A NOTE ON THE DIAGONIZABLE ALGEBRAS OF PA AND ZF

V.Yu. Shavrukov

ITLI Prepublication Series
for Mathematical Logic and Foundations ML-91-09

University of Amsterdam
A NOTE ON THE DIAGONIZABLE
ALGEBRAS OF PA AND ZF

V.Yu. Shavrukov
Department of Mathematics and Computer Science
University of Amsterdam
Abstract

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taken to be the provability predicate of $T$ (which shall be identified with $\eta_T$) after its only free variable has been replaced by the Gödel number of $\gamma$.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

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

where $\text{Prf}_\alpha(x, y)$, 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 $\alpha$. The formula $\alpha(\cdot)$ with exactly one free variable occurs in the proof predicate as a subformula and is assumed to be $\Sigma_1$ so that the proof and provability predicates also are $\Sigma_1$ formulas.

To the theory $T$ this $\alpha$ has to bear the following relation:

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

for all sentences $\gamma$ where $S$ is a set of sentences which axiomatizes $T$. Of course neither the set of theorems of $T$ nor $S$ determines $\alpha$ 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 $\sigma_\mathcal{T} \gamma = \top$ implies $\gamma = \top$ for each $\gamma \in \mathcal{D}_\mathcal{T}$ (this holds for $\Sigma_1$ sound theories $\mathcal{T}$, that is, for those theories that prove no false $\Sigma_1$ sentences), and such algebras that there exists a $\gamma \in \mathcal{D}_\mathcal{T}$ satisfying $\sigma_\mathcal{T} \gamma = \top$ but $\gamma \neq \top$ ($\Sigma_1$ ill theories). Moreover, in the latter case for any $m \in \omega$ the equality $\sigma_\mathcal{A}^n \gamma = \top$ 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 the author to be precisely all that is presently 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

$$\text{ZF} \vdash \forall \sigma \in \Sigma_1 (\sigma_\text{PA} \sigma \rightarrow c)$$

The reader is also supposed to believe that ZF is $\Sigma_1$ sound. In this setting we have

Theorem. The diagonalizable algebras $\mathcal{D}_\text{PA}$ and $\mathcal{D}_\text{ZF}$ are not isomorphic.

In connection with this theorem we would like to mention two related facts. First, Pour-El & Kripke [3] show the Lindenbaum sentence algebras $\mathfrak{A}_\text{PA}$ and $\mathfrak{A}_\text{ZF}$ to be recursively isomorphic. Second, the algebras $\mathcal{D}_\text{PA}$ and $\mathcal{D}_\text{ZF}$ are recursively embeddable in one another (cf. Shavrukov [4]).
The Theorem settles (a particular case of) a tiny 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 do 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 negligibly 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

$f \preceq_V g$ iff there exists an elementary function $q$ s.t.

$f \preceq_V q \circ g$, that is, $f(n) \preceq_V q \circ g(n)$ for each $n \in V$

We write $f \simeq_V g$ to mean both $f \preceq_V g$ and $g \preceq_V f$. In case $V = \omega$ we just write $<$ and $\approx$ instead of $\preceq_V$ and $\simeq_V$ 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 $V \cap \text{dom } f = V \cap \text{dom } g$ 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 Gödel number and $\varphi_i$ will
stand for the function \( f \) computed by the \( i \)th Turing machine. In an alternative manner of speaking, \( i \) is a \( \psi \)-index for (computing) \( f \). The expression \( \psi_i(n) \) 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 \( \psi_i(n) \downarrow \) or \( \psi_i(n) \uparrow \) according to whether this computation converges or diverges, and the expression

the number of steps in the computation \( \psi_i(n) \)

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

\[
\Phi_i(n) = i + n + \text{the number of steps in the computation } \psi_i(n)
\]

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 \( \Phi_i(n) \leq m \).

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

\( f \) is elementarily cumulative iff

there exist a \( \psi \)-index \( f \) for \( f \) s.t. \( \Phi_f \lesssim \text{dom } f \)

(Note that we then also have \( \Phi_f \approx \text{dom } f \).) 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 \( \psi_i \) and \( \Phi_i \) (or even partial recursi-
ve functions if it is clear which particular \( \varphi \)-index is meant) will also occur in formalized contexts. We convene 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 \( \Phi_i(n) \leq m \) 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 Gödel numbering of syntax and of the proof predicates of formal theories under consideration, that is, the relation \( T \vdash \gamma \) defined by

\[
T \vdash \gamma \iff T \text{ proves } \gamma \text{ by a proof of Gödel number } \leq n
\]
is elementary in \( n \) and \( \gamma \) and is expressed by an elementary formula \( \varrho_{T,n} \gamma \), which by abuse of terminology will also be referred to as the proof predicate of \( T \). In the presence of the \( \Sigma_1 \) collection schema, for any provability predicate \( \varrho_T \) 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 \( \varrho_{T,n} \) s.t.

