Provability algebras and proof-theoretic ordinals

Lev D. Beklemishev

1.08.2002

Contents

1. Introduction

K. Gödel (31): T is consistent $\Rightarrow$ $T \nvdash \mathrm{Con}(T)$.
Holds for all reasonable T.

G. Gentzen (37):
$\mathrm{PA} +$ (transfinite ind. up to ε_0) $\vdash \mathrm{Con}(\mathrm{PA})$.
Specific for PA.

Ordinal $\varepsilon_0 = sup\{\omega, \omega^\omega, \dots\}$ is represented by an elementary well-ordering $\prec$ on $\mathbb{N}$.

- Transf. ind. depends on the formula representing $\prec$
- Con depends on the proof system

theory $\rightsquigarrow$ *ordinal (notation system)*

complex simple

- The problem of canonical ordinal notations
- General lack of canonicity. Category of proofs?
- Category of ordinal notation systems?

Ordinals with additional operations, like

$$(\varepsilon_0, <, 0, +, \omega^x)$$

What is the right notion of 'theory'?
What is the right choice of operations?

'Coordinate-free' proof theory?

Graded Provability Algebras

- Decent 'simple' structures
- Ordinal notation systems are canonically extractable
- Closely linked to the theories by 'arithmetical interpretation'
- Clear proof-theoretic analysis

Provability logic:

$$\underset{\text{complex}}{\textit{theory}} \quad \rightsquigarrow \quad \underset{\text{simple}}{\textit{provability logic}}$$

2. Background

Elementary arithmetic EA is formulated in the language $(0, 1, +, \cdot, 2^x, \leq, =)$ and has some minimal set of basic axioms defining these symbols plus the induction schema for bounded formulas.[1]

Peano arithmetic PA is EA with full induction:

$$\varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(x+1)) \to \forall x \varphi(x).$$

Σ_n-*formulas*: $\exists x_1 \forall x_2 \ldots \mathsf{Q} x_n \varphi(x_1, \ldots, x_n)$, with $\varphi(\vec{x})$ bounded.

$I\Sigma_n = \mathsf{EA} +$ induction for Σ_n-formulas

$$\mathsf{EA} \subset I\Sigma_1 \subset I\Sigma_2 \cdots \subset \mathsf{PA}$$

[1] EA is also known as $I\Delta_0 + \exp$ and EFA.

2.1. Lindenbaum Algebras

Lindenbaum algebra of T, the space of all T-independent sentences:

$\mathcal{L}_T = \{T\text{-sentences}\}/\sim_T$, where

$$\varphi \sim_T \psi \iff T \vdash \varphi \leftrightarrow \psi$$

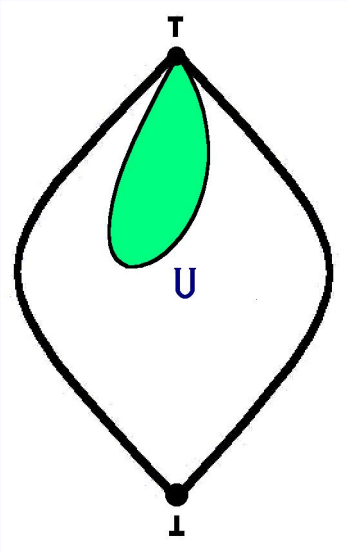
Ordering: $[\varphi] \leq [\psi] \iff T \vdash \varphi \to \psi$.
Boolean algebra with $\wedge$, $\vee$, $\neg$, $\top$, $\bot$.

Identities = boolean tautologies, like

$$x \vee \neg x = \top \qquad \varphi \vee \neg\varphi,$$
$$\neg\neg x = x \qquad \neg\neg\varphi \leftrightarrow \varphi,$$

Extension $T \subseteq U \longmapsto$ filter in $\mathcal{L}_T$.

$\mathcal{L}_U \simeq \mathcal{L}_T/U$.



Fact. T is consistent $\Rightarrow$ $\mathcal{L}_T$ is dense.

$$x < y \Rightarrow \exists z \; x < z < y$$

(Follows from Rosser's theorem.)

Fact. $\mathcal{A}$, $\mathcal{B}$ countable, dense $\Rightarrow$ $\mathcal{A} \simeq \mathcal{B}$.
Hence $\mathcal{L}_T \simeq \mathcal{L}_U$, for all reasonable T, U.
(By Pour-El and Kripke, even recursively isomorphic.)

How to enrich the structure of Lindenbaum algebras?
Cylindric algebras $\rightsquigarrow$ difficulties.

