Institute for Language, Logic and Information

A SEMANTICAL PROOF OF DE JONGH'S THEOREM

Jaap van Oosten

ITLI Prepublication Series
for Mathematical Logic and Foundations ML-90-02

University of Amsterdam

The ITLI Prepublication Series

1986
86-01 The Institute of Language, Logic and Information
86-02 Peter van Emde Boas — A Semantical Model for Integration and Modularization of Rules
86-03 Johan van Benthem — Categorial Grammar and Lambda Calculus
86-04 Reinhard Muskens — A Relational Formulation of the Theory of Types
86-05 Kenneth A. Bowen, Dick de Jongh — Some Complete Logics for Branched Time, Part I Well-founded Time,
86-06 Johan van Benthem — Logical Syntax — Forward looking Operators

1987
87-01 Jeroen Groenendijk, Martin Stokhof — Type shifting Rules and the Semantics of Interrogatives
87-02 Renate Bartsch — Frame Representations and Discourse Representations
87-03 Jan Willem Klop, Roel de Vrijer — Unique Normal Forms for Lambda Calculus with Surjective Pairing
87-04 Johan van Benthem — Polyadic quantifiers
87-05 Víctor Sánchez Valencia — Traditional Logicians and de Morgan's Example
87-06 Eleonore Oversteegen — Temporal Adverbials in the Two Track Theory of Time
87-07 Johan van Benthem — Categorial Grammar and Type Theory
87-08 Renate Bartsch — The Construction of Properties under Perspectives
87-09 Herman Hendriks — Type Change in Semantics: The Scope of Quantification and Coordination

1988
Logic, Semantics and Philosophy of Language:
LP-88-01 Michiel van Lambalgen — Algorithmic Information Theory
LP-88-02 Yde Venema — Expressiveness and Completeness of an Interval Tense Logic
LP-88-03 — Year Report 1987
LP-88-04 Reinhard Muskens — Going partial in Montague Grammar
LP-88-05 Johan van Benthem — Logical Constants across Varying Types
LP-88-06 Johan van Benthem — Semantic Parallels in Natural Language and Computation
LP-88-07 Renate Bartsch — Tenses, Aspects, and their Scopes in Discourse
LP-88-08 Jeroen Groenendijk, Martin Stokhof — Context and Information in Dynamic Semantics
LP-88-09 Theo M.V. Janssen — A mathematical model for the CAT framework of Eurotra
LP-88-10 Anneke Kleppe — A Blissymbolics Translation Program

Mathematical Logic and Foundations:
ML-88-01 Jaap van Oosten — Lifschitz' Realizabiility
ML-88-02 M.D.G. Swaen — The Arithmetical Fragment of Martin Löf's Type Theories with weak Σ-elimination
ML-88-03 Dick de Jongh, Frank Veltman — Provability Logics for Relative Interpretability
ML-88-04 A.S. Troelstra — On the Early History of Intuitionistic Logic
ML-88-05 A.S. Troelstra — Remarks on Intuitionism and the Philosophy of Mathematics

Computation and Complexity Theory:
CT-88-01 Ming Li, Paul M.B.Vitanyi — Two Decades of Applied Kolmogorov Complexity
CT-88-02 Michiel H.M. Smid — General Lower Bounds for the Partitioning of Range Trees
CT-88-03 Michiel H.M. Smid, Mark H. Overmars, Leen Torenvliet, Peter van Emde Boas — Maintaining Multiple Representations of Dynamic Data Structures
CT-88-04 Dick de Jongh, Lex Hendriks, Gerard R. Renardel de Lavalette — Computations in Fragments of Intuitionistic Propositional Logic
CT-88-05 Peter van Emde Boas — Machine Models and Simulations (revised version)
CT-88-06 Michiel H.M. Smid — A Data Structure for the Union-find Problem having good Single-Operation Complexity
CT-88-07 Johan van Benthem — Time, Logic and Computation
CT-88-08 Michiel H.M. Smid, Mark H. Overmars, Leen Torenvliet, Peter van Emde Boas — Multiple Representations of Dynamic Data Structures
CT-88-09 Theo M.V. Janssen — Towards a Universal Parsing Algorithm for Functional Grammar
CT-88-10 Edith Spaan, Leen Torenvliet, Peter van Emde Boas — Nondeterminism, Fairness and a Fundamental Analogy
CT-88-11 Sieger van Denneheuvel, Peter van Emde Boas — Towards implementing RL

Other prepublications:
X-88-01 Marc Jumelet — On Solovay's Completeness Theorem

1989
Logic, Semantics and Philosophy of Language:
LP-89-01 Johan van Benthem — The Fine-Structure of Categorial Semantics
LP-89-02 Jeroen Groenendijk, Martin Stokhof — Dynamic Predicate Logic, towards a compositional, non-representational semantics of discourse
LP-89-03 Yde Venema — Two-dimensional Modal Logics for Relation Algebras and Temporal Logic of Intervals
LP-89-04 Johan van Benthem — Language in Action
LP-89-05 Johan van Benthem — Modal Logic as a Theory of Information
LP-89-06 Andreja Prijatelj — Intensional Lambek Calculi: Theory and Application
LP-89-07 Heinrich Wansing — The Adequacy Problem for Sequential Propositional Logic
LP-89-08 Víctor Sánchez Valencia — Peirce's Propositional Logic: From Algebra to Graphs
LP-89-09 Zhisheng Huang — Dependency of Belief in Distributed Systems