\[
T \vdash \forall \gamma (\varrho_T \gamma \iff \exists n \varrho_{T,n} \gamma)
\]
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 \( \Sigma_1 \) sound theory \( T \) containing \( \mathsf{IA}_0 + \mathsf{exp} \) we associate an indexing \( \delta_T \) of 0-1-valued partial recursive functions by sentences of \( T \) in the following manner:
Define the sequence of sentences \( \{ \#_T^n \}_{n \in \omega} \)

\[ \#_T^n = \circ^{n+1} \land \circ^n T \]

(\( \circ \) is short for \( \forall \circ \) and the upper indices of \( \circ \) and \( \circ \) denote iteration) and put

\[ \delta^T_y (n) = \begin{cases} 0 & \text{if } T \vdash \#_T^n \rightarrow y \\ 1 & \text{if } T \vdash \#_T^n \rightarrow \neg y \\ \text{divergent} & \text{if } T + \#_T^n \text{ does not decide } y \end{cases} \]

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

\( \Delta^T \) is a complexity measure associated with \( \delta^T \) which is defined as follows:

\[ \Delta^T_y (n) = \text{the minimal } d \text{ s.t. } T \vdash_{d} \#_T^n \rightarrow y \text{ or } T \vdash_{d} \#_T^n \rightarrow \neg y \]

The crucial fact connecting \( \delta^T \) and \( \Delta^T \) with \( \varphi \) and \( \Phi \) is

**Lemma 2.** Let \( T \) be an r.e. \( \Sigma_1 \) sound theory containing \( \text{IA}_0 + \text{exp} \). To each \( \varphi \)-index \( k \) for a 0-1-valued partial recursive function there corresponds a sentence \( y \) of \( T \) s.t.

\[ \delta^T_y = \varphi_k \quad \text{and} \quad \Delta^T_y \leq \text{dom } \varphi_k \Phi_k \]

Conversely, to each sentence \( y \) of \( T \) there corresponds a \( \varphi \)-index \( k \) for a 0-1-valued partial recursive function s.t.

\[ \varphi_k = \delta^T_y \quad \text{and} \quad \Phi_k \leq \text{dom } \delta^T_y \Delta^T_y \]
We are now ready to start. Our strategy is to assume the existence of an isomorphism $e: \mathcal{D}_{PA} \to \mathcal{D}_{ZF}$ 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 $\varphi$-index $h$ for it s.t. $\text{dom } h = X$ and whenever $i$ is a $\varphi$-index for $h$ one has

$$\phi_h \leq_X \phi_i$$

By Lemma 3 pick a partial recursive 0-1-valued function $h$ and a $\varphi$-index $h$ for it s.t. $\text{dom } h = X$ and whenever $i$ is a $\varphi$-index for $h$ there holds

$$\phi_h \leq_X \phi_i$$

Next let $\alpha$ be a sentence of PA corresponding to $h$ by Lemma 2 s.t.

$$\delta_{\alpha}^{PA} = h \quad \text{and} \quad \Delta_{\alpha}^{PA} \leq_X \phi_h$$

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

$$\delta_{A}^{ZF} = \delta_{\alpha}^{PA} = h$$

and hence for some $\varphi$-index $i$ for the function $h$

$$\Delta_{\alpha}^{PA} \leq_X \phi_h \leq_X \phi_i \leq_X \Delta_{A}^{ZF}$$

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

$$\Delta_{\alpha}^{PA} \leq_X p \circ \Delta_{A}^{ZF}$$

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

Consider a total recursive function \( d \) s.t. for each natural number \( n \) the value \( d(n) \) is s.t. whenever

\[
\text{PA} \vdash_{n} \Box_{\text{PA}} \sigma_1 \lor \Box_{\text{PA}} \sigma_2
\]

for a pair of sentences \( \sigma_1 \) and \( \sigma_2 \), there holds

\[
\text{PA} \vdash_{d(n)} \sigma_1 \text{ or } \text{PA} \vdash_{d(n)} \sigma_2
\]