2.2. Provability algebras

R. Magari[2] [Mag75], F. Montagna [Mon75], V. Shavrukov [Sha93, Sha97]

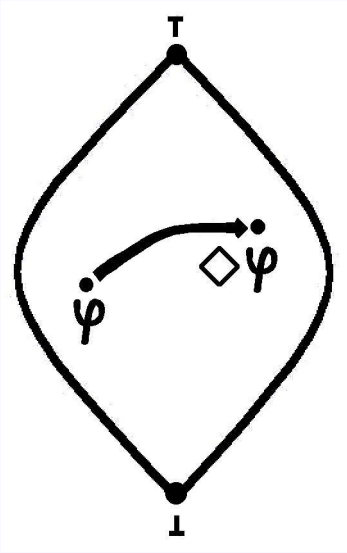
Consistency operator $\Diamond : \mathcal{L}_T \longrightarrow \mathcal{L}_T$

$$\varphi \longmapsto \mathrm{Con}(T + \varphi)$$

$(\mathcal{L}_T, \Diamond) =$ *the provability algebra of* T

$\Box\varphi = \neg\Diamond\neg\varphi =$ "φ is T-provable"

Gödel 2nd: $\varphi \neq \bot \Rightarrow \varphi \not\leq \Diamond\varphi$.



[2] provability algebras = Magari algebras, diagonalizable algebras

Modal logic = propositional logic with $\Box, \Diamond$.
Identities of $\mathcal{L}_T$ = *the provability logic of* T

GL (Gödel–Löb logic)

1. boolean tautologies
2. $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$
3. $\Box\varphi \to \Box\Box\varphi$
4. $\Box(\Box\varphi \to \varphi) \to \Box\varphi$

Rules: modus ponens, $\varphi \vdash \Box\varphi$.

Decidable, fmp, Craig interpolation, ...

More on provability logics see [Boo93, Smo85].

R. Solovay [Sol76]:

$$\mathbf{GL} \vdash \varphi(\vec{x}) \iff (\mathcal{L}_T, \Box) \vDash \forall \vec{x}\, (\varphi(\vec{x}) = \top).$$

K. Segerberg [Seg71]: **GL** is sound and complete for the class of converse well-founded Kripke frames.

2.3. Graded provability algebras

$\mathcal{L}_T$ is stratified by the quantifier complexity levels:

$$\Pi_1 \subseteq \Pi_2 \subseteq \ldots, \qquad \bigcup_{i\geq 1} \Pi_i = \mathcal{L}_T$$

n-Consistency:
$n\text{-}\mathrm{Con}(U) =$ "$(U +$ all true $\Pi_n)$ is consistent"

$$\langle n \rangle : \varphi \longmapsto n\text{-}\mathrm{Con}(T + \varphi)$$

$\Box = [0], \ [n] = \neg\langle n \rangle \neg$ (n-provability)

Notice that $\langle n \rangle \varphi$ is Π_{n+1} for any φ.

Graded provability algebra of T:

$$\mathcal{M}_T = (\mathcal{L}_T, \langle 0 \rangle, \langle 1 \rangle, \dots).$$

Identities (Japaridze [Jap85]):

GLP

1. **GL** for each $[n]$
2. $[n]\varphi \to [n+1]\varphi$
3. $\langle n \rangle \varphi \to [n+1]\langle n \rangle \varphi$

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

Lem. 1. [Σ_{n+1}-completeness] For $\varphi \in \Sigma_{n+1}$,

$$\mathsf{EA} \vdash \forall x\, (\varphi(x) \to [n]_T \varphi(\dot{x})).$$

Proof. If $\exists y \psi(y, k)$ is true, then for some m, $\psi(m, k)$ is true Π_n. Hence, $\psi(\bar{m}, \bar{k})$ is n-provable. $\exists y \psi(y, \bar{k})$ follows.

Lem. 2. [Reflection] Over EA,

$$n\text{-}\mathrm{Con}(T) \equiv \{\forall x(\Box_T \varphi(\dot{x}) \to \varphi(x)) : \varphi \in \Pi_{n+1}\}.$$

Proof. $(\Rightarrow)$ If $\varphi \in \Pi_{n+1}$ is false, then $\neg\varphi$ is true Σ_{n+1}. Hence, $[n]\neg\varphi$. Therefore $\Box\varphi$ implies $[n](\varphi \wedge \neg\varphi)$, that is, $[n]\bot$.

