Annals of Pure and Applied Logic 61 (1993) 161–173
North-Holland

A note on the diagonalizable algebras of PA and ZF

V.Yu. Shavrukov

Department of Mechanics and Mathematics, Moscow State University, 119899 Moscow, Russian Federation

Communicated by D. van Dalen
Received 1 September 1991
Revised 1 June 1992

Abstract

Shavrukov, V.Yu., A note on the diagonalizable algebras of PA and ZF, Annals of Pure and Applied Logic 61 (1993) 161–173.

We prove that the diagonalizable algebras of PA and ZF are not isomorphic.

A *diagonalizable algebra* of an r.e. theory T is a pair $(\mathscr{A}_T, \Box_T) = \mathscr{D}_T$ where $\mathscr{A}_T$ is the quotient of the Boolean algebra of sentences of T modulo the ideal of theorems of T. $\mathscr{A}_T$ is usually called the *Lindenbaum sentence algebra of T*. $\Box_T$ is a unary operator on $\mathscr{A}_T$ which takes a sentence γ to the statement asserting that γ is provable in T. Thus T is assumed to contain enough arithmetic to express syntactical notions such as "$\cdots$ is a T-proof of $\cdots$". More specifically, the sentence $\Box_T\gamma$ is taken to be the *provability predicate of T* (which shall be identified with $\Box_T$) after its only free variable has been replaced by the Gödelnumber of γ. The provability predicate is assumed to have the following form:

$$\exists x \, \mathrm{Prf}_\alpha(x, y)$$

where $\mathrm{Prf}_\alpha(x, y)$, the *proof predicate of T*, is the formula expressing in the natural way that x codes a Hilbert-style proof of (the formula coded by) y from the extralogical axioms specified by α. The formula $\alpha(\cdot)$ with exactly one free variable occurs in the proof predicate as a subformula and is assumed to be Σ_1 so that the proof and provability predicates also are Σ_1 formulas. To the theory T this α has to bear the following relation:

$$\gamma \in S \text{ iff } \alpha(\gamma) \text{ is true}$$

Correspondence to: V.Yu. Shavrukov, Department of Mathematics and Informatics, University of Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, Netherlands.

for all sentences γ where S is a set of sentences which axiomatizes T. Of course neither the set of theorems of T nor S determines α uniquely.

The diagonalizable algebras of theories were introduced by Magari [2] and have since then been studied in close connection with *provability logics* (see Smoryński [7]).

How large is the collection of isomorphism types that diagonalizable algebras of various theories can offer? Among these algebras one finds such (cf. Smoryński [6]) that $\Box_T\gamma = \top$ implies $\gamma = \top$ for each $\gamma \in \mathscr{D}_T$ (this holds for Σ_1 sound theories T, that is, for those theories that prove no false Σ_1 sentences), and such algebras that there exists a $\gamma \in \mathscr{D}_T$ satisfying $\Box_T\gamma = \top$ but $\gamma \neq \top$ (Σ_1 ill theories). Moreover, in the latter case for any $m \in \omega$ the equality $\Box^n\bot = \top$ can hold for all $n > m$, or it can hold for no $n \in \omega$ at all. ($\bot$ and $\top$ are the zero and the unit of a Boolean or of a diagonalizable algebra.) This appears to be precisely all that has been known of distinctions between the diagonalizable algebras of different theories.

The present paper is devoted to the question whether the diagonalizable algebras of PA and ZF are isomorphic. We assume that the provability predicate of PA is natural enough so that

$$\mathrm{ZF} \vdash \forall \sigma \in \Sigma_1 (\Box_{\mathrm{PA}}\sigma \rightarrow \sigma).$$

The reader is also supposed to believe that ZF is Σ_1 sound. In this setting we have

Theorem. *The diagonalizable algebras $\mathscr{D}_{\mathrm{PA}}$ and $\mathscr{D}_{\mathrm{ZF}}$ are not isomorphic.*

In connection with this theorem we would like to mention two related facts. First, Pour-El and Kripke [3] show the Lindenbaum sentence algebras $\mathscr{A}_{\mathrm{PA}}$ and $\mathscr{A}_{\mathrm{ZF}}$ to be recursively isomorphic. Second, the algebras $\mathscr{D}_{\mathrm{PA}}$ and $\mathscr{D}_{\mathrm{ZF}}$ are recursively embeddable in one another (cf. Shavrukov [4]).

The Theorem settles (a particular case of) a question in Smoryński [6]. The method we use to prove the Theorem is similar to (and derives from) a trick employed in Shavrukov [4].

Proof. To carry out the proof we shall have to introduce a number of auxiliary notions and formulate a number of lemmas as we go along. The lemmas we use are very well-known and/or very easy to believe and hardly shed much light on the proof of the Theorem and therefore their proofs are only given in the Appendix.

Since our proof is going to deal with rates of growth of functions we need to fix a class of functions of neglectibly slow growth, elements of which are to be used as small change. As such we choose the class of (Kalmar) elementary functions. So for a set $V \subseteq \omega$ and functions f and g we define

$f \preccurlyeq_V g$ iff there exists an elementary function q such that
$f \leqslant_V q \circ g$, that is, $f(n) \leqslant q \circ g(n)$ for each $n \in V$.

We write $f \approx_V g$ to mean both $f \preccurlyeq_V g$ and $g \preccurlyeq_V f$. In case $V = \omega$ we just write $\preccurlyeq$ and $\approx$ instead of $\preccurlyeq_V$ and $\approx_V$ respectively.