The function \( d \) is a provably recursive function of ZF for

\[
\text{ZF} \vdash \forall \sigma \in \Sigma_1 (\Box_{\text{PA}} \sigma \rightarrow \sigma)
\]

and so

\[
\text{ZF} \vdash \forall \sigma_1 \forall \sigma_2 \left( \Box_{\text{PA}} \left( \Box_{\text{PA}} \sigma_1 \lor \Box_{\text{PA}} \sigma_2 \right) \rightarrow \Box_{\text{PA}} \sigma_1 \lor \Box_{\text{PA}} \sigma_2 \right)
\]

\[
\vdash \forall x \exists y \forall \sigma_1 \forall \sigma_2 \left( \Box_{\text{PA},x} \left( \Box_{\text{PA}} \sigma_1 \lor \Box_{\text{PA}} \sigma_2 \right) \rightarrow \Box_{\text{PA},y} \sigma_1 \lor \Box_{\text{PA},y} \sigma_2 \right)
\]

(the last step uses \( \Sigma_1 \) collection).

By a result of Parikh (cf. Shavrukov [4]) the function \( d \) can be chosen to eventually majorize every provably recursive function of \( \text{PA} \). Now let \( g = d \circ d \circ d \) and note that for each pair \( q, r \) of elementary functions \( g \) eventually majorizes the function \( q \circ d \circ r \).

At this point we need more lemmas.

**Lemma 4.** The function \( d \) is cumulative.

**Lemma 5.** For each r.e. \( \Sigma_1 \) sound theory containing \( \text{IA}_0 + \text{exp} \) and each sentence \( \gamma \) of \( T \) the function \( \Lambda_{\gamma}^T \) 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 $\text{dom } a = X$. Then there exists a partial recursive 0-1-valued function $k$ and a $\varphi$-index $k$ for it s.t. $\text{dom } k = X$ and whenever $i$ is a $\varphi$-index for a 0-1-valued (partial) recursive function satisfying $\varphi_i \equiv_X k$ there holds

$$a \equiv_X \Phi_k \equiv_X \Phi_i$$

Since by Lemmas 4 - 6 the function $g \circ p \circ \Delta^ZF_A$ is cumulative, Lemma 7 provides a 0-1-valued partial recursive function $f$ and a $\varphi$-index $f$ for it s.t. $\text{dom } f = X$ and

$$g \circ p \circ \Delta^ZF_A \equiv_X \Phi_f \equiv_X \Phi_i$$

whenever $i$ is a $\varphi$-index for a 0-1-valued (partial) recursive function extending $f$. Let $s$ be an elementary function s.t.

$$\Phi_f \equiv_X s \circ g \circ p \circ \Delta^ZF_A$$

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

$$\delta^ZF_A(x) \downarrow \rightarrow \left[ \Phi_f(x) \leq s \circ g \circ p \circ \Delta^ZF_A(x) \rightarrow f(x) = 0 \right]$$

and define the formula $B$ to be

$$\forall x \left[ \#^ZF_A \rightarrow B(x) \right]$$

We want to show that
\[ \delta_B^ZF \equiv_X f \]

Indeed if \( n \in \chi \) then \( \delta_A^Z(n) \downarrow \) and \( B(n) \) provably reduces to
\[ \Phi_f(n) \leq s \circ g \circ p \circ \Delta_A^Z(n) \rightarrow f(n) = 0 \]
and then, since the antecedent of this formula is true and hence provable, to
\[ f(n) = 0 \]
From this derives
\[
\begin{align*}
ZF \vdash \#n^ZF_{\chi} & \rightarrow \left( \forall x \left( \#x^ZF_{\chi} \rightarrow B(x) \right) \leftrightarrow \left( \#n^ZF_{\chi} \rightarrow B(n) \right) \right) \\rightarrow B \leftrightarrow B(n) \\
& \rightarrow B \leftrightarrow f(n) = 0
\end{align*}
\]
whence \( \delta_B^ZF(n) \equiv_X f(n) \). Moreover by formalizing the above argument we have
\[
\begin{align*}
ZF \vdash \forall x \left( \varnothing_{\chi}^ZF(\#x^ZF_{\chi} \rightarrow A) \lor \varnothing_{\chi}^ZF(\#x^ZF_{\chi} \rightarrow \neg A) \rightarrow \delta_A^Z(x) \downarrow \right) & \rightarrow s \circ g \circ p \circ \Delta_A^Z(x) \downarrow \\
& \rightarrow \varnothing_{\chi}B(x) \lor \varnothing_{\chi}B(x) \\
& \rightarrow \varnothing_{\chi}B(\#x^ZF_{\chi} \rightarrow B) \lor \varnothing_{\chi}B(\#x^ZF_{\chi} \rightarrow \neg B)
\end{align*}
\]
and in particular for each \( n \in \omega \)
\[
ZF \vdash \varnothing_{\chi}^ZF(\#n^ZF_{\chi} \rightarrow A) \lor \varnothing_{\chi}^ZF(\#n^ZF_{\chi} \rightarrow \neg A) \rightarrow \\
\rightarrow \varnothing_{\chi}^ZF(\#n^ZF_{\chi} \rightarrow B) \lor \varnothing_{\chi}^ZF(\#n^ZF_{\chi} \rightarrow \neg B)
\]
Let \( \beta = e^{-1}(B) \). \( e^{-1} \) should also be an isomorphism and so
\[ \delta^P_A \equiv \delta^F_B \equiv X \ell \]