Mathematical Logic and Foundations:
ML-89-01 Dick de Jongh, Albert Visser — Explicit Fixed Points for Interpretability Logic
ML-89-02 Roel de Vrijer — Extending the Lambda Calculus with Surjective Pairing is conservative
ML-89-03 Dick de Jongh, Franco Montagna — Rosser Orderings and Free Variables
ML-89-04 Dick de Jongh, Marc Jumelet, Franco Montagna — On the Proof of Solovay's Theorem
ML-89-05 Rineke Verbrugge — Σ-completeness and Bounded Arithmetic
ML-89-06 Michiel van Lambalgen — The Axiomatization of Randomness
ML-89-07 Dirk Roorda — Elementary Inductive Definitions in HA: from Strictly Positive towards Monotone
ML-89-08 Dirk Roorda — Investigations into Classical Linear Logic
ML-89-09 Alessandra Carbone — Provable Fixed points in $I\Delta_0+\Omega_1$

Computation and Complexity Theory:
CT-89-01 Michiel H.M. Smid — Dynamic Deferred Data Structures
CT-89-02 Peter van Emde Boas — Machine Models and Simulations
CT-89-03 Ming Li, Herman Neuféglise, Leen Torenvliet, Peter van Emde Boas — On Space Efficient Simulations
CT-89-04 Harry Buhrman, Leen Torenvliet — A Comparison of Reductions on Nondeterministic Space
CT-89-05 Pieter H. Hartel, Michiel H.M. Smid, Leen Torenvliet, Willem G. Vree — A Parallel Functional Implementation of Range Queries
CT-89-06 H.W. Lenstra, Jr. — Finding Isomorphisms between Finite Fields
CT-89-07 Ming Li, Paul M.B. Vitanyi — A Theory of Learning Simple Concepts under Simple Distributions and Average Case Complexity for the Universal Distribution (Prel. Version)
CT-89-08 Harry Buhrman, Steven Homer, Leen Torenvliet — Honest Reductions, Completeness and Nondeterminstic Complexity Classes
CT-89-09 Harry Buhrman, Edith Spaan, Leen Torenvliet — On Adaptive Resource Bounded Computations
CT-89-10 Sieger van Denneheuvel — The Rule Language RL/1
CT-89-11 Zhisheng Huang, Sieger van Denneheuvel, Peter van Emde Boas — Towards Functional Classification of Recursive Query Processing

Other Prepublications:
X-89-01 Marianne Kalsbeek — An Orey Sentence for Predicative Arithmetic
X-89-02 G. Wagemakers — New Foundations: a Survey of Quine's Set Theory
X-89-03 A.S. Troelstra — Index of the Heyting Nachlass
X-89-04 Jeroen Groenendijk, Martin Stokhof — Dynamic Montague Grammar, a first sketch
X-89-05 Maarten de Rijke — The Modal Theory of Inequality
X-89-06 Peter van Emde Boas — Een Relationele Semantiek voor Conceptueel Modelleren: Het RL-project

1990 SEE INSIDE BACK COVER

Instituut voor Taal, Logica en Informatie
Institute for Language, Logic and Information

Faculteit der Wiskunde en Informatica
(Department of Mathematics and Computer Science)
Plantage Muidergracht 24
1018TV Amsterdam

Faculteit der Wijsbegeerte
(Department of Philosophy)
Nieuwe Doelenstraat 15
1012CP Amsterdam

A SEMANTICAL PROOF OF DE JONGH'S THEOREM

Jaap van Oosten
Department of Mathematics and Computer Science
University of Amsterdam

Received February 1990

A semantical proof of De Jongh's Theorem

Jaap van Oosten

Abstract. In 1969, De Jongh proved the "maximality" of a fragment of intuitionistic predicate calculus for **HA**. Leivant strengthened the theorem in 1975, using proof-theoretical tools (normalisation of infinitary sequent calculi). By a refinement of De Jongh's original method (using Beth models instead of Kripke models and sheafs of partial combinatory algebras), a semantical proof is given of a result that is almost as good as Leivant's. Furthermore, it is shown that **HA** can be extended to Higher Order Heyting Arithmetic + all true Π^0_2-sentences + transfinite induction over primitive recursive well-orderings.

Key words and phrases: maximality, **IQC**, **HA**, realisability, sheaf.

AMS Subject classification: 03F50

0. Introduction

In 1969, Dick de Jongh proved an interesting theorem. In order to state it, let us introduce the following notation.
If A is a formula of intuitionistic predicate calculus **IQC**, and P a unary predicate symbol not occurring in A, let $A^{(P)}$ be A with all quantifiers relativised to P (i.e. replace $\forall x$ by $\forall x(P(x)\rightarrow...)$ and $\exists x$ by $\exists x(P(x)\wedge...)$), and $A' \equiv \exists x P(x) \rightarrow A^{(P)}$. **HA** denotes, as usual, intuitionistic first order arithmetic.