The partial functions f and g are equal, $f \equiv g$, if their domains coincide and for each element n of their domain one has $f(n) = g(n)$. The expression $f \equiv_V g$ means that $V \cap \operatorname{dom} f = V \cap \operatorname{dom} g$ and $f(n) = g(n)$ for each element n of the latter set.

In fact we shall only deal with recursive partial functions. These are computed by the usual Turing machines. A Turing machine will be identified with its Gödelnumber and φ_i will stand for the function f computed by the ith Turing machine. In an alternative manner of speaking, i is a φ-index for (computing) f. The expression $\varphi_i(n)$ will not only stand for the output (if any) of the Turing machine (of Gödelnumber) i on the input n but also for the *computation* executed by that Turing machine on this input. Thus we write $\varphi_i(n)\downarrow$ or $\varphi_i(n)\uparrow$ according to whether this computation con- or diverges, and the expression

the number of steps in the computation $\varphi_i(n)$

also makes sense. We shall employ a (Blum) complexity measure Φ (cf. Blum [1]) associated with the φ-indexing which is slightly different from the usual ones, namely

$$\Phi_i(n) = i + n + \text{the number of steps in the computation } \varphi_i(n).$$

Our favourite feature of this complexity measure is that for each $m \in \omega$ there only exists a finite number of pairs (i, n) for which there is a chance of $\Phi_i(n) \leqslant m$.

Next we define the class of (*elementarily*) *cumulative* partial recursive functions by putting

f is elementarily cumulative

iff there exists a φ-index $\bar{f}$ for f s.t. $\Phi_{\bar{f}} \preccurlyeq_{\operatorname{dom} f} f$.

(Note that we then also have $\Phi_{\bar{f}} \approx_{\operatorname{dom} f} f$.) The intuition is that the rate of growth of f correctly reflects the complexity of computing it.

Lemma 1. *Each Kalmar elementary function is majorized by an elementarily cumulative elementary function.*

Expressions concerning φ_i and Φ_i (or even partial recursive functions if it is clear which particular φ-index is meant) will also occur in formalized contents. We assume that the underlying formalization is reasonable, so that some simple facts about Turing machines and the complexity measure are provable in formal theories in question, and economic, that is that the Kleene T-predicate is expressed by an elementary formula so that the relation $\Phi_i(n) \leqslant m$ is also expressed by an elementary formula, the relation $\varphi_i(n) = m$ is an elementary formula preceded by an existential quantifier etc.

Elementarity is also assumed of Gödelnumbering of syntax and of the proof predicates of formal theories under consideration, that is, the relation $T \vdash_n \gamma$

defined by

$$T \vdash_n \gamma \text{ iff } T \text{ proves } \gamma \text{ by a proof of Gödelnumber } \leqslant n$$

is elementary in n and γ and is expressed by an elementary formula $\Box_{T,n}\gamma$, which by abuse of terminology will also be referred to as the *proof predicate of T.* In the presence of the Σ_1 collection schema, for any provability predicate $\Box_T$ we can, using a trick due to Craig which possibly involves a minor rearranging of the set of axioms of T, find an elementary proof predicate $\Box_{T,n}$ such that

$$T \vdash \forall\gamma\,(\Box_T\gamma \leftrightarrow \exists n\, \Box_{T,n}\gamma).$$

Note that the *natural* proof predicates of PA and ZF are elementary because these theories are axiomatized by a finite number of axioms and axiom schemas.

Next, to every Σ_1 sound theory T containing $I\Delta_0 + exp$ we associate an indexing δ^T of 0-1-valued partial recursive functions by sentences of T in the following manner.

Define the sequence of sentences $\{\#^n_T\}_{n\in\omega}$

$$\#^n_T = \Box^{n+1}_T \perp \wedge \Diamond^n_T \top$$

($\Diamond$ is short for $\neg\Box\neg$ *and the upper indices of* $\Box$ *and* $\Diamond$ *denote iteration*) *and put*

$$\delta^T_\gamma(n) = \begin{cases} 0 & \text{if } T \vdash \#^n_T \rightarrow \gamma, \\ 1 & \text{if } T \vdash \#^n_T \rightarrow \neg\gamma, \\ \text{divergent} & \text{if } T + \#^n_T \text{ does not decide } \gamma. \end{cases}$$

From the viewpoint of T itself it is not clear that the value of $\delta^T_\gamma(n)$ is determined uniquely. Therefore, if one wants to deal with δ^T_γ in T, one has to add that the value $\delta^T_\gamma(n)$ is determined according to the shortest proof of either of the two sentences in question.

Δ^T is a complexity measure associated with δ^T which is defined as follows:

$$\Delta^T_\gamma(n) = \text{the minimal } d \text{ s.t. } T \vdash_d \#^n_T \rightarrow \gamma \text{ or } T \vdash_d \#^n_T \rightarrow \neg\gamma.$$

The crucial fact connecting δ^T and Δ^T with φ and Φ is:

Lemma 2. *Let T be an r.e.* Σ_1 *sound theory containing* $I\Delta_0 + exp$. *To each* φ*-index k for* 0-1-*valued partial recursive function there corresponds a sentence* γ *of T such that*

$$\delta^T_\gamma \equiv \varphi_k \quad \textit{and} \quad \Delta^T_\gamma \leqslant_{\mathrm{dom}\,\varphi_k} \Phi_k.$$

Conversely, to each sentence γ *of T there corresponds a* φ*-index k for a* 0-1-*valued partial recursive function such that*

$$\varphi_k \equiv \delta^T_\gamma \quad \textit{and} \quad \Phi_k \leqslant_{\mathrm{dom}\,\delta^T_\gamma} \Delta^T_\gamma.$$

We are now ready to start. Our strategy is to assume the existence of an isomorphism $e : \mathcal{D}_{\mathrm{PA}} \rightarrow \mathcal{D}_{\mathrm{ZF}}$ and use it to derive an absurdity.