$(\Leftarrow)$ If $[n]\bot$, then for some true $\pi \in \Pi_n$, $\Box\neg\pi$. Take $\varphi(x) := \neg\mathsf{True}_{\Pi_n}(x)$ so that

$$\mathsf{EA} \vdash \pi \leftrightarrow \mathsf{True}_{\Pi_n}(\ulcorner\pi\urcorner).$$

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

2.4. Reduction property

(generalizes U. Schmerl [Sch79])

Π_{n+1}-*conservativity* relation between filters:

$$U \equiv_n V \Leftrightarrow \forall \pi \in \Pi_{n+1}(\pi \in U \Leftrightarrow \pi \in V)$$

Th. 1. Assume T is Π_{n+2}-axiomatized. Then in $\mathcal{M}_T$

$$\{\langle n+1\rangle\varphi\} \equiv_n \{\langle n\rangle\varphi, \langle n\rangle(\varphi \wedge \langle n\rangle\varphi), \dots\}$$

Proof: formalizable in $\mathsf{EA}^+ = \mathsf{EA} + 1\text{-}\mathrm{Con}(\mathsf{EA})$.

Ex. 1. $\langle 2\rangle\top \equiv_1 \{\langle 1\rangle\top, \langle 1\rangle\langle 1\rangle\top, \dots\}$.

Consistency ordering:

$$\psi <_0 \varphi \Leftrightarrow T \vdash \varphi \to \Diamond\psi.$$

Define: if $\alpha = \langle n+1 \rangle \varphi$, then

$$\alpha[\![k]\!] := \underbrace{\langle n \rangle(\varphi \wedge \langle n \rangle(\varphi \wedge \ldots))}_{k \text{ times}}$$

Cor. 3. $\vdash \alpha \to \Diamond\psi \Rightarrow \exists k : \vdash \alpha[\![k]\!] \to \Diamond\psi$,
hence $\alpha[\![0]\!] <_0 \alpha[\![1]\!] <_0 \ldots \longrightarrow \alpha$

3. Consistency proof for PA

3.1. An algebraic view of ε_0

Work in **GLP**.

Let S be generated from $\top$ by $\langle 0\rangle$, $\langle 1\rangle$, $\ldots$

$$\alpha = \langle n_1\rangle\langle n_2\rangle\ldots\langle n_k\rangle\top$$

We identify S with words

$$\alpha = n_1 n_2 \ldots n_k$$

S_n is the restriction of S to the alphabet $\{n, n{+}1, \ldots\}$.

Th. 2. $(S, <_0)$ is well-founded of height ε_0.
Modulo $\sim_{\mathbf{GLP}}$ the ordering is linear.

Proof: purely in **GLP**. The ordinal $o(0^k) = k$.
If $\alpha = \alpha_1 0 \alpha_2 0 \cdots 0 \alpha_n$, then

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

where $(132)^- = 021$.

Ex. 2. $o(2101) = \omega^{o(0)} + \omega^{o(10)} = \omega + \omega^{\omega^0 + \omega^1} = \omega^\omega$

$$2101 \sim_{\mathbf{GLP}} 2$$

Let α^* denote the interpretation of $\alpha \in S$ in $\mathcal{M}_T$. Notice that

$$\textbf{GLP} \vdash \alpha \leftrightarrow \beta \Rightarrow \mathcal{M}_T \vDash \alpha^* = \beta^*$$

The converse also holds, provided T is sound (i.e., true).

K. Ignatiev [Ign93]: normal forms for the letterless fragment of **GLP**. Interpretations of letterless formulas constitute the *prime subalgebra* $\mathcal{P} \subset \mathcal{M}_T$.

Th. 3. [Ignatiev] Suppose T is sound. On $\mathcal{P} \setminus \{\bot\}$ the ordering $<_0$ is well-founded of height ε_0.

Technically, we do not need this result, but it shows that ε_0 is an intrinsic *characteristic* of the algebra $\mathcal{M}_T$.

3.2. A closure property of S

Lem. 4. 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):

$$\begin{aligned} \langle n\rangle\varphi \wedge \langle m\rangle\psi &\to [n]\langle m\rangle\psi \quad \text{by Axiom 3} \\ &\to \langle n\rangle(\varphi \wedge \langle m\rangle\psi) \end{aligned}$$

Statement (ii) follows by repeated application of (i). Statement (iii) is axiom $[m]\varphi \to [m][m]\varphi$ of **GL**.

Lem. 5. $\alpha = \langle n+1 \rangle \varphi \in S \;\Rightarrow\; \exists \beta \in S \vdash \beta \leftrightarrow \alpha[\![k]\!]$.

Proof: by induction on k. For $k = 0$ we have $\alpha[\![0]\!] = \langle n \rangle \varphi \in S$.

Write $\alpha[\![k]\!] \in S$ in the form $n\gamma m\beta$, where $\gamma \in S_{n+1}$ and $m \leq n$.

$$\begin{aligned} \alpha[\![k+1]\!] &\leftrightarrow \langle n \rangle (\gamma m\beta \wedge n\gamma m\beta) \\ &\leftrightarrow \langle n \rangle (\gamma (m\beta \wedge n\gamma m\beta)) \quad \text{by Lem.4(i)} \\ &\leftrightarrow \langle n \rangle (\gamma n\gamma m\beta) \quad \text{by Lem.4(iii)} \end{aligned}$$

Cor. 6. For any k, $\vdash \alpha[\![k]\!] \leftrightarrow (n\gamma)^{k+1} m\beta$.