Theorem 0.1. *If* **HA** *proves every arithmetical substitution instance of* A', *then* A' *is provable in* **IQC**.

The proof was an ingenious combination of Kripke semantics and realisability. However, De Jongh never published it and his method remained unknown until N. Goodman [1978] presented a very similar semantics, for different purposes (A theorem similar to Theorem 0.1, concerning **HA** and *propositional* logic, was also proved by De Jongh by the same method. This theorem is given by Smorynski in Troelstra [1973] with a proof that uses only Kripke models and some proof-theoretic facts).
By purely proof-theoretic means, D. Leivant was able to strengthen Theorem 0.1 considerably (Leivant [1975]):

Theorem 0.2. *There are* Π^0_2*-predicates* $\{A_{ij}\}_{i,j<\omega}$, *such that* A_{ij} *has j free variables and for any formula* F *of* **IQC** *with* n_j*-ary predicate letters* $P_{i_j n_j}$, *j=1,...,k, if* $\mathbf{HA} \vdash F[A_{i_1 n_1},...,A_{i_k n_k}]$ *then* $\mathbf{IQC} \vdash F[P_{i_1 n_1},...,P_{i_k n_k}]$.

The aim of this paper is to give a semantical proof of a slightly weaker version of Theorem 0.2. Throughout the rest of this paper, we assume that languages contain relation symbols only, and furthermore, that they admit an enumeration $(A_i)_{i\in\mathbb{N}}$ of their predicate symbols such that the arity of the A_i is a primitive recursive function of i.

Theorem 0.3. *Let* T *be a recursively enumerable theory, formulated in a language* $\mathfrak{L}$ *in* **IQC**. *Then for every j-place predicate letter* A_{ij} *of* $\mathfrak{L}$ *there is a j-place number-theoretic predicate* B_{ij}, *resulting in a translation (by substitution)* $(-)^*: \mathfrak{L}\rightarrow\mathfrak{L}(\mathbf{HA})$ *such that for every sentence* F *of* $\mathfrak{L}$: $T \vdash F$ *if and only if* $\mathbf{HA}+(T)^* \vdash F^*$.

Note that Theorem 0.3 is contained in Theorem 0.2, so we do not claim a new result. We believe, however, that our proof, which is a refinement of De Jongh's original one, has some interest of its own, besides being much shorter than Leivant's.

The proof consists of the construction of a realisability model that "matches" the truth in an appropriate Beth model: we will be using a "universal Beth model" for T.

We could, of course, have formulated Theorem 0.3 the same way as Theorem 0.2, without reference to T (let T be the empty theory in a universal language); however, we would like to point out that there is a mass of realisability models obtained in this way, one for each T, and this is not immediately clear if one restricts attention to just the empty theory (if this paper has any interest, it is the *method* , not the result).

The reader will have noted that we didn't mention the complexity of our substitutions in the statement of Theorem 0.3. We cannot have Π^0_2-substitutions since our models will satisfy exactly the true Π^0_2-sentences, but classically they will be in Π^0_4.

It is possible to replace **HA** in Theorem 0.3 by certain extensions of **HA**. These extensions will be easy corollaries of our proof and will be discussed in section 3. Section 1 gives preliminaries; the actual construction of the model will take up section 2.

The author is grateful to D. de Jongh, A.S. Troelstra and I. Moerdijk for reading the manuscript and for discussions.

1. Beth models and realisability

Definition 1.1. A (fallible) Beth model for a language $\mathcal{L}$ in **IQC** consists of the following:

i) a tree P and a P-indexed collection of sets (this is, for every $p\in P$ a set X_p as well as a collection of functions $(f_{pp'}:X_p\to X_{p'})_{p,p'\in P, p\leq p'}$ such that f_{pp} is the identity and $f_{p'p''}\circ f_{pp'}=f_{pp''}$ whenever $p\leq p'\leq p''$);

ii) a specified upwards closed subset U of P such that for any $p\in P$, if every path through p meets U somewhere, then already $p\in U$;

iii) for every n-ary relation symbol A of $\mathcal{L}$ an interpretation $A^*=(A^*_p)_{p\in P}$ with $A^*_p\subseteq(X_p)^n$ such that:

a) $(d_1,\ldots,d_n)\in A^*_p$ and $p\leq p'$ implies $(f_{pp'}(d_1),\ldots,f_{pp'}(d_n))\in A^*_{p'}$;

b) If $(d_1,\ldots,d_n)\in (X_p)^n$ is such that on every path through p there is a p' with $(f_{pp'}(d_1),\ldots,f_{pp'}(d_n))\in A^*_{p'}$, then $(d_1,\ldots,d_n)\in A^*_p$;

c) $A^*_p=(X_p)^n$ for $p\in U$.

