha = \alpha_0 0 \ldots 0\alpha_k$ with all $\alpha_i \in S_1$ and $o(\alpha) = \omega^{o(\alpha_k)} + \cdots + \omega^{o(\alpha_0)}$ in Cantor normal form. $o(\alpha)$ being a limit ordinal means that the word α_0 is not empty, hence $\alpha_0 = \langle m+1\rangle\beta$ for some $\beta \in S_1$. By Lemma 12 the sequence $\alpha[\![n]\!]$ can be computed according to the two cases below.

(a) $m = 0$. Then $\alpha[\![n]\!] = (0\beta)^{n+1} 0\alpha_1 0 \cdots 0\alpha_k$, because $\beta \in S_1$ and is followed by 0 in α.

(b) $m > 0$. Then $\alpha[\![n]\!] = \alpha_0' 0 \alpha_1 0 \cdots 0 \alpha_k$, where $\alpha_0' = \alpha_0[\![n]\!] = ((m\beta^-)[\![n]\!])^+$. The latter equality holds because from Lemma 12 one immediately concludes that $\gamma^+[\![n]\!] = \gamma[\![n]\!]^+$ whenever γ begins with $m > 0$ and it makes sense to speak about $\gamma[\![n]\!]$.

This means that the fundamental sequence for an ordinal $\alpha = \omega^{\alpha_k} + \cdots + \omega^{\alpha_0}$ in Cantor normal form is as follows:

$$\alpha[\![n]\!] = \begin{cases} \omega^{\alpha_k} + \cdots + \omega^{\alpha_1} + \omega^{\beta} \cdot (n+1) + 1, & \text{if } \alpha_0 = \beta + 1; \\ \omega^{\alpha_k} + \cdots + \omega^{\alpha_1} + \omega^{\alpha_0[\![n]\!]}, & \text{if } \alpha_0 \text{ is a limit ordinal.} \end{cases}$$

So, the only difference with the standard fundamental sequences is the second "+1" in the first case.

There is a well-known exact correspondence between the standard fundamental sequences and a particular strategy for Hercules in his battle with Hydra: always chop off the rightmost head. This provides an immediate relationship between the Worms and Hydras.

Essentially, the Worm battle is slightly longer because it costs the Hercules additional steps each time to eliminate an extra new head of the Hydra sprouting from the grandfather of the head that has been cut away (this corresponds to the extra "+1"). But we can also estimate the worm function by the hydra function from above.

Let $\alpha[n]$ denote the standard fundamental sequences assignment and let $h'_\alpha(n)$ denote the minimal k such that $\alpha[n \dots n+k] = \varnothing$. This essentially measures the length of the Hydra battle for the hydra associated with α. As before, $h_\alpha(n)$ stands for $h_w(n)$ where w is the unique worm in normal form corresponding to the ordinal $\alpha < \epsilon_0$.

Lemma 31 *For all ordinals α, for all n, $h_\alpha(n) \leq h'_\alpha(n+1)$.*

Proof. First of all, observe that $\alpha[\![n]\!] \trianglelefteq \alpha[n+1]$, for any limit ordinal α. Here, the relation $\trianglelefteq$ on ordinals is induced by the corresponding relation on worms. This relationship is clear from the clauses (a) and (b) above.

To prove the lemma one argues by transfinite induction on α: $h_\alpha(n) = h_{\alpha[\![n]\!]}(n+1) \leq h_{\alpha[n+1]}(n+1)$ by Lemma 25. Then $h_{\alpha[n+1]}(n+1) \leq h'_{\alpha[n+1]}(n+2) = h'_\alpha(n+1)$, by the induction hypothesis. ⊠

Therefore, by Theorem 2 the functions $h'_\alpha(n)$ majorize all provably total computable functions of PA which also implies the independence of the Hydra battle principle.

11 Acknowledgements

We thank A. Weiermann, G. Lee, L. Carlucci and A. Visser for various helpful remarks and comments.

References

[1] Г. Е. Минц. Бескванторные и однокванторные системы. *Записки научных семинаров ЛОМИ*, 20:115–133, 1971. English translation: G. Minc. Quantifier-free and one-quantifier systems. *Journal of Soviet Math.* 1, No.1, 71–84 (1973).

[2] Г.К. Джапаридзе. Полимодальная логика доказуемости. In *Интенсиональные логики и логическая структура научных теорий. Тезисы докладов IV Советско-финского коллоквиума по логике, Телави, 20–24 мая 1985 г.*, pages 16–48. Мецниереба, Тбилиси, 1988.

[3] W. Ackermann. Zur Wiederspruchsfreiheit der reinen Zahlentheorie. *Math. Ann.*, 117:162–194, 1940.

[4] L.D. Beklemishev. Induction rules, reflection principles, and provably recursive functions. *Annals of Pure and Applied Logic*, 85:193–242, 1997.

[5] L.D. Beklemishev. Proof-theoretic analysis by iterated reflection. Preprint, `http://wwwmath.uni-muenster.de/logik/publ/pre/6.html`. To appear in Archive for Mathematical Logic, 1999.

[6] L.D. Beklemishev. Provability algebras and proof-theoretic ordinals, I. Logic Group Preprint Series 208, University of Utrecht, March 2001. `http://preprints.phil.uu.nl/lgps/`.

[7] G. Boolos. *The Logic of Provability.* Cambridge University Press, Cambridge, 1993.

[8] W. Buchholz. An independence result for Π^1_1-CA + BI. *Annals of Pure and Applied Logic*, 33:131–155, 1987.

[9] W. Buchholz and S. Wainer. Provably computable functions and the fast growing hierarchy. In *Contemporary Math. 65*, pages 179–198, 1987.

[10] A. Grzegorczyk. Some classes of recursive functions. *Rozprawy Matematiczne*, 4:1–46, 1953. Russian translation: Классы вычислимых функций. *Проблемы мат. логики и сложность алгоритмов*, с. 9–49, 1970.

[11] M. Hamano and M. Okada. A relationship among Gentzen's proof-reduction, Kirbi-Paris' Hydra game, and Buchholz's Hydra game. *Mathematical Logic Quarterly*, 43(1):103–120, 1997.

[12] L.A.S. Kirby and J.B. Paris. Accessible independence results for Peano arithmetic. *Bull. London Math. Soc.*, 14:285–293, 1982.

[13] G. Kreisel. On the interpretation of non-finitist proofs, II. *The Journal of Symbolic Logic*, 17:43–58, 1952.

[14] G. Kreisel. Wie die Beweistheorie zu ihren Ordinalzahlen kam und kommt. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 78(4):177–223, 1977.

[15] G. Kreisel and A. Lévy. Reflection principles and their use for establishing the complexity of axiomatic systems. *Zeitschrift f. math. Logik und Grundlagen d. Math.*, 14:97–142, 1968.

[16] D. Leivant. The optimality of induction as an axiomatization of arithmetic. *The Journal of Symbolic Logic*, 48:182–184, 1983.

[17] C. Parsons. On a number-theoretic choice schema and its relation to induction. In A. Kino, J. Myhill, and R.E. Vessley, editors, *Intuitionism and Proof Theory*, pages 459–473. North Holland, Amsterdam, 1970.

[18] H.E. Rose. *Subrecursion: Functions and Hierarchies.* Clarendon Press, Oxford, 1984.