Operations on ordinals vs. operations of the algebra

- ω^α corresponds to α^+ (not in the signature of the algebra!).
- $\alpha + n$ is $0^n\alpha$.
- $\alpha + \beta$ is $\beta 0 \alpha$, if $\beta \geq \omega$.
- Conjunction of ordinals: $o(\alpha \wedge \beta) = ?$

$$2 \wedge 12 = 212, \quad \omega^\omega \wedge \omega^{\omega+1} = \omega^{\omega+\omega}$$

3.3. Embedding of PA into $\mathcal{M}_{\mathsf{EA}}$

Lem. 7. [Kreisel] $\mathsf{PA} \equiv \{\langle n\rangle\top : n < \omega\}$

Proof. ($\subseteq$) Let $P := \varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(x+1))$.
Obviously, $\forall n\ \mathsf{EA} \vdash P \to \varphi(\bar{n})$, so

$$\mathsf{EA} \vdash \forall x\, \Box(P \to \varphi(\dot{x})).$$

By Lem. 2 $\langle n\rangle\top$ implies $\forall x\,(P \to \varphi(\dot{x}))$, where n is the complexity of $P \to \varphi$.

($\supseteq$) Assume $\Box\varphi(\dot{x})$. There is a cut-free proof of φ. Prove that all formulas in the proof are true by induction on depth.

Cor. 8. $\mathsf{EA}^+ \vdash \forall n \Diamond\langle n\rangle\top \leftrightarrow \mathsf{Con}(\mathsf{PA})$.

3.4. Consistency proof

Work in $\mathcal{M}_{\mathsf{EA}}$. We claim:

$$\mathsf{EA}^+ \vdash \forall\beta <_0 \alpha \, \Diamond\beta^* \to \Diamond\alpha^*.$$

Assume $\forall\beta <_0 \alpha \, \Diamond\beta^*$.

If $\alpha = 0\beta$, then $\Diamond\beta^*$, hence $\Diamond\Diamond\beta^*$ using $\langle 1\rangle\top$.

If $\alpha = \langle n{+}1\rangle\beta$, then $\forall k \Diamond\alpha[\![k]\!]^*$, because $\alpha[\![k]\!] <_0 \alpha$.

By Reduction (provably in EA^+)

$$\alpha^* \equiv_n \{\alpha[\![k]\!]^* : k < \omega\}.$$

Therefore $\forall k \, \Diamond\alpha[\![k]\!]^*$ yields $\Diamond\alpha^*$.

So, $\mathsf{EA}^+ + (S, <_0)$-induction $\vdash \forall\alpha \in S \Diamond\alpha^*$
$\vdash \mathsf{Con}(\mathsf{PA})$ by Cor.8
END

De facto we apply $(S, <_0)$-induction rule for Π_1-formula $\varphi(\alpha) := \Diamond\alpha^*$ once:

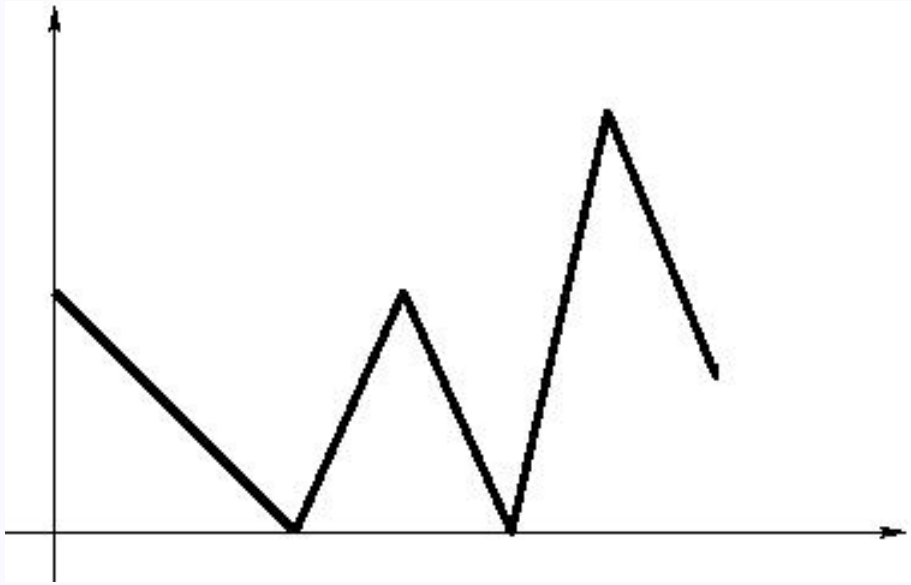
$$\frac{\forall\beta <_0 \alpha\ \varphi(\beta) \to \varphi(\alpha)}{\forall\alpha\varphi(\alpha)}$$