Let us call a set R that is such that every path through p meets R eventually, a *bar* for p. Given a fallible Beth model we can interpret, in any $p\in P$, sentences of $\mathcal{L}(X_p)$ (constants for elements of X_p added) as follows:

$p\Vdash A(d_1,\ldots,d_n)$ iff $(d_1,\ldots,d_n)\in A^*_p$;

$p\Vdash \phi\wedge\psi$ iff $p\Vdash\phi$ and $p\Vdash\psi$;

$p\Vdash \phi\vee\psi$ iff there is a bar R for p with $\forall r\in R\,(r\Vdash\phi$ or $r\Vdash\psi)$;

$p \Vdash \phi \rightarrow \psi$ iff for every $p' \geq p$, if $p' \Vdash \phi$ then $p' \Vdash \psi$;

$p \Vdash \exists x \phi(x)$ iff there is a bar R for p with $\forall r \in R \exists d \in X_r (r \Vdash \phi(d))$;

$p \Vdash \forall x \phi(x)$ iff for every $p' \geq p$ and for all $d \in X_{p'}$, $p' \Vdash \phi(d)$.

Here, if $\phi \equiv \phi(d_1,...,d_n)$ with $d_1,...,d_n \in X_p$ and $p \leq p'$, $p' \Vdash \phi$ is read as $p' \Vdash \phi(f_{pp'}(d_1),...,f_{pp'}(d_n))$. From the definition it follows immediately that if $p \in U$, $p \Vdash \phi$ for any formula ϕ (we take the absurdity as a 0-place predicate); this is why these models are called *fallible*. A fallible Beth model is said to have a *constant domain* if all X_p are equal and the maps $f_{pp'}$ are identities. The main result about fallible Beth models is the following.

Theorem 1.2. *Let* T *be a recursively enumerable theory in a language* $\mathfrak{L}$ *in* **IQC**. *Then there is a fallible Beth model* $\mathfrak{B}$ *with constant domain* $\mathbb{N}$ *and as underlying poset the binary tree* P, *such that for every sentence* A *in the language of* $\mathfrak{L}$: $\langle\rangle \Vdash A$ *iff* $T \vdash A$ *(* $\mathfrak{B}$ *is called a* universal Beth model *for* T*). Moreover, there is an enumeration* $(A_i)_i$ *of* $\mathfrak{L}$ *such that the relation* $p \Vdash A_i(n_1,...,n_{k_i})$ *is* Σ^0_1 *in* p,i,n.

This result can be found in Troelstra & Van Dalen [1988], chapter 13. It is an adaptation by the authors of a proof by Friedman.

Definition 1.3. A *partial combinatory algebra* (pca) consists of a set A and a partial binary operation • on A, as well as elements K and S of A, for which hold:

i) For every $x,y \in A$, $K \bullet x$ and $(K \bullet x) \bullet y$ are defined and $(K \bullet x) \bullet y$ is equal to x;

ii) For $x,y,z \in A$, $S \bullet x$ and $(S \bullet x) \bullet y$ are defined, and $((S \bullet x) \bullet y) \bullet z$ is defined whenever $(x \bullet z) \bullet (y \bullet z)$ is, and equal to it in that case.

The reader is referred to Barendregt [1981] for proofs of the following facts:

i) λ-abstraction can be defined in A;

ii) A contains a definable system of natural numbers $\{\bar{n} \mid n \in \mathbb{N}\}$, such that for every partial recursive function f there is a definable element $\bar{f}$ of A which satisfies: f(n) is defined and equal to m $\Leftrightarrow$ $\bar{f} \bullet \bar{n}$ is defined and equal to $\bar{m}$, for $n,m \in \mathbb{N}$.

Now suppose we have a tree P and a specified upwards closed subset U as in definition 1.1. Consider a P-indexed system of pca's: that is, a pca A_p is attached to every $p \in P$, and functions $f_{pp'}: A_p \rightarrow A_{p'}$ are given for each inequality $p \leq p'$ satisfying the same conditions as in definition 1.1, and furthermore:

i) the $f_{pp'}$ preserve the combinators K and S, and

ii) application: if $a \bullet b$ is defined in A_p, then $f_{pp'}(a) \bullet f_{pp'}(b)$ is defined in $A_{p'}$ and equal to $f_{pp'}(a \bullet b)$

(This ensures that every closed λ-term retains its meaning under the $f_{pp'}$).

Furthermore we fix a λ-definable choice of natural numbers, denoted $\{\bar{n} \mid n\in\mathbb{N}\}$, as well as λ-definable pairing and unpairing operators j, j_1, j_2. We will now define, for sentences A of arithmetic, elements p of P, and a of A_p, what it means that a "p-realises A", by induction on A. Let us call a set R such that $R\cup U$ is a bar for p, a *U-bar* for p.