Let X be a nonrecursive r.e. set.

Lemma 3. *There exists a partial recursive* 0-1-*valued function h and a φ-index $\bar{h}$ for it such that* $\operatorname{dom} h = X$ *and whenever i is a φ-index for h one has*

$$\Phi_{\bar{h}} \leqslant_X \Phi_i.$$

By Lemma 3 pick a partial recursive 0-1-valued function h and a φ-index $\bar{h}$ for it such that $\operatorname{dom} h = X$ and whenever i is a φ-index for h there holds

$$\Phi_{\bar{h}} \leqslant_X \Phi_i.$$

Next let α be a sentence of PA corresponding to h by Lemma 2 such that

$$\delta_\alpha^{\mathrm{PA}} \equiv h \quad \text{and} \quad \Delta_\alpha^{\mathrm{PA}} \leqslant_X \Phi_{\bar{h}}.$$

Let A be a sentence of ZF such that $A = e(\alpha)$. Since e is an isomorphism, and as such has to send $\#_{\mathrm{PA}}^n$ to $\#_{\mathrm{ZF}}^n$, we have that

$$\delta_A^{\mathrm{ZF}} \equiv \delta_\alpha^{\mathrm{PA}} \equiv h$$

and hence for some φ-index i for the function h

$$\Delta_\alpha^{\mathrm{PA}} \leqslant_X \Phi_{\bar{h}} \leqslant_X \Phi_i \leqslant_X \Delta_A^{\mathrm{ZF}}$$

by Lemma 2 and the choice of h. We have now that

$$\Delta_\alpha^{\mathrm{PA}} \leqslant_X p \circ \Delta_A^{\mathrm{ZF}}$$

for some elementary function p which we can by Lemma 1 assume cumulative and which will bear this name p throughout the sequel.

At this point we need more lemmas.

Lemma 4. *There exists a* ZF-*provably recursive monotonic elementarily cumulative function d eventually majorizing every provably recursive function of* PA *and such that if σ_1 and σ_2 are sentences satisfying*

$$\mathrm{PA} \vdash_n \Box_{\mathrm{PA}}\sigma_1 \vee \Box_{\mathrm{PA}}\sigma_2$$

then

$$\mathrm{PA} \vdash_{d(n)} \sigma_1 \quad \text{or} \quad \mathrm{PA} \vdash_{d(n)} \sigma_2.$$

Lemma 5. *For each r.e. Σ_1 sound theory containing $I\Delta_0 + exp$ and each sentence γ of T the function Δ_γ^T is cumulative.*

Lemma 6. *If a and b are cumulative partial recursive functions, then $a \circ b$ is also cumulative.*

The next lemma is a specialization of the Compression Theorem (cf. Blum [1]) and an improvement on Lemma 3.

Lemma 7. *Let a be a cumulative function with* $\operatorname{dom} a = X$. *Then there exists a partial recursive* 0-1-*valued function k and a φ-index $\bar{k}$ for it such that* $\operatorname{dom} k = X$

and whenever i is a φ-index for a 0-1-*valued* (*partial*) *recursive function satisfying $\varphi_i \equiv_X k$ there holds*

$$a \approx_X \Phi_{\tilde{k}} \preccurlyeq_X \Phi_i.$$

Define $g = d \circ d \circ d$, d being introduced through Lemma 4. Note that for each pair q, r of elementary functions g eventually majorizes the function $q \circ d \circ r$.

Since by Lemmas 4–6 the function $g \circ p \circ \Delta_A^{\mathrm{ZF}}$ is cumulative, Lemma 7 provides a 0-1-valued partial recursive function f and a φ-index $\tilde{f}$ for it such that $\operatorname{dom} f = X$ and

$$g \circ p \circ \Delta_A^{\mathrm{ZF}} \approx_X \Phi_{\tilde{f}} \preccurlyeq_X \Phi_i$$

whenever i is a φ-index for a 0-1-valued (partial) recursive function extending f. Let s be an elementary function such that

$$\Phi_{\tilde{f}} \preccurlyeq_X s \circ g \circ p \circ \Delta_A^{\mathrm{ZF}}.$$