Th. 4. $\mathsf{EA}^+ +$ $(S, <_0)$-induction rule for Π_1-formulas is equivalent to

$$\mathsf{EA}^+ + \mathsf{Con}(\mathsf{PA}) + \mathsf{Con}(\mathsf{PA} + \mathsf{Con}(\mathsf{PA})) + \ldots$$

4. The Worm Principle

Worm is a function $f : [0, n] \to \mathbb{N}$.
List: $w = (f(0), f(1), \ldots, f(n))$
Word: $w = 2102031$



4.1. Rules of the game

First define a function $\mathrm{next}(w, m)$:

1. If $f(n) = 0$ then
   $\mathrm{next}(w, m) := (f(0), \ldots, f(n-1))$.
2. If $f(n) > 0$ let $k := \max_{i<n} f(i) < f(n)$;
   $r := (f(0), \ldots, f(k))$;
   $s := (f(k+1), \ldots, f(n-1), f(n) - 1)$;
   $\mathrm{next}(w, m) := r * \underbrace{s * s * \cdots * s}_{m+1 \text{ times}}$.

$\mathrm{next}(2102031, 1) = 210203030$
$k = 4$; $r = 21020$; $s = 30$.

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

$$w_0 = 2102031$$
$$w_1 = 210203030$$
$$w_2 = 21020303$$
$$w_3 = 21020302222$$
$$w_4 = 2102030222122212221221221221$$
$$w_5 = 2102030(2221222122212221222 20)^6$$
$$\ldots$$

Notice that w_n is an elementary function.

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

Every Worm Dies $\Leftrightarrow \forall w \exists n\, w_n = \varnothing$

Th. 5. *EWD is true but unprovable in* PA.

Th. 6. *EWD is* EA*-equivalent to* $1\text{-}\mathrm{Con}(\mathsf{PA})$.

$1\text{-}\mathrm{Con}(T)$ means "$(T +$ all true $\Pi^0_1)$ *is consistent*"

4.2. Validity of EWD

To prove: $\mathsf{EA} + 1\text{-}\mathrm{Con}(\mathsf{PA}) \vdash \mathsf{EWD}$.

Work in $\mathcal{M}_{\mathsf{EA}}$. Shift the interpretation of worms:

$$\begin{aligned} 0 &\mapsto \langle 1 \rangle \\ 1 &\mapsto \langle 2 \rangle \\ &\dots \end{aligned}$$

Let α be the inverse of w. Then $w^\star = (\alpha^+)^*$, where $(132)^+ = 243$.

Thus, $(103)^\star = \langle 4 \rangle \langle 1 \rangle \langle 2 \rangle \top$

Plan of the proof

Lem. 9. For any w, PA $\vdash w^\star$.

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

$$\begin{aligned} \text{EA} \vdash v^\star \wedge \langle m+1 \rangle \top &\rightarrow \langle m+1 \rangle v^\star \quad \text{by Lem. 4} \\ &\rightarrow \langle n+1 \rangle v^\star \end{aligned}$$

By Lem. 7 and the induction hypothesis

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

Lem. 10. For any w,

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

Proof. It is sufficient to prove

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

Let α be the converse of w. By Cor. 6, $\alpha[\![n]\!]$ is the converse of $\mathrm{next}(w,n)$.

$$\alpha \neq \varnothing \ \Rightarrow\ \mathbf{GLP} \vdash \alpha \to \Diamond\alpha[\![n]\!]$$

GLP is stable under $(\cdot)^+$, so

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

Lem. 11. EA $\vdash \langle 1\rangle w_0^\star \to \exists n\, w_n = \varnothing$

Proof. We prove $\forall n\, w_n \neq \varnothing \to \forall n\, [1]\neg w_n^\star$ using Löb.

$$\begin{aligned}
\forall n\, w_n \neq \varnothing \wedge [1]\forall n[1]\neg w_n^\star &\to [1]\forall n[1]\neg w_{n+1}^\star \\
&\to \forall n[1][1]\neg w_{n+1}^\star \\
&\to \forall n[1]\neg w_n^\star \text{ by Lem. 10}
\end{aligned}$$

$$\begin{aligned}
[1]\forall n\, w_n \neq \varnothing &\to [1]([1]\forall n[1]\neg w_n^\star \to \forall n[1]\neg w_n^\star) \\
&\to [1]\forall n[1]\neg w_n^\star \text{ by Löb}
\end{aligned}$$

$$\begin{aligned}
\forall n\, w_n \neq \varnothing &\to [1]\forall n\, w_n \neq \varnothing \text{ by } \Sigma_2\text{-compl.} \\
&\to [1]\forall n[1]\neg w_n^\star \\
&\to \forall n[1]\neg w_n^\star
\end{aligned}$$

4.3. The proof

From Lemmas 9 and 11 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, provably in EA,

$$\forall w\ \mathsf{PA} \vdash \exists n\, w_n = \varnothing.$$

So, $1\text{-}\mathrm{Con}(\mathsf{PA})$ implies $\forall w \exists n\, w_n = \varnothing$.