1) a p-realises t=s iff there is a U-bar R for p with $\forall r\in R$ (t=s is true and $f_{pr}(a)=\bar{t}$);
2) a p-realises $A\wedge B$ iff j_1a p-realises A and j_2a p-realises B;
3) a p-realises $A\vee B$ iff there is a U-bar R for p with $\forall r\in R\,(j_1(f_{pr}(a))=\bar{0}$ and $j_2(f_{pr}(a))$ r-realises A, or $j_1(f_{pr}(a))=\bar{1}$ and $j_2(f_{pr}(a))$ r-realises B);
4) a p-realises $A\rightarrow B$ iff for every $p'\geq p$ and for every $b\in A_{p'}$, if b p'-realises A then there is a U-bar R for p' such that $\forall r\in R\,(f_{pr}(a)\bullet f_{p'r}(b)$ is defined and r-realises B);
5) a p-realises $\exists xA(x)$ iff there is a U-bar R for p with $\forall r\in R\,\exists n\in\mathbb{N}\,(j_1(f_{pr}(a))=\bar{n}$ and $j_2(f_{pr}(a))$ r-realises A(n));
6) a p-realises $\forall xA(x)$ iff for every n there is a U-bar R for p with $\forall r\in R\,(f_{pr}(a)\bullet\bar{n}$ is defined and r-realises A(n)).

When talking about $\bar{t}$ and $\bar{n}$ we mean, of course, their interpretations in the appropriate pca; but since these are stable in the sense that, for $p\leq p'$, $f_{pp'}((\bar{t})_p)=(\bar{t})_{p'}$ for every term t of $\mathfrak{L}(\mathbf{HA})$, we suppress the reference to p.

We say that a sentence A is p-*realisable* iff there is an $a\in A_p$ that p-realises A. We say that A is *realisable* iff A is $\perp$-realisable, where $\perp$ denotes the bottom element of the tree P. A trivial induction on A shows that:

i) A is always p-realisable when $p\in U$;
ii) if a p-realises A then $f_{pp'}(a)$ p'-realises A, for $p\leq p'$;
iii) if $a\in A_p$ and R is a U-bar for p such that for every $r\in R$, $f_{pr}(a)$ r-realises A, then a p-realises A.

Theorem 1.4. *All axioms and rules of* **HA** *are p-realisable, for every $p\in P$.*

The reader is referred to Goodman [1978] for a proof (some obvious modifications have to be made); people familiar with topos theory may be satisfied with the remark that we have just defined the internal logic of the natural numbers object in an appropriate realisability topos defined over the topos of sheaves on a closed subset of Cantor space. Finally, one may note that a P-indexed system of pca's is just a Kripke model of an intuitionistic theory of pca's, and that the normal soundness theorem is entirely constructive (note, however, that there is a difference from the constructivist's point of view between working with U-bars and simply cutting U out).

Definition 1.5. Let a system of pca's and functions be given as above. We say that this system is a *sheaf* iff the following two conditions are satisfied:

i) For every p and every minimal U-bar R for p (meaning that no proper subset of R is a U-bar for p), for every family $(a_r \in A_r)_{r\in R}$ there is a *unique* $a\in A_p$ with $\forall r\in R\,(f_{pr}(a)=a_r)$;

ii) For every p, every $a,b\in A_p$, if there is a U-bar R for p with $\forall r\in R\,(f_{pr}(a)\bullet f_{pr}(b)$ is defined), then $a\bullet b$ is defined.

Suppose the system of pca's given in the definition of realisability is a sheaf. Then the clauses for implication and universal quantification in the realisability definition can be simplified into:

4') a p-realises $A\rightarrow B$ iff for all $p'\geq p$ and all $b\in A_{p'}$, if b p'-realises A then $f_{pp'}(a)\bullet b$ is defined and p'-realises B;

6') a p-realises $\forall x A(x)$ iff for all $n\in\mathbb{N}$, $a\bullet\bar{n}$ is defined and p-realises A(n).

Furthermore, an induction on A shows that in this case, A has a p-realiser iff there is a U-bar R for p with $\forall r\in R$(A has an r-realiser).

Since a similar property holds for fallible Beth models ($p\Vdash A$ iff there is a U-bar R for p with $\forall r\in R(r\Vdash A)$), and we are we are steering towards realisabilities that match the truth in certain Beth models, it is clear that we need sheafs of pca's.

2. Construction of the model

The structure of the proof of Theorem 0.3 will be the following. Given a recursively enumerable theory T, we have a universal Beth model for T (i.e. the model given by theorem 1.2); this model will be used to define a sheaf of pca's, as well as substitutions for the predicates of $\mathfrak{L}$, such that the following will hold: for any formula A in the language $\mathfrak{L}$ with, say, n free variables, for any $p\in P$ and for any n-tuple $y_1,\ldots,y_n\in\mathbb{N}$, $A^*(y_1,\ldots,y_n)$ has a p-realiser if and only if $p\Vdash A(y_1,\ldots,y_n)$.

We start with a P-indexed system of pca's of the following form. Consider an acceptable Gödel-numbering (i.e., satisfying enumeration and smn-theorem, see Odifreddi[1989]) of Turing machines that are enriched with two types of standard instructions, namely ask for values of F and G at a certain argument, where F and G are abstract partial oracle functions. A pca will be obtained by providing interpretations for F,G, i.e. concrete partial functions f and g: $\mathbb{N}\rightarrow\mathbb{N}$. The interpretations f,g will vary with $p\in P$ and since we will declare a computation to diverge whenever a value of F (or G) is asked at an argument not in the domain of f (resp. g), in order to satisfy the conditions for a P-indexed system of pca's we must have $f(p)\subseteq f(p')$ and $g(p)\subseteq g(p')$ whenever $p\leq p'$.