whence by Lemma 2 and the choice of \( \ell \)

\[ \psi \ell \preceq X \Delta^P_A \]

Also one has by the same isomorphism that

\[ \text{PA} \vdash \alpha^P_A (\#^n_{PA} \rightarrow \alpha) \vee \alpha^P_A (\#^n_{PA} \rightarrow \gamma \alpha) \rightarrow \]

\[ \rightarrow \alpha^P_A (\#^n_{PA} \rightarrow \beta) \vee \alpha^P_A (\#^n_{PA} \rightarrow \gamma \beta) \]

for all \( n \in \omega \). Since PA is r.e. there exists a total recursive function \( j \) s.t. for each \( n \in \omega \)

\[ \text{PA} \vdash \alpha^P_A (\#^n_{PA} \rightarrow \alpha) \vee \alpha^P_A (\#^n_{PA} \rightarrow \gamma \alpha) \rightarrow \]

\[ \rightarrow \alpha^P_A (\#^n_{PA} \rightarrow \beta) \vee \alpha^P_A (\#^n_{PA} \rightarrow \gamma \beta) \]

The totality of \( j \) implies that the set

\[ Y = \{ \ n \in X \mid j(n) \leq \Delta^P_A(n) \} \]

is infinite for otherwise \( \text{dom} \Delta^P_A = X \) would be recursive. For the same reason the set \( \{ \Delta^P_A(n) \mid n \in Y \} \) is unbounded.

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

\[ \text{PA} \vdash \alpha^P_A (\#^n_{PA} \rightarrow \alpha) \vee \alpha^P_A (\#^n_{PA} \rightarrow \gamma \alpha) \]

for some partial recursive \( l \preceq \Delta^P_A \) because constructing a PA-proof of \( \alpha^P_A \gamma \) from that of \( \gamma \) is quite an elementary task. Hence for all \( n \in X \) and some partial recursive \( m \) s.t.

\[ m \preceq X \max (j, l) \preceq \gamma \Delta^P_A \]

there holds

\[ \text{PA} \vdash \alpha^P_A (\#^n_{PA} \rightarrow \beta) \vee \alpha^P_A (\#^n_{PA} \rightarrow \gamma \beta) \]

whence by the choice of the function \( d \) we have
\[ PA \vdash d \cdot m(n) \#_{PA}^n \to \beta \quad \text{or} \quad PA \vdash d \cdot m(n) \#_{PA}^n \to \gamma \beta \]

that is,

\[ \Delta_{\beta}^{PA} \preceq_X d \cdot m \preceq_Y d \cdot t \cdot \Delta_{\alpha}^{PA} \]

for some elementary function \( t \) for \( m \preceq_Y \Delta_{\alpha}^{PA} \) and \( d \) is monotone. Next recall that

\[ g \cdot \Delta_{\alpha}^{PA} \preceq_X g \cdot p \cdot \Delta_{A}^{ZF} \preceq_X \Phi_{\ell} \preceq_X \Delta_{\beta}^{PA} \]

(the first inequality holds because \( g \) is monotone and \( \Delta_{\alpha}^{PA} \preceq_X p \cdot \Delta_{A}^{ZF} \)). Putting things together we get

\[ g \cdot \Delta_{\alpha}^{PA} \preceq_Y d \cdot t \cdot \Delta_{\alpha}^{PA} \]