Let $B(x)$ be the following formula of ZF:

$$\delta_A^{\mathrm{ZF}}(x){\downarrow} \to (\Phi_{\tilde{f}}(x) \leqslant s \circ g \circ p \circ \Delta_A^{\mathrm{ZF}}(x) \to f(x) = 0)$$

and define the formula B to be

$$\forall x\, (\#^x_{\mathrm{ZF}} \to B(x)).$$

We want to show that

$$\delta_B^{\mathrm{ZF}} \equiv_X f.$$

Indeed if $n \in X$ then $\delta_A^{\mathrm{ZF}}(n){\downarrow}$ and $B(n)$ provably reduces to

$$\Phi_{\tilde{f}}(n) \leqslant s \circ g \circ p \circ \Delta_A^{\mathrm{ZF}}(n) \to f(n) = 0$$

and then, since the antecedent of this formula is true and hence provable, to

$$f(n) = 0.$$

From this one derives

$$\begin{aligned} \mathrm{ZF} \vdash \#^n_{\mathrm{ZF}} &\to \forall x\, (\#^x_{\mathrm{ZF}} \to x = n) \\ &\to (\forall x\, (\#^x_{\mathrm{ZF}} \to B(x)) \leftrightarrow . \, (\#^n_{\mathrm{ZF}} \to B(n))) \\ &\to (B \leftrightarrow B(n)) \\ &\to (B \leftrightarrow f(n) = 0) \end{aligned}$$

whence $\delta_B^{\mathrm{ZF}}(n) \equiv_X f(n)$. Moreover, by formalizing the above argument we have

$$\begin{aligned} \mathrm{ZF} \vdash \forall x\, (&\Box_{\mathrm{ZF}}(\#^x_{\mathrm{ZF}} \to A) \vee \Box_{\mathrm{ZF}}(\#^x_{\mathrm{ZF}} \to \neg A) \to . \; \delta_A^{\mathrm{ZF}}(x){\downarrow}) \\ &\to . \; s \circ g \circ p \circ \Delta_A^{\mathrm{ZF}}(x){\downarrow}) \\ &\to . \; \Box_{\mathrm{ZF}} B(x) \vee \Box_{\mathrm{ZF}} \neg B(x)) \\ &\to . \; \Box_{\mathrm{ZF}}(\#^x_{\mathrm{ZF}} \to B) \vee \Box_{\mathrm{ZF}}(\#^x_{\mathrm{ZF}} \to \neg B)), \end{aligned}$$

and in particular for each $n \in \omega$

$$\mathrm{ZF} \vdash \Box_{\mathrm{ZF}}(\#^n_{\mathrm{ZF}} \to \mathrm{A}) \vee \Box_{\mathrm{ZF}}(\#^n_{\mathrm{ZF}} \to \neg A) \to . \Box_{\mathrm{ZF}}(\#^n_{\mathrm{ZF}} \to B) \vee \Box_{\mathrm{ZF}}(\#^n_{\mathrm{ZF}} \to \neg B).$$

Let $\beta = e^{-1}(B)$. e^{-1} should also be an isomorphism and so

$$\delta^{\mathrm{PA}}_\beta \equiv \delta^{\mathrm{ZF}}_B \equiv_X f$$

whence by Lemma 2 and the choice of f

$$\Phi_{\bar{f}} \leqslant_X \Delta^{\mathrm{PA}}_\beta.$$

Also one has by the same isomorphism that

$$\mathrm{PA} \vdash \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \alpha) \vee \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \neg\alpha) \to . \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \beta) \vee \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \neg\beta)$$

for all $n \in \omega$. Since PA is r.e. there exists a total recursive function j such that for each $n \in \omega$

$$\mathrm{PA} \vdash_{j(n)} \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \alpha) \vee \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \neg\alpha) \to . \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \beta) \vee \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \neg\beta).$$

The totality of j implies that the set

$$Y = \{n \in X \mid j(n) \leqslant \Delta^{\mathrm{PA}}_\alpha(n)\}$$

is infinite for otherwise dom $\Delta^{\mathrm{PA}}_\alpha$, that is, X would be recursive. Therefore the set $\{\Delta^{\mathrm{PA}}_\alpha(n) \mid n \in Y\}$ is unbounded.

Now we concentrate our attention on Y. For $n \in X$ we clearly have

$$\mathrm{PA} \vdash_{l(n)} \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \alpha) \vee \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \neg\alpha)$$

for some partial recursive function $l \leqslant_X \Delta^{\mathrm{PA}}_\alpha$ because constructing a PA-proof of $\Box_{\mathrm{PA}}\gamma$ from that of γ is quite an elementary task. Hence for all $n \in X$ and some partial recursive m such that

$$m \leqslant_X \max(j, l) \leqslant_Y \Delta^{\mathrm{PA}}_\alpha$$

there holds

$$\mathrm{PA} \vdash_{m(n)} \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \beta) \vee \Box_{\mathrm{PA}}(\#^n_{\mathrm{PA}} \to \neg\beta)$$

whence by the choice of the function d we have

$$\mathrm{PA} \vdash_{d \circ m(n)} \#^n_{\mathrm{PA}} \to \beta \quad \text{or} \quad \mathrm{PA} \vdash_{d \circ m(n)} \#^n_{\mathrm{PA}} \to \neg\beta$$

that is,

$$\Delta^{\mathrm{PA}}_\beta \leqslant_X d \circ m \leqslant_Y d \circ t \circ \Delta^{\mathrm{PA}}_\alpha$$

for some elementary function t for $m \leqslant_Y \Delta^{\mathrm{PA}}_\alpha$ and d is monotonic. Next recall that

$$g \circ \Delta^{\mathrm{PA}}_\alpha \leqslant_X g \circ p \circ \Delta^{\mathrm{ZF}}_A \leqslant_X \Phi_{\bar{f}} \leqslant_X \Delta^{\mathrm{PA}}_\beta$$

(the first inequality holds because g is monotonous and $\Delta^{\mathrm{PA}}_\alpha \leqslant_X p \circ \Delta^{\mathrm{ZF}}_A$). Putting things together we get

$$g \circ \Delta^{\mathrm{PA}}_\alpha \leqslant_Y d \circ t \circ \Delta^{\mathrm{PA}}_\alpha.$$

By the unboundedness of $\{\Delta_\alpha^{\mathrm{PA}}(n) \mid n \in Y\}$ we infer that there exists an elementary function u such that $u \circ d \circ t$ exceeds g for infinitely many arguments which contradicts the choice of g.