Let F_p be the pca $(\mathbb{N},\{\cdot\}^{f(p),g(p)}(\cdot))$ where $\{x\}^{f(p),g(p)}(y)$ will denote the outcome (if there is any) of a computation of machine x with input y, and f(p) and g(p) interpreting F and G. Transition maps:$F_p\rightarrow F_{p'}$ are identities. This gives a system of pca's which is not a sheaf; therefore we let the system $(A_p)_{p\in P}$ be the sheafification of it : A_p consists of equivalence classes of partial functions $\alpha{:}\uparrow(p)\rightarrow\bigcup_{q\geq p}F_q$ that satisfy:

i) $q\in dom(\alpha) \Rightarrow \alpha(q)\in F_q$;

ii) $q\in dom(\alpha)$, $q'\geq q \Rightarrow q'\in dom(\alpha)$ and $\alpha(q')=f_{qq'}(\alpha(q))$;

iii) there is a U-bar R for p such that $R\subseteq dom(\alpha)$).

Two such functions are equivalent iff there is a U-bar for p at which they are both defined and equal. In A_p an application is defined by: $[\alpha]\bullet[\beta]$ is defined iff there is a U-bar R for p with $\forall r\in R(\{\alpha(r)\}^{f(r),g(r)}(\beta(r))$ is defined in F_r), and in that case $[\alpha]\bullet[\beta]$ is the equivalence class of the function that assigns $\{\alpha(r)\}^{f(r),g(r)}(\beta(r))$ to r (note, that this does not depend on the choice of representatives).

Now for the choice of the functions f(p) and g(p) we need a recursion-theoretic fact.

Theorem 2.1. *Let u be a numerical function in 0', i.e. u is the characteristic function of some non-recursive Σ^0_1-predicate. Then there is a 2-place number-theoretic predicate* $D(x,y)\in 0''$ *such that (putting* $D_n(x)\equiv D(x,n)$, $D^m(x,n)\equiv D(x,n+sg(n+1-m))$*),* D_n *is not recursive in u,* D^n *(the sequence* D_n *is called* recursively independent).

This is Theorem 2 of Kleene & Post [1951]. We owe the use of this theorem to De Jongh[1969].

Suppose $\mathfrak{B}$ is a universal Beth model for T as given by theorem 1.2. Let $(A_i|\ i=0,1,...)$ be an enumeration of $\mathfrak{L}$, such that for some primitive recursive f and #, $R_j=A_{f(j)}$ and A_i has exactly #(i) free variables. Furthermore, we suppose that the enumeration $(A_i|\ i=0,1,...)$ is such that, for instance, $A_i\wedge A_j=A_{g(i,j)}$ for primitive recursive g, etc. Then the function u defined by:

$u(p,i,y)=1$ if $y=\langle y_1,...,y_{\#(i)}\rangle$ and $p\Vdash A_i(y_1,...,y_{\#(i)})$, and 0 otherwise,

is in 0' by theorem 1.2. Let D be a 2-place predicate as given by theorem 2.1. For $p\in P$ define the predicate $D^{(p)}$ by: $D^{(p)}(x,y)$ iff $y=\langle i,y_1,...,y_{\#(i)}\rangle$ and $u(p,i,y)=1$ and $D(x,y)$. Then $D^{(p)}$ is obviously recursive in u,D; and if $u(p,i,\langle w_1,...,w_{\#(i)}\rangle)=0$ then $D^{(p)}$ is recursive in u, $D^{\langle i,w_1,...,w_{\#(i)}\rangle}$. So D_y is recursive in $D^{(p)}$ iff $y=\langle i,y_1,...,y_{\#(i)}\rangle$ and $u(p,i,\langle y_1,...,y_{\#(i)}\rangle)=1$; for if not ($y=\langle i,y_1,...,y_{\#(i)}\rangle$ and $u(p,i,\langle y_1,...,y_{\#(i)}\rangle)=1$), then $D^{(p)}$ is recursive in u,D^y, and D_y is not.

We are now ready to define the partial functions f(p),g(p) and the substitutions ϕ_j for the predicates R_j.

Put f(p)(i,y) = 1 if $y=\langle i,y_1,...,y_{\#(i)}\rangle$ and $p\Vdash A_i(y_1,...,y_{\#(i)})$, and undefined otherwise.

Put g(p)(y,x) = undefined if y is not of form $\langle i,y_1,...,y_{\#(i)}\rangle$ or $y=\langle i,y_1,...,y_{\#(i)}\rangle$ and $p\nVdash A_i(y_1,...,y_{\#(i)})$;

= 1 if $y=\langle i,y_1,...,y_{\#(i)}\rangle$, $p\Vdash A_i(y_1,...,y_{\#(i)})$ and $D(x,y)$;

= 0 if $y=\langle i,y_1,...,y_{\#(i)}\rangle$, $p\Vdash A_i(y_1,...,y_{\#(i)})$ and not $D(x,y)$.