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

Thus from out of existence of an isomorphism \( e: D_{PA} \to D_{ZF} \) 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 $\Sigma_1$ 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 $\Sigma_1$ sound r.e. theories $T$ and $S$ containing $\text{I}\Delta_0 + \text{exp}$ s.t. $S$ proves a "smoothened" version of uniform $\Sigma_1$ reflection for the chosen elementary proof predicate of $T$:

$$S \vdash \forall x \exists y \forall \sigma_0(\cdot) \in \Delta_0 \left[ a_T, x \exists y, \sigma_0(y) \rightarrow \exists z \leq y, \sigma_0(z) \right]$$

which follows from the usual uniform $\Sigma_1$ reflection schema

$$\forall \sigma \in \Sigma_1 \ (a_T \sigma \rightarrow c)$$

if $S$ proves the appropriate instance of $\Sigma_1$ collection.
Appendix

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

Proof of Lemma 2. Constructing the \( \varphi \)-index \( k \) from a sentence \( \gamma \) 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 \( \#_T^n \rightarrow \lnot \gamma \) is found, respectively. The task is clearly elementary in the Gödel number of the shortest proof of this kind, that is, in \( \Delta^T_y(n) \). Of course, it is important that the proof predicates we use are elementary as well as the Gödel numbering of the syntax of \( T \).

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

\[
T \vdash \#_T^n \rightarrow \gamma \quad \text{iff} \quad \varphi_k(n) = 0
\]

\[
\text{iff} \quad T \vdash q \circ \Phi_k(n) \quad \#_T^n \rightarrow \gamma
\]

and

\[
T \vdash \#_T^n \rightarrow \lnot \gamma \quad \text{iff} \quad \varphi_k(n) = 0
\]

\[
\text{iff} \quad T \vdash q \circ \Phi_k(n) \quad \#_T^n \rightarrow \lnot \gamma
\]

In order to construct such \( \gamma \) we shall essentially reproduce the proof of the Uniform Dual Semi-Representability Theorem of Słomczyński [5] (slightly weakened).
By self-reference define $G(x)$ to be the formula

$$\exists y \left( \left( \Phi_k(x) < y \land \varphi_k(x) = 0 \right) \lor \varnothing_{T^y} \left[ \#_T^x \rightarrow \neg G(x) \right] \right) \land$$

$$\land \forall z < y \left( \left( \Phi_k(x) < z \land \varphi_k(x) = 1 \right) \lor \varnothing_{T^z} \left[ \#_T^x \rightarrow G(x) \right] \right)$$

Note that for no $n \in \omega$ can the theory $T$ refute $\#_T^n$ because $T$ is $\Sigma_1$ sound. First we show that

$$\Delta_T^T(n) \leq \Phi_k(n)$$

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

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

or

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

These two possibilities after being formalized imply on inspection of the definition of $G(n)$

$$T \models \neg G(n) \quad \text{or} \quad T \models G(n)$$

respectively whence in either case $T \models \neg \#_T^n$ quod non. So $\Delta_T^T(n) \leq \Phi_k(n)$ 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 $\Phi_k(n) < \Delta_T^T(n)$ and this easily implies

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

Finally put $\gamma$ to be

$$\forall x \left( \#_T^x \rightarrow G(x) \right)$$

Since

15
$$T \vdash \forall x \forall y \left( \#^X_T \land \#^Y_T \rightarrow x = y \right)$$

we have

$$T \vdash \#^n_T \rightarrow \left( \forall x \left( \#^x_T \rightarrow G(x) \right) \leftrightarrow \left( \#^n_T \rightarrow G(n) \right) \right)$$

$$\rightarrow \left( \gamma \leftrightarrow G(n) \right)$$

and therefore

$$T \vdash \#^n_T \rightarrow \gamma \text{ if } \varphi_k(n) = 0,$$

$$T \vdash \#^n_T \rightarrow \neg \gamma \text{ if } \varphi_k(n) = 1 \text{ and}$$

$$T + \#^n_T \text{ does not decide } \gamma \text{ if } \varphi_k(n) \uparrow$$

which amounts to $\delta_T^\gamma = \varphi_k$.

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

$$\Delta_T^\gamma \leq \text{dom } \varphi_k \Phi_k$$

q.e.d. ■

**Proof** of Lemma 4. The computation of $d(n)$ consists of constructing all the T-proofs with Gödel numbers $\leq d(n)$ and a simple analysis of their structure. This task is clearly elementary in $d(n)$. ■

**Proof** of Lemma 5. See the proof of Lemma 4 reading $\Delta_T^\gamma(n)$ instead of $d(n)$. ■
Proof of Lemma 6. The cumulativity of $a$ and $b$ means that there exist $\varphi$-indices $a$ and $b$ for computing these functions and elementary functions $q_a$ and $q_b$ s.t.

$$\Phi_a \leq \text{dom } a \cdot q_a \circ a \quad \text{and} \quad \Phi_b \leq \text{dom } b \cdot q_b \circ b$$

Clearly the following can be assumed of $q_b$:

- $q_b$ is monotonous;
- $q_b(n) \geq n$ and
- $q_b(n+m) \geq q_b(n) + q_b(m)$

We want to prove the existence of a $\varphi$-index $c$ for computing $c = a \circ b$ and of a Kalmar elementary function $q_c$ s.t.

$$\Phi_c \leq \text{dom } a \circ b \cdot q_c \circ a \circ b$$

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

$$\Phi_c(n) = c + n + \text{the number of steps in the computation } \varphi_b(n) +$$

$$+ \text{the number of steps in the computation } \varphi_a[b(n)]$$

Now set

$$q_c(m) = c + q_b \circ q_a(m)$$

We only have to calculate:
\[ q_c \cdot a \cdot b(n) = c + q_b \cdot q_a \cdot a \cdot b(n) \geq \]
\[ \geq c + q_b \cdot \phi_a \left[ b(n) \right] = \]
\[ = c + q_b \left[ a + b(n) + \right. \]
\[ + \text{the number of steps in the computation } \varphi_a \left[ b(n) \right] \geq \]
\[ \geq c + a + q_b \cdot b(n) \geq \]
\[ + \text{the number of steps in the computation } \varphi_a \left[ b(n) \right] = \]
\[ = c + b + n + \]
\[ + \text{the number of steps in the computation } \varphi_b(n) + \]
\[ + \text{the number of steps in the computation } \varphi_a \left[ b(n) \right] \geq \]
\[ \geq c + n + \]
\[ + \text{the number of steps in the computation } \varphi_b(n) + \]
\[ + \text{the number of steps in the computation } \varphi_a \left[ b(n) \right] = \]
\[ = \phi_c(n) \]

q.e.d. \[ \Box \]

**Proof** of Lemma 7. Since \( a \) is cumulative there exists a \( \varphi \)-
index \( a \) for computing \( a \) s.t. \( a \equiv_x \Phi_a \) and in the sequel we can
deal with \( \Phi_a \) 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
\[ D_m = \left\{ n \in X \mid \Phi_a(n) < m \right\} \quad \text{and} \quad N_m = \left\{ n \in X \mid \Phi_a(n) = m \right\} \]

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

\[ W_m = \left\{ h \in \omega \mid \text{there exists an } n \in N_m \text{ s.t. } \Phi_h(n) \leq m = \Phi_a(n), \right. \\
\text{and } \Phi_h(n) = k(n) \text{ for each } n \in D_m \text{ s.t. } \Phi_h(n) \leq \Phi_a(n) \right\} \]

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

\[ k(n) = 1 - \varphi_{w_m}(n) \quad \text{for those } n \in N_m \text{ that satisfy } \Phi_{w_m}(n) \leq m \]

\[ k(n) = 0 \quad \text{for the remaining } n \in N_m \]

Finally go to Step \( m+1 \).

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

\[ \Phi_k \preceq_X \Phi_a \preceq_X a \]

Consider the set
\[ Z = \left\{ h \in \omega \mid \varphi_h(n) = k(n) \text{ for all } n \in X \text{ s.t. } \Phi_h(n) \leq \Phi_a(n), \right. \]
\[ \left. \text{ and } \Phi_h(n) \leq \Phi_a(n) \text{ for infinitely many } n \in X \right\} \]

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 \( n \in X \text{ s.t. } \varphi_h(n) = k(n) \) and \( \Phi_h(n) \leq \Phi_a(n) \), or there exists a \( j \in \omega \text{ s.t. the value of } k \text{ is defined during the first } j \text{ Steps on all } n \in X \text{ satisfying } \Phi_h(n) \leq \Phi_a(n) \). Now let \( J \in \omega \) be so large that for each \( h < h_0 \)

(i) there exists an \( n \in X \text{ s.t. } \varphi_h(n) = k(n) \) and \( \Phi_h(n) \leq \Phi_a(n) \leq J \), or

(ii) the value of \( k \) is defined during the first \( J \) Steps on all \( n \in X \text{ s.t. } \Phi_h(n) \leq \Phi_a(n) \)

Since we assumed that \( \Phi_{h_0}(n) \leq \Phi_a(n) \) for infinitely many \( n \in X \) there should be an \( n_0 \in X \text{ s.t. } \)

\[ J < \Phi_{h_0}(n_0) \leq \Phi_a(n_0) \]

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

Next imagine a \( \varphi \)-index \( i \) s.t. \( \varphi_i \equiv_X k \). Since \( i \notin Z \) the relation \( \Phi_i(n) \leq \Phi_a(n) \) can only hold for finitely many \( n \in X \) so

\[
\Phi_k \equiv_X \Phi_a \leq_X \Phi_i
\]