EWD

4.4. Independence of EWD

Let $w[\![n]\!] := \mathrm{next}(w, n)$ and

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

Let $h_w(n)$ be the smallest k such that

$$w[\![n \ldots n+k]\!] = \varnothing.$$

Some properties of h:

Lem. 12. $h_{u0v}(n) = h_u(h_v(n)+1) + h_v(n) + 1$

Proof: $u0v \twoheadrightarrow u0 \twoheadrightarrow \varnothing$.

Cor. 13. If $w \in S_1$, then $h_{w1}(n) > h_w^{(n)}(n)$.

Proof: $w1[\![n]\!] = w0w0 \ldots w0$.

Let $v \trianglelefteq u$ iff $v = u[\![0]\!][\![0]\!] \ldots [\![0]\!]$.

Lem. 14. If $h_w(m)\downarrow$ and $u \trianglelefteq w$, then

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

Proof. The n-th letter in w can only change if all letters to the right of it are deleted.

Cor. 15. $\forall m \leq n \; \exists k \; w[\![n \ldots n+k]\!] = w[\![m]\!]$.

Lem. 16. If $v \trianglelefteq u$ and $x \leq y$ then $h_v(x) \leq h_u(y)$.

Proof. Repeating Cor. 15 obtain $s_0, s_1, \ldots$ s.t.

$$\begin{aligned} u[\![y \ldots y+s_0]\!] &= v[\![x]\!] \\ u[\![y \ldots y+s_0+s_1]\!] &= v[\![x]\!][\![x+1]\!] \\ &\ldots \end{aligned}$$

Let $h_w\downarrow := (\forall x \exists y\, h_w(x) = y)$.

Lem. 17. EA $\vdash \forall w \in S_1\, (h_{1111w}\downarrow \to \langle 1\rangle w^\star)$.

Proof of the independence of EWD:

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

We use additional general fact (to be proved later):

Th. If f is provably increasing, has an el. graph and $f(x) > 2^x$, then

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

Proof of Lem. 17: $\forall w \in S_1\ (h_{1111w}\downarrow \to \langle 1\rangle w^\star)$.

By Löb we can use as an additional assumption

$$\forall w \in S_1\ [1](h_{1111w}\downarrow \to \langle 1\rangle w^\star).$$

If $1111w = v1$, then $h_{v1}\downarrow \to \lambda x.h_v^{(x)}(x)\downarrow$.
Since h_v is increasing, has an elementary graph and grows at least exponentially,

$$\begin{aligned} \lambda x.h_v^{(x)}(x)\downarrow &\to \langle 1\rangle h_v\downarrow \\ &\to \langle 1\rangle\langle 1\rangle v^\star \\ &\to \langle 1\rangle w^\star \end{aligned}$$

If $1111w = v$ ends with $m > 1$, then

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

Fix n. If $x \leq n$, then $h_{v[\![n]\!]}(x) \leq h_{v[\![n]\!]}(n+1)$.

If $x \geq n$, then $h_{v[\![n]\!]}(x) \leq h_{v[\![x]\!]}(x+1)$.

$$\begin{aligned} \forall n\ h_{v[\![n+1]\!]}\downarrow &\to \forall n\ h_{v[\![n]\!]1}\downarrow \quad \text{as } v[\![n]\!]1 \trianglelefteq v[\![n+1]\!] \\ &\to \forall n\ \langle 1\rangle h_{v[\![n]\!]}\downarrow \quad \text{as before} \\ &\to \forall n\ \langle 1\rangle\langle 1\rangle w[\![n]\!]^\star \\ &\to \langle 1\rangle w^\star \text{ by Reduction} \end{aligned}$$

5. Proof-theoretic analysis

5.1. Provably total computable functions

Let $\mathcal{F}(T)$ be the class of *provably total computable functions* of a theory T.