Thus from the existence of an isomorphism $e: \mathfrak{D}_{\mathrm{PA}} \rightarrow \mathfrak{D}_{\mathrm{ZF}}$ we derived a contradiction and therefore proved the absence of such e. □

The theories PA and ZF occupy a special place in the study of diagonalizable algebras and provability logics in that they constitute a conventional example of a pair of theories of which the second is much stronger than the first one (cf. Smoryński [7]). In the Theorem of the present paper this pair can be replaced by a wide class of others. For convenience we now bring together the conditions on the two theories under which this replacement is possible.

First, we either have to assume that both employed proof predicates are elementary, or that both theories T and S contain enough Σ_1 collection to provably equivalently replace their given proof predicates by elementary versions.

In fact our proof of the Theorem goes through for any pair of Σ_1 sound r.e. theories T and S containing $I\Delta_0 + exp$ such that S proves a 'smoothened' version of uniform Σ_1 reflection for the chosen elementary proof predicate of T:

$$S \vdash \forall x\, \exists y\, \forall \sigma_0(\cdot) \in \Delta_0\, (\Box_{T,x}\, \exists w\, \sigma_0(w) \rightarrow \exists z \leqslant y\, \sigma_0(z))$$

which follows from the usual uniform Σ_1 reflection schema

$$\forall \sigma \in \Sigma_1\, (\Box_T \sigma \rightarrow \sigma)$$

if S proves the appropriate instance of Σ_1 collection.

Appendix

Proof of Lemma 1. It is well known that each elementary function can be majorized by one of the functions $\{\lambda x.2_n^x\}_{n \in \omega}$ and that each of these functions is cumulative. □

Proof of Lemma 2. Constructing the φ-index k from a sentence γ is easy. The required Turing machine looks through the T-proofs and outputs 0 or 1 on input n once a proof of $\#_T^n \rightarrow \gamma$ or of $\#_T^n \rightarrow \neg\gamma$ is found, respectively. The task is clearly elementary in the Gödelnumber of the shortest proof of this kind, that is, in $\Delta_\gamma^T(n)$. Of course, it is important that the proof predicates we use are elementary as well as the Gödelnumbering of the syntax of T.

We turn to the converse construction. Thus we are given a Turing machine (of Gödelnumber) k which can only output 0 or 1 (this latter fact need not be provable in T). We have to produce a sentence γ and an elementary function q such that for all $n \in \omega$

$$\begin{aligned} T \vdash \#_T^n \rightarrow \gamma \ &\text{ iff } \ \varphi_k(n) = 0, \\ &\text{ iff } \ T \vdash_{q \circ \Phi_k(n)} \#_T^n \rightarrow \gamma \end{aligned}$$

and

$$T \vdash \#_T^n \rightarrow \neg\gamma \text{ iff } \varphi_k(n) = 1,$$
$$\text{iff } T \vdash_{q \circ \Phi_k(n)} \#_T^n \rightarrow \neg\gamma.$$

In order to construct such γ we shall essentially reproduce the proof of the Uniform Dual Semi-Representability Theorem of Smoryński [5] (slightly weakened).

By self-reference define $G(x)$ to be the formula

$$\exists y\, (((\Phi_k(x) < y \wedge \varphi_k(x) = 0) \vee \Box_{T,y}(\#_T^x \rightarrow \neg G(x))$$
$$\wedge\, \forall z < y \neg((\Phi_k(x) < z \wedge \varphi_k(x) = 1) \vee \Box_{T,z}(\#_T^x \rightarrow G(x)))).$$

Note that for no $n \in \omega$ can the theory T refute $\#_T^n$ because T is Σ_1 sound. First we show that

$$\Delta_{G(n)}^T(n) \leqslant \Phi_k(n)$$

for no $n \in \omega$ either. For if this did hold for some n then we would have

$$T \vdash_{\Phi_k(n)} \#_T^n \rightarrow G(n) \quad \text{and hence} \quad T \nvdash_{\Phi_k(n)} \#_T^n \rightarrow \neg G(n)$$

or

$$T \vdash_{\Phi_k(n)} \#_T^n \rightarrow \neg G(n) \quad \text{and hence} \quad T \nvdash_{\Phi_k(n)} \#_T^n \rightarrow G(n)$$

(if $\varphi_k(n)\uparrow$ then $\vdash_{\Phi_k(n)}$ is an euphemism for $\vdash$). These two possibilities after being formalized imply on inspection of the definition of $G(n)$

$$T \vdash \neg G(n) \quad \text{or} \quad T \vdash G(n) \quad \text{resp.}$$

whence in either case $T \vdash \neg\#_T^n$ quod non. So $\Delta_{G(n)}^T \leqslant \Phi_k(n)$ holds for no $n \in \omega$ and in particular if $\varphi_k(n)\uparrow$ then $T + \#_T^n$ does not decide $G(n)$. If $\varphi_k(n)\downarrow$ then we have $\Phi_k(n) < \Delta_{G(n)}^T$ and this easily implies

$$T \vdash G(n) \quad \text{if } \varphi_k(n) = 0, \quad \text{and} \quad T \vdash \neg G(n) \quad \text{if } \varphi_k(n) = 1.$$