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


1990  Logic, Semantics and Philosophy of Language

LP-90-01 Jaap van der Does  A Generalized Quantifier Logic for Naked Infinitives
LP-90-02 Jeroen Groenendijk, Martin Stokhof  Dynamic Montague Grammar
LP-90-03 Renate Bartsch  Concept Formation and Concept Composition
LP-90-04 Anne Ranta  Intuitionistic Categorial Grammar
LP-90-05 Patrick Blackburn  Nominal Tense Logic
LP-90-06 Gennaro Chierchia  The Variability of Impersonal Subjects
LP-90-07 Gennaro Chierchia  Anaphora and Dynamic Logic
LP-90-08 Herman Hendriks  Flexible Montague Grammar
LP-90-09 Paul Dekker  The Scope of Negation in Discourse, towards a flexible dynamic Montague grammar
LP-90-10 Theo M.V. Janssen  Models for Discourse Markers
LP-90-11 Johan van Bentheim  General Dynamics
LP-90-12 Serge Lapierre  A Functional Partial Semantics for Intensional Logic
LP-90-13 Zhisheng Huang  Logics for Belief Dependence
LP-90-14 Jeroen Groenendijk, Martin Stokhof  Two Theories of Dynamic Semantics
LP-90-15 Maarten de Rijke  The Modal Logic of Inequality
LP-90-16 Zhisheng Huang, Karen Kwast  Awareness, Negation and Logical Omniscience
LP-90-17 Paul Dekker  Existential Disclosure, Implicit Arguments in Dynamic Semantics

Mathematical Logic and Foundations

ML-90-01 Harald Schellinx  Isomorphisms and Non-Isomorphisms of Graph Models
ML-90-02 Jaap van Oosten  A Semantical Proof of De Jongh's Theorem
ML-90-03 Yde Venema  Relational Games
ML-90-04 Maarten de Rijke  Unary Interpretability Logic
ML-90-05 Domenico Zambella  Sequences with Simple Initial Segments
ML-90-06 Jaap van Oosten  Extension of Lifschitz' Realizability to Higher Order Arithmetic, and a Solution to a Problem of F. Richman
ML-90-07 Maarten de Rijke  A Note on the Interpretability Logic of Finitely Axiomatized Theories
ML-90-08 Harold Schellinx  Some Syntactical Observations on Linear Logic
ML-90-09 Dick de Jongh, Duccio Pianigiani  Solution of a Problem of David Guaspari
ML-90-10 Michel van Lambalgen  Randomness in Set Theory
ML-90-11 Paul C. Gilmore  The Consistency of an Extended NaDSt
ML-90-12 John Tromp, Peter van Emde Boas  The Consistency of an Extended NaDSt
ML-90-13 Johan van Benthem, Peter van Emde Boas  Associative Storage Modification Machines
ML-90-14 Johan van Benthem, Peter van Emde Boas  The Consistency of an Extended NaDSt
ML-90-15 Joel Vieru  Unique Normal Forms for Combinatory Logic with Parallel Conditional: a Study in Computational Rewriting

Other Prepublications

X-90-01 A.S. Troelstra  Remarks on Intuitionism and the Philosophy of Mathematics, Revised Version
X-90-02 Maarten de Rijke  Some Chapters on Interpretability Logic
X-90-03 L.D. Beklemishev  On the Complexity of Arithmetic Interpretations of Modal Formulae
X-90-04 Y. Peter van Emde Boas  Annual Report 1989
X-90-05 Valentin Shehtman  Derived Sets in Euclidean Spaces and Modal Logic
X-90-06 Valentin Shehtman, Solomon Passy  Using the Universal Modality: Gains and Questions
X-90-07 V.Y. Shavrukov  The Lindenbaum Fixed Point Algebra is Undecidable
X-90-08 L.D. Beklemishev  Provability Logics for Natural Turing Progressions of Arithmetical Theories
X-90-09 V.Y. Shavrukov  On Rosser's Provability Predicate
X-90-10 Sieger van den Heuvel, Peter van Emde Boas  An Overview of the Rule Language RUL
X-90-11 Alessandra Carbone  Provably Fixed points in Δ0+Ω1 revisited
X-90-12 Maarten de Rijke  Bi-Unary Interpretability Logic
X-90-13 V.Y. Shavrukov  Arithmetic Completeness, Fixed Point Property, Craig's Property
X-90-14 L.A. Chagrova  Undecidable Problems in Correspondence Theory
X-90-15 A.S. Troelstra  Lectures on Linear Logic