Def. 1. $g \in \mathcal{F}(T)$ *iff for some* $\varphi(x, y) \in \Sigma_1$,

(i) $g(x) = y \Leftrightarrow \mathbb{N} \vDash \varphi(x, y)$

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

Examples. $\mathcal{F}(\mathsf{EA}) = \mathcal{E}$ (elementary functions)
$\mathcal{F}(I\Sigma_1) =$ primitive rec. functions (Parsons 70)
$\mathcal{F}(\mathsf{PA}) = \ < \varepsilon_0$-recursive functions (Ackermann 44)

In general,

- $\mathcal{F}(T) \supseteq \mathcal{E}$ and closed under composition
- $\mathcal{F}(T)$ only depends on the Π_2-fragment of T
- $\mathcal{F}(T) = \mathcal{F}(T + \mathbf{Th}_{\Pi_1}(\mathbb{N}))$

$$f \leq_c g \iff f \text{ is obtained from } \mathcal{E} \cup \{g\} \text{ by composition}$$

Lem. 18. Let g have an elementary graph. Then

$$f \in \mathcal{F}(\mathsf{EA} + g{\downarrow}) \iff f \leq_c g.$$

Proof: follows from Herbrand theorem.

Internal indexing

Def. 2. 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* $\forall x \exists y \varphi_{e_1}(x) = y$

Universal function: $\psi_e(x) := \varphi_{e_1}(x)$.

Jump: $\mathcal{F}(T)' :=$ closure under composition of

$$\mathcal{F}(T) \cup \{\psi\}.$$

Lem. 19. $\mathsf{EA} \vdash \forall e, x \exists y\, \psi_e(x) = y \leftrightarrow 1\text{-}\mathrm{Con}(T)$

Proof. The formulas are basically the same:

$$\forall e_1, e_2, x\, (\mathsf{Prf}_T(e_2, \ulcorner \forall x \exists y \varphi_{e_1}(x) = y \urcorner) \to \exists y \varphi_{e_1}(x) = y).$$

Cor. 20. $\mathcal{F}(\mathsf{EA} + 1\text{-}\mathrm{Con}(T)) = \mathcal{F}(T)'$

In EA^+: $\langle e_1, e_2 \rangle \leftrightsquigarrow$ term, so the internal indexing is equivalent to the Gödel numbering of terms.

Th. 7. If f is provably increasing, has an el. graph and $f(x) > 2^x$, then

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

Proof. By monotonicity every function $\leq_c f$ is bounded by a fixed iterate of f. Hence, $\lambda x.f^{(x)}(x)\downarrow$ iff $\psi\downarrow$.

5.2. Proof-theoretic analysis

theories $\rightsquigarrow$ ordinals

Π^1_1-**analysis:** Provable well-orderings

$$|S|_{\Pi^1_1} := \sup\{|\prec| : S \vdash WF(\prec)\}.$$

Π^0_2-**analysis:** Provably total computable functions

$$S \rightsquigarrow \mathcal{F}(S) \rightsquigarrow \mathcal{E}_\alpha$$

$$\mathcal{E}_\alpha := \mathbf{E}(\{F_\beta : \beta < \alpha\})$$

$$\begin{cases} F_0(x) & := x+1 \\ F_{\alpha+1}(x) & := F_\alpha^{(x+1)}(x) \\ F_\alpha(x) & := F_{\alpha[\![x]\!]}(x), \quad \text{if } \alpha \text{ is a limit ordinal.} \end{cases}$$

$$|S|_{\Pi^0_2} := \min\{\alpha : S \nvdash \forall x \exists y\, F_\alpha(x) = y\}$$

Ex. 3. $|\mathsf{PA} + \mathit{EWD}|_{\Pi^1_1} = |\mathsf{PA}|_{\Pi^1_1} = \varepsilon_0$

Ex. 4. $|\mathsf{PA} + \mathsf{Con}(\mathsf{PA})|_{\Pi^0_2} = |\mathsf{PA}|_{\Pi^0_2} = \varepsilon_0$

Π^1_1-ordinal is insensitive to true Σ^1_1 axioms.
Π^0_2-ordinal is insensitive to true Π^0_1 axioms.

Π^0_1-analysis: Iterated consistency assertions

$$|S|_{\Pi^0_1} := \min\{\alpha : S \nvdash \mathsf{Con}(\mathsf{EA}_\alpha)\}.$$

$$T_0 := T; \quad T_{\alpha+1} := T_\alpha + \mathsf{Con}(T_\alpha); \quad T_\alpha := \bigcup_{\beta<\alpha} T_\beta$$

Ex. 5.