Finally put γ to be

$$\forall x\, (\#_T^x \rightarrow G(x)).$$

Since

$$T \vdash \forall x\, \forall y\, (\#_T^x \wedge \#_T^y \rightarrow .\, x = y),$$

we have

$$T \vdash \#_T^n \rightarrow (\forall x\, (\#_T^x \rightarrow G(x)) \leftrightarrow .\, (\#_T^n \rightarrow G(n)))$$
$$\rightarrow (\gamma \leftrightarrow G(n)),$$

and therefore

$$T \vdash \#_T^n \rightarrow \gamma \qquad \text{if } \varphi_k(n) = 0,$$
$$T \vdash \#_T^n \rightarrow \neg\gamma \qquad \text{if } \varphi_k(n) = 1, \quad \text{and}$$
$$T + \#_T^n \text{ does not decide } \gamma \quad \text{if } \varphi_k(n)\uparrow$$

which amounts to $\delta_\gamma^T \equiv \varphi_k$.

For $n \in \operatorname{dom} \varphi_k$ the T-proofs of $\#_T^n \rightarrow \gamma$ and of $\#_T^n \rightarrow \neg\gamma$ are elementary in those of $G(n)$ and of $\neg G(n)$ respectively and the latter essentially amount to verifying $D(n, \Phi_k(n))$ for $D(x, y)$ an elementary formula which only takes elementrily long. Hence

$$\Delta_\gamma^T \preccurlyeq_{\operatorname{dom} \Phi_k} \Phi_k. \qquad \square$$

The proof of Lemma 3 will follow that of Lemma 7.

Proof of Lemma 4. First we show that there is a function D satisfying all the conditions of the Lemma except possibly the majorization property. This is easy. One just lets $D(n)$ be the minimal m such that

$$\mathrm{PA} \vdash_m \sigma_1 \quad \text{or} \quad \mathrm{PA} \vdash_m \sigma_2 \quad \text{whenever} \quad \mathrm{PA} \vdash_n \square_{\mathrm{PA}} \sigma_1 \vee \square_{\mathrm{PA}} \sigma_2.$$

D is then monotonic and cumulative for the computation of $D(n)$ consists of constructing all the PA-proofs with Gödelnumbers $\leqslant D(n)$ and a simple analysis of their structure. This is clearly elementary in $D(n)$.

Moreover, D is provably recursive in ZF for

$$\mathrm{ZF} \vdash \forall \sigma \in \Sigma_1 (\square_{\mathrm{PA}} \sigma \rightarrow \sigma)$$

and so

$$\begin{aligned} \mathrm{ZF} &\vdash \forall \sigma_1 \forall \sigma_2 (\square_{\mathrm{PA}}(\square_{\mathrm{PA}} \sigma_1 \vee \square_{\mathrm{PA}} \sigma_2) \rightarrow . \square_{\mathrm{PA}} \sigma_1 \vee \square_{\mathrm{PA}} \sigma_2) \\ &\vdash \forall x \exists y \forall \sigma_1 \forall \sigma_2 (\square_{\mathrm{PA},x}(\square_{\mathrm{PA}} \sigma_1 \vee \square_{\mathrm{PA}} \sigma_2) \rightarrow . \square_{\mathrm{PA},y} \sigma_1 \vee \square_{\mathrm{PA},y} \sigma_2) \end{aligned}$$

(the last step uses Σ_1 collection).

Second, we construct a ZF-provably recursive monotonic cumulative function F majorizing all the PA-provably recursive functions:

$$F(n) = \sum \{ \Phi_f(m) \mid m \leqslant n \text{ and } \mathrm{PA} \vdash_n \forall z\, \varphi_f(z) \downarrow \}.$$

F is clearly recursive, monotonic and majorizes each provably recursive function of PA.

To see that F is cumulative we note that the identity function $\mathrm{id} = \varphi_i$ is among those provably recursive in PA and so $\mathrm{id} \preccurlyeq \Phi_i \preccurlyeq F$. The computation of $F(n)$ consists of looking through the first n proofs of PA and calculating and summing up $\leqslant n^2$ values, each of the calculations taking $\leqslant F(n)$ time. This is clearly elementary in n and $F(n)$ and since $\mathrm{id} \preccurlyeq F$, also in just $F(n)$.

Now we have to show that ZF proves F total. This is done in several steps. Let

$$G(m, n) = \sum \{ \Phi_f(m) \mid \mathrm{PA} \vdash_n \forall z\, \varphi_f(z) \downarrow \}.$$

By induction on y within ZF one shows that for some elementary function q

$$\mathrm{ZF} \vdash \forall x \forall y\, \square_{\mathrm{PA},q(x,y)}\, G(x, y) \downarrow$$

(the bound q enables us to do with just elementary induction). Applying induction on y again we get an elementary function r such that

$$\mathrm{ZF} \vdash \forall x\, \forall y\, \Box_{\mathrm{PA},r(x,y)} \sum \{G(z, x) \mid z \leq y\}\downarrow.$$