1991  Logic, Semantics and Philosophy of Language

LP-91-01 Wiebe van der Hoek, Maarten de Rijke  Generalized Quantifiers and Modal Logic
LP-91-02 Frank Veltman  Defaults in Update Semantics
LP-91-03 Willem Groeneveld  Dynamic Semantics and Circular Propositions
LP-91-04 Makoto Kuzuhara  The Lambek calculus enriched with additional Connectives
ML-91-01 Yde Venema  Mathematical Logic and Foundations
ML-91-02 Alessandro Berarducci, Rineke Verbrugge  On the Metamathematics of Weak Theories
ML-91-03 Domenico Zambella  On the Proofs of Arithmetical Completeness for Interpretability Logic
ML-91-04 Raymond Hoofman, Harold Schellinx  Cylindric Modal Logic
ML-91-05 A.S. Troelstra  History of Constructivism in the Twentieth Century
ML-91-06 Inge Bethke  Finite Type Structures within Combinatory Algebras
ML-91-07 Yde Venema  Modal Derivation Rules
ML-91-08 Inge Bethke  Going Stable in Graph Models
ML-91-09 V.Y. Shavrukov  A Note on the Diagonizable Algebras of PA and ZF
CT-91-01 Ming Li, Paul M.B. Vitáň  Computation and Modal Logic
CT-91-02 Ming Li, John Tromp, Paul M.B. Vitáň  How to Share Concurrent Wait-Free Variables
CT-91-03 Ming Li, Paul M.B. Vitáň  Average Case Complexity under the Universal Distribution Equals Worst Case Complexity
CT-91-04 Sieger van den Heuvel, Karen Kwast  Weak Equivalence
CT-91-05 Sieger van den Heuvel, Karen Kwast  Weak Equivalence for Constraint Sets
CT-91-06 Edith Spaan  The Complete Database
CT-91-07 Karen L. Kwast  The Incomplete Database
CT-91-08 Kees Doets  Levitation Systems
CT-91-09 Ming Li, Paul M.B. Vitáň  Combinatorial Properties of Finite Sequences with high Kolmogorov complexity
CT-91-10 John Tromp, Paul Vitáň  A Randomized Algorithm for Two-Process Wait-Free Test-and-Set
CT-91-11 Lane A. Hemachandra, Edith Spaan  Quasi-Injective Reductions
CT-91-12 Alexander Chapoval, Michael Zacharyaschev  The Disjunction Property of Intermediate Propositional Logics
CT-91-13 Alexander Chapoval, Michael Zacharyaschev  On the Undecidability of the Disjunction Property of Intermediate Propositional Logics
CT-91-14 Alexander Chapoval, Michael Zacharyaschev  Canonical Formulas for K4, Part I: Basic Results
CT-91-15 Alexander Chapoval, Michael Zacharyaschev  The Horn Fragment of Linear Logic is NP-Complete
CT-91-16 Alexander Chapoval, Michael Zacharyaschev  The Multiplicative Fragment of Linear Logic is NP-Complete
CT-91-17 Alexander Chapoval, Michael Zacharyaschev  Subalgebras of Diagonizable Algebras of Theories containing Arithmetic
CT-91-18 Alexander Chapoval, Michael Zacharyaschev  Partial Conservativity and Modal Logics
X-91-01 Leon A. Hemachandra, Yde Venema  Quasi-Injective Reductions
X-91-02 Alexander Chagrov, Michael Zacharyaschev  The Disjunction Property of Intermediate Propositional Logics
X-91-03 V. Yu. Shavrukov  Subalgebras of Diagonizable Algebras of Theories containing Arithmetic
X-91-04 K.N. Ignatiev  Partial Conservativity and Modal Logics
X-91-05 Johan van Benthem  Temporal Logic
X-91-06 Annual Report 1990
X-91-07 A.S. Troelstra  Lectures on Linear Logic, Errata and Supplement
X-91-08 George Dzhaparidze  Logic of Tolerance
X-91-09 L.D. Beklemishev  On Bimodal Provability Logics for Pi1-1 axiomatized Extensions of Arithmetical Theories
X-91-10 Michel van Lambalgen  Independence, Randomness and the Axiom of Choice
X-91-11 Michael Zacharyaschev  Flexibilität der Schema-Syntax und Semantik: de proefschriften van Frans Zwarts en Michael Moortgat
X-91-12 Herman Hendriks  The Multiplicative Fragment of Linear Logic is NP-Complete
X-91-13 Max L. Kanovich  The Horn Fragment of Linear Logic is NP-Complete
X-91-14 Max L. Kanovich  The Multiplicative Fragment of Linear Logic is NP-Complete