For j=1,... let $C_j(x,y_1,...,y_{\#(f(j))})$ be a negative formula, expressing $D(x,\langle f(j),y_1,...,y_{\#(f(j))}\rangle)$, and put $\phi_j(y_1,...,y_{\#(f(j))})\equiv\forall x(C_j(x,y_1,...,y_{\#(f(j))})\vee\neg C_j(x,y_1,...,y_{\#(f(j))}))$.

By a *partial term* we mean something that is built up from: free variables, primitive recursive functions, λ-abstraction, and $\{\cdot\}^{F,G}(\cdot)$. If t is a partial term we denote by t_p its (possibly undefined) meaning in F_p, interpreting F,G by f(p),g(p) respectively. t represents an element of A_p if t is defined on a U-bar for p. We express this by "$t\in A_p$".

Lemma 2.2. For every negative formula $C(x_1,\dots,x_k)$ of $\mathfrak{L}(\mathbf{HA})$ there is a partial term t(C), whose free variables are contained in $\{x_1,\dots,x_k\}$, such that for all $p\in P$ and all $n_1,\dots,n_k$:
i) $C(n_1,\dots,n_k)$ is true in $\mathbb{N} \Rightarrow (t(C)(\bar{n}_1,\dots,\bar{n}_k))_p \in A_p$ and $(t(C)(\bar{n}_1,\dots,\bar{n}_k))_p$ p-realises $C(n_1,\dots,n_k)$;
ii) $C(n_1,\dots,n_k)$ has a p-realiser and $p\notin U \Rightarrow C(n_1,\dots,n_k)$ is true in $\mathbb{N}$.

Proof. Standard. ⊠

The translation $(-)^*$: $\mathfrak{L}\to\mathfrak{L}(\mathbf{HA})$ is given by substituting ϕ_j for R_j.Theorem 0.3 will now follow from the following lemma:

Lemma 2.3. For every formula A of $\mathfrak{L}$ there is a parti ıl term t_A with the same number k of free variables, such that the following holds: for every p and all $y_1,\dots,y_k\in\mathbb{N}$,

i) $p\Vdash A(y_1,\dots,y_k) \Rightarrow t_A(y_1,\dots,y_k)_p\in A_p$ & $t_A(y_1,\dots,y_k)_p$ p-realises $A^*(y_1,\dots,y_k)$;

ii) $A^*(y_1,\dots,y_k)$ has a p-realiser $\Rightarrow p\Vdash A(y_1,\dots,y_k)$.

Proof. By induction on A. We define t_A and prove i) and ii) simultaneously. The main step is the one for prime formulas.

If $A\equiv R_j$ let $t_A(y_1,\dots,y_{\#(f(j))})$ be $\lambda x.\begin{cases} j(0,t(C_j)(x,y_1,\dots,y_{\#(f(j))})) \text{ if } G(\langle f(j), y_1,\dots,y_{\#(f(j))}\rangle,x)=1 \\ j(1,t(\neg C_j)(x,y_1,\dots,y_{\#(f(j))})) \text{ if } G(\langle f(j),y_1,\dots,y_{\#(f(j))}\rangle,x)=0\end{cases}$

here the expressions $t(C_j)$ and $t(\neg C_j)$ are as defined in lemma 2.2.
Then i) is immediate; for ii), suppose $[\alpha]$ p-realises $\forall x(C_j(x,y_1,\dots,y_{\#(f(j))})\vee\neg C_j(x,y_1,\dots,y_{\#(f(j))}))$and $p\Vdash R_j(y_1,\dots,y_{\#(f(j))})$. There is a U-bar R for p such that $R\subseteq\text{dom}(\alpha)$ and for at least one $r\in R$, $r\Vdash R_j(y_1,\dots,y_{\#(f(j))})$, so we may as well assume $p\in\text{dom}(\alpha)$. Then for all n, $[\alpha]\bullet n$ is defined and $[\alpha]\bullet\bar{n}$ p-realises $C_j(n,y_1,\dots,y_{\#(f(j))})\vee\neg C_j(n,y_1,\dots,y_{\#(f(j))})$, so for all n there is a U-bar R_n for p with $\forall r\in R_n$ $(j_1(\alpha\bullet\bar{n})(r)=\bar{0}$ & $j_2(\alpha\bullet\bar{n})(r)$ r-realises $C_j(n,y_1,\dots,y_{\#(f(j))})$ or $j_1(\alpha\bullet\bar{n})(r)=\bar{1}$ & $j_2(\alpha\bullet\bar{n})(r)$ r-realises $\neg C_j(n,y_1,\dots,y_{\#(f(j))}))$.
But since C_j is negative and $p\notin U$ (because $p\Vdash R_j(y_1,\dots,y_{\#(f(j))})$), exactly one of $C_j,\neg C_j$ is realised at p, according to whether C_j is true or not. So if $\beta\equiv\lambda n.j_1(\alpha\bullet\bar{n})$, then β is a decision function for $D_{\langle f(j),y_1,\dots,y\#f(j)\rangle}$. But if β needs $G(\langle f(j),y_1,\dots,y_{\#f(j)}\rangle,n)$ for some n then $\beta\bullet\bar{n}$ can never be defined. So $D_{\langle f(j),y_1,\dots,y\#f(j)\rangle}$ is recursive in $D^{\langle f(j),y_1,\dots,y_{\#f(j)}\rangle}$, contradiction.