In particular,

$$\mathrm{ZF} \vdash \forall x\, \Box_{\mathrm{PA},r(x,x)} \sum \{G(z, x) \mid z \leq x\}\downarrow,$$

that is,

$$\mathrm{ZF} \vdash \forall x\, \Box_{\mathrm{PA}} F(x)\downarrow$$

and since ZF proves uniform Σ_1 reflection for $\Box_{\mathrm{PA}}$,

$$\mathrm{ZF} \vdash \forall x\, F(x)\downarrow.$$

Finally put $d = D + F$ and observe that all the conditions of the lemma are met. □

Proof of Lemma 5. The reasons for Δ_γ^T's being cumulative are exactly the same as those for that of the function D defined in the proof of Lemma 4. □

Proof of Lemma 6. The cumulativity of a and b means that there exist φ-indices $\tilde{a}$ and $\tilde{b}$ for computing these functions and elementary functions $q_{\tilde{a}}$ and $q_{\tilde{b}}$ such that

$$\Phi_{\tilde{a}} \leq_{\mathrm{dom}\, a} q_{\tilde{a}} \circ a \quad \text{and} \quad \Phi_{\tilde{b}} \leq_{\mathrm{dom}\, b} q_{\tilde{b}} \circ b.$$

Clearly the following can be assumed of $q_{\tilde{b}}$:

- $q_{\tilde{b}}$ is monotonic,
- $q_{\tilde{b}}(n) \geq n$, and
- $q_{\tilde{b}}(n + m) \geq q_{\tilde{b}}(n) + q_{\tilde{b}}(m)$.

We want to prove the existence of a φ-index $\tilde{c}$ for computing $c = a \circ b$ and of a Kalmar elementary function $q_{\tilde{c}}$ such that

$$\Phi_{\tilde{c}} \leq_{\mathrm{dom}\, a \circ b} q_{\tilde{c}} \circ a \circ b.$$

Take the Turing machines (with Gödelnumbers) $\tilde{a}$ and $\tilde{b}$ and rename the states of $\tilde{a}$ so that each one of them be distinct from every state of $\tilde{b}$ and then identify the starting state of $\tilde{a}$ with the halting state of $\tilde{b}$. Let $\tilde{c}$ be (the Gödelnumber of) the resulting Turing machine. One has

$$\Phi_{\tilde{c}}(n) = \tilde{c} + n + \text{the number of steps in the computation } \varphi_{\tilde{b}}(n)$$
$$+ \text{the number of steps in the computation } \varphi_{\tilde{a}}(b(n)).$$

Now set

$$q_{\tilde{c}}(m) = \tilde{c} + q_{\tilde{b}} \circ q_{\tilde{a}}(m).$$

We only have to calculate:

$$\begin{aligned}
q_{\tilde{c}} \circ a \circ b(n) &= \tilde{c} + q_{\tilde{b}} \circ q_{\tilde{a}} \circ a \circ b(n) \geqslant \tilde{c} + q_{\tilde{b}} \circ \Phi_{\tilde{a}}(b(n)) \\
&= \tilde{c} + q_{\tilde{b}}(\tilde{a} + b(n) + \text{the number of steps in the computation } \varphi_{\tilde{a}}(b(n))) \\
&\geqslant \tilde{c} + \tilde{a} + q_{\tilde{b}} \circ b(n) + \text{the number of steps in the computation } \varphi_{\tilde{a}}(b(n)) \\
&\geqslant \tilde{c} + \Phi_{\tilde{b}}(n) + \text{the number of steps in the computation } \varphi_{\tilde{a}}(b(n)) \\
&= \tilde{c} + \tilde{b} + n + \text{the number of steps in the computation } \varphi_{\tilde{b}}(n) \\
&\quad + \text{the number of steps in the computation } \varphi_{\tilde{a}}(b(n)) \\
&\geqslant \tilde{c} + n + \text{the number of steps in the computation } \varphi_{\tilde{b}}(n) \\
&\quad + \text{the number of steps in the computation } \varphi_{\tilde{a}}(b(n)) \\
&= \Phi_{\tilde{c}}(n). \qquad \square
\end{aligned}$$

Proof of Lemma 7. Since a is a cumulative there exists a φ-index $\tilde{a}$ for computing a such that $a \approx_X \Phi_{\tilde{a}}$ and in the sequel we can deal with $\Phi_{\tilde{a}}$ instead of a.

We describe an algorithm for computing the required function k step by step starting with Step 0. At Step m the value of k is defined precisely for those $n \in X$ that satisfy $\Phi_a(n) = m$.

Step m. Let

$$D_m = \{n \in X \mid \Phi_{\tilde{a}}(n) < m\} \quad \text{and} \quad N_m = \{n \in X \mid \Phi_{\tilde{a}}(n) = m\}.$$

Our present task is to define k on the elements of N_m. We assume the value of k to have already been defined on elements of D_m and note that the cardinality of D_m and of N_m does not exceed m. If N_m is empty then we just go to Step $m+1$. Otherwise put

$$\begin{aligned}
W_m = \{h \in \omega \mid{} & \text{there exists an } n \in N_m \text{ s.t. } \Phi_h(n) \leqslant m = \Phi_{\tilde{a}}(n), \\
& \text{and } \varphi_h(n) = k(n) \text{ for each } n \in D_m \text{ s.t. } \Phi_h(n) \leqslant \Phi_{\tilde{a}}(n)\}.
\end{aligned}$$

Again, note that W_m can contain at most m elements. If W_m is empty then let the value of k on every element of N_m be 0. Else let $w_m = \min W_m$ and define $k(n) = 1 \dot{-} \varphi_{w_m}(n)$ for those $n \in N_m$ that satisfy $\Phi_{w_m}(n) \leqslant m$, and $k(n) = 0$ for the remaining $n \in N_m$.