$|\mathsf{PA} + \mathsf{Con}(\mathsf{PA})|_{\Pi^0_1} = \varepsilon_0 \cdot 2$ $\quad |I\Sigma_1 + \mathsf{Con}(\mathsf{PA})|_{\Pi^0_1} = \varepsilon_0 + \omega^\omega$

$|\mathsf{PA} + \mathit{EWD}|_{\Pi^0_1} = \varepsilon_0^2$ $\quad |\mathsf{PA} + \mathit{EWD}|_{\Pi^0_2} = \varepsilon_0 \cdot 2$

5.3. Analysis by iterated consistency

S_n is the fragment of S in the language with $\langle n \rangle$, $\langle n{+}1 \rangle$, $\ldots$ equipped with the ordering

$$\varphi <_n \psi \Leftrightarrow \textbf{GLP} \vdash \psi \to \langle n \rangle \varphi.$$

Def. 3. $T^n_\alpha \equiv T + \{n\text{-}\mathit{Con}(T^n_\beta) : \beta <_n \alpha, \beta \in S_n\}$

Theories T^n_α are uniquely defined for $\alpha \in S_n$.

Th. 8. If T is Π_{n+1} axiomatized, then (provably in EA^+)

$$\forall \alpha \in S_n,\ T + \alpha^* \equiv_n T^n_\alpha.$$

Proof: reduction + Löb.

Cor. 21. $\mathsf{PA} \equiv_n \bigcup_\alpha (\mathsf{EA}^+)^n_\alpha$

Lem. 22. $\mathcal{F}(\mathsf{EA}^1_\alpha) = \mathcal{E}_\alpha$, where $\mathcal{E}_\alpha$ is the α-th class of the fast growing hierarchy.

Proof: an extension of Theorem 7.

Hence: analysis by iterated 1-consistency yields the same information as the usual Π^0_2-analysis.

Cor. 23. $\mathcal{F}(\mathsf{PA}) = \bigcup_\alpha \mathcal{E}_\alpha$

Ex. 6. $|\mathsf{PA} + \mathsf{EWD}|_{\Pi^0_2} = \varepsilon_0 \cdot 2$.

Proof. Consider $T := \mathsf{EA} + \mathsf{EWD}$. Work in $\mathcal{M}_T$. We have

$$\mathsf{PA} + \mathsf{EWD} = \{\langle n \rangle \top : n < \omega\}.$$

Reduction property holds in $\mathcal{M}_T$, as T is Π_2. Hence,

$$\begin{aligned} \mathsf{PA} + \mathsf{EWD} &\equiv_1 T^1_{\varepsilon_0} \\ &\equiv_1 (\mathsf{EA}^1_{\varepsilon_0+1})^1_{\varepsilon_0} \\ &\equiv_1 \mathsf{EA}^1_{\varepsilon_0 \cdot 2} \end{aligned}$$

Open questions

1. Generalizations of graded provability algebras for stronger theories: RA, KP_ω, ...

2. A general argument for the well-foundedness of GPA.

3. New combinatorial independent principles from Kripke models?

4. Infinitely generated filters on GPA, regularity, automata.

5. Is the elementary theory of the prime subalgebra of $\mathcal{M}_T$ decidable?

References

[Boo93] G. Boolos. *The Logic of Provability*. Cambridge University Press, Cambridge, 1993.

[Ign93] K.N. Ignatiev. On strong provability predicates and the associated modal logics. *Journal of Symbolic Logic*, 58:249–290, 1993.

[Jap85] G.K. Japaridze. The polymodal logic of provability. In *Intensional Logics and Logical Structure of Theories: Material from the fourth Soviet–Finnish Symposium on Logic, Telavi*, pages 16–48. Metsniereba, Tbilisi, 1985. In Russian.

[Mag75] R. Magari. The diagonalizable algebras (the algebraization of the theories which express Theor.:II). *Bollettino della Unione Matematica Italiana,* Serie 4, 12, 1975. Suppl. fasc. 3, 117–125.

[Mon75] F. Montagna. On the diagonalizable algebra of Peano arithmetic. *Bollettino della Unione Matematica Italiana,* B (5), 16:795–812, 1975.

[Sch79] U.R. Schmerl. A fine structure generated by reflection formulas over Primitive Recursive Arithmetic. In M. Boffa, D. van Dalen, and K. McAloon, editors, *Logic Colloquium'78*, pages 335–350. North Holland, Amsterdam, 1979.

[Seg71] K. Segerberg. *An essay in classical modal logic*. Filosofiska Föreningen och Filosofiska Institutionen vid Uppsala Universitet, Uppsala, 1971.

[Sha93] V.Yu. Shavrukov. Subalgebras of diagonalizable algebras of theories containing arithmetic. *Dissertationes Mathematicae*, 323, 1993.

[Sha97] V.Yu. Shavrukov. Undecidability in diagonalizable algebras. *Journal of Symbolic Logic*, 62(2):79–116, 1997.

[Smo85] C. Smoryński. *Self-Reference and Modal Logic*. Springer-Verlag, Berlin, 1985.

[Sol76] R.M. Solovay. Provability interpretations of modal logic. *Israel Journal of Mathematics*, 28:33–71, 1976.