Finally go to Step $m+1$.

Let $\tilde{k}$ φ-index the Turing machine corresponding to the above algorithm. We easily have that $\Phi_{\tilde{k}} \preccurlyeq_X \Phi_{\tilde{a}}$ because $k(n)$ is defined at Step $\Phi_{\tilde{a}}(n)$ (for this reason we also have $\Phi_{\tilde{a}} \preccurlyeq_X \Phi_{\tilde{k}}$) and clearly each Step m is elementary in m because to carry it out $\tilde{k}$ executes at most m first steps of at most m first Turing machines on at most m inputs along with some simple bookkeeping. Thus

$$\Phi_{\tilde{k}} \approx_X \Phi_{\tilde{a}} \approx_X a.$$

Consider the set

$$\begin{aligned}
Z = \{h \in \omega \mid{} & \varphi_h(n) = k(n) \text{ for all } n \in X \text{ s.t. } \Phi_h(n) \leqslant \Phi_{\tilde{a}}(n), \\
& \text{and } \Phi_h(n) \leqslant \Phi_{\tilde{a}}(n) \text{ for infinitely many } n \in X\}.
\end{aligned}$$

We are going to show that Z is empty. Suppose h_0 is its minimal element. Then for each $h < h_0$ there is an $n \in X$ such that $\varphi_h(n) \neq k(n)$ and $\Phi_h(n) \leqslant \Phi_{\bar{a}}(n)$, or there exists a $j \in \omega$ such that the value of k is defined during the first j steps on all $n \in X$ satisfying $\Phi_h(n) \leqslant \Phi_{\bar{a}}(n)$. Now let $J \in \omega$ be so large that for each $h < h_0$,

(i) there exists an $n \in X$ such that $\varphi_h(n) \neq k(n)$ and $\Phi_h(n) \leqslant \Phi_{\bar{a}}(n) \leqslant J$, or

(ii) the value of k is defined during the first J steps on all $n \in X$ such that $\Phi_h(n) \leqslant \Phi_{\bar{a}}(n)$.

Since we assumed that $\Phi_{h_0}(n) \leqslant \Phi_{\bar{a}}(n)$ for infinitely many $n \in X$ there should be an $n_0 \in X$ such that

$$J < \Phi_{h_0}(n_0) \leqslant \Phi_{\bar{a}}(n_0).$$

Let us now compute $k(n_0)$. This value is defined at Step $\Phi_{\bar{a}}(n_0)$. We claim that $w_{\Phi_{\bar{a}}(n_0)} = \min W_{\Phi_{\bar{a}}(n_0)} = h_0$. It is straightforward to see that $h_0 \in W_{\Phi_{\bar{a}}(n_0)}$ since $n_0 \in N_{\Phi_{\bar{a}}(n_0)}$ and $\Phi_{h_0}(n_0) \leqslant \Phi_{\bar{a}}(n_0)$. Let $h < h_0$. If (i) holds for h, then we have that k was defined to differ from φ_h at an earlier step because $J < \Phi_{\bar{a}}(n_0)$. If (ii) is the case for h, then $\Phi_{\bar{a}}(n_0) < \Phi_h(n_0)$ (or even $\Phi_h(n_0)\uparrow$). In either case $h \notin W_{\Phi_{\bar{a}}(n_0)}$. Thus $h_0 = w_{\Phi_{\bar{a}}(n_0)}$ and therefore $k(n_0) = 1 \dot{-} \varphi_{h_0}(n_0)$ since $\Phi_{h_0}(n_0) \leqslant \Phi_{\bar{a}}(n_0)$. But this contradicts the assumption $h_0 \in Z$. The contradiction proves Z to be empty.

Next imagine a φ-index i such that $\varphi_i \equiv_X k$. Since $i \notin Z$ the relation $\Phi_i(n) \leqslant \Phi_{\bar{a}}(n)$ can only hold for finitely many $n \in X$, so

$$\Phi_{\bar{k}} \approx_X \Phi_{\bar{a}} \preccurlyeq_X \Phi_i$$

which completes the proof of Lemma 7. □

Proof of Lemma 3. This lemma follows from Lemma 7 once we know that cumulative functions whose domain is X exist. By Lemmas 2 and 5, they do. □

References

[1] M. Blum, A machine-independent theory of the complexity of recursive functions, J. Assoc. Comput. Mach. 14 (1967) 322–336.

[2] R. Magari, The diagonalizable algebras (the algebraization of the theories which express Theor.: II), Boll. Un. Mat. Ital. 12 (4) (1975) suppl.fasc. 3, 117–125.

[3] M.B. Pour-El and S. Kripke, Deduction-preserving ‘recursive isomorphisms’ between theories, Fund. Math. 61 (1967) 141–163.

[4] V. Yu. Shavrukov, Subalgebras of diagonalizable algebras of theories containing arithmetic, ITLI Prepublication Series X-91-03, Instiute for Language Logic and Information, University of Amsterdam, 1991. To appear in Dissertationes Math.

[5] C. Smoryński, Calculating self-referential statements, Fund. Math. 109 (1980) 189–210.

[6] C. Smoryński, Fixed point algebras, Bull. (N.S.) Amer. Math. Soc. 6 (1982) 317–356.

[7] C. Smoryński, Self-Reference and Modal Logic (Springer, New York, 1985).