2) If $A \equiv B_1 \wedge B_2$ put $t_A \equiv j(t_{B_1}, t_{B_2})$.

3) If $A \equiv B_1 \rightarrow B_2$ put $t_A \equiv \lambda x.t_{B_2}$.

4) If $A \equiv B_1 \vee B_2$, say $B_1 = A_k$, $B_2 = A_l$, $\#(k) \leq \#(l)$ and $A \leftrightarrow B_1(y_1,\ldots,y_{\#(k)}) \vee B_2(y_1,\ldots,y_{\#(l)})$ (Otherwise, permute the variables). Let e be a code such that $\{e\}^{F,G}(i,y) \simeq F(i,y)$; and f such that

$$\{f\}^{F,G}(y_1,\ldots,y_{\#(l)}) \simeq j(\bar{0}, t_{B_1}(y_1,\ldots,y_{\#(k)})) \text{ if}$$
$$T^{F,G}(e,k,\langle y_1,\ldots,y_{\#(k)}\rangle, \mu z.(T^{F,G}(e,k,\langle y_1,\ldots,y_{\#(k)}\rangle) \vee T^{F,G}(e,l,\langle y_1,\ldots,y_{\#(l)}\rangle)))$$
$$\simeq j(\bar{1}, t_{B_2}(y_1,\ldots,y_{\#(l)})) \text{ if}$$
$$T^{F,G}(e,l,\langle y_1,\ldots,y_{\#(l)}\rangle, \mu z.(T^{F,G}(e,k,\langle y_1,\ldots,y_{\#(k)}\rangle) \vee T^{F,G}(e,l,\langle y_1,\ldots,y_{\#(l)}\rangle))).$$

Then if $p \Vdash A$ there is a U-bar R for p with $\forall r \in R\ (r \Vdash B_1 \text{ or } r \Vdash B_2)$, so it is easy to see that then $\{f\}^{F,G}(y_1,\ldots,y_{\#(l)})$ is defined at p and p-realises A.

For ii) suppose $\alpha \in [\![A_k^* \vee A_l^*]\!]_p$. Pick a U-bar R for p such that $\forall r \in R\ (\alpha(r)\downarrow \ \&\ (j_1(\alpha(r)) = \bar{0} \rightarrow j_2\alpha$ r-realises $A_k^*)\ \&\ (j_1(\alpha(r)) = \bar{1} \rightarrow j_2\alpha$ r-realises $A_l^*))$. Then $\forall r \in R$ (A_k^* has a r-realiser or A_l^* has a r-realiser), so by induction hypothesis $p \Vdash A_k \vee A_l$.

5) $A \equiv \forall x B(x)$. Similar to 3).

6) $A \equiv \exists x B(x)$. Similar to 4): say $B(x) = A_k(y_1,\ldots,y_{\#(k)})$ and x is y_1.Put $t_A(y_2,\ldots,y_{\#(k)}) \equiv j(n, t_{A_k}(n,y_2,\ldots,y_{\#(k)}))$, where n is $j_1(\mu z.T^{F,G}(e,k,\langle j_1 z, y_2,\ldots,y_{\#(k)}\rangle, j_2 z))$, with e as in case 4).⊠

To conclude the proof of the theorem: $\Rightarrow$ is obvious. Suppose $\mathbf{HA}+(T)^* \vdash A^*$, then A^* has a $\langle\rangle$-realiser, so by lemma 2.3 $\langle\rangle \Vdash A$, which means $T \vdash A$ by the property of a universal Beth model.⊠

3. Extensions of ***HA****; some corollaries*

A casual glance at the model will convince the reader that it satisfies all true Π^0_2-sentences; moreover, we have remarked that our model is part of a topos (this has not been explained, but since this is a general phenomenon we prefer to leave this for a separate treatment). So it is immediate that **HA**, in theorem 0.3, can be replaced by **HAH**+all true Π^0_2-sentences, where **HAH** is Higher Order Heyting Arithmetic.

We now want to show that transfinite induction over all primitive recursive well-orderings holds in our model. Let $\mathbf{HA}^+$ be the expansion of **HA** in a language that contains an extra partial function symbol •, and with additional axioms asserting that $(\mathbb{N},\bullet)$ is a partial combinatory algebra. Since the sheaf of pca's constructed in the model has the sheafification of $\mathbb{N}$ as underlying sheaf, it is an ordinary sheaf model of $\mathbf{HA}^+$. Moreover, the realisability definition in our model is the sheaf model interpretation of Kleene realisability with •. So if F is some arithmetical principle or schema that holds in the model, and we have, for every instance A of F, a proof in **HA**+F that A is Kleene-realisable such that the proof doesn't use any particular property of the pca of partial recursive application, then the proof can be carried out in $\mathbf{HA}^+$, doing realisability with $\bullet$, and consequently the principle will be realised in our model, if it is valid in it.

Let us apply this to the transfinite induction schema $TI_{\prec}$, which is:

$\forall u\,(\forall v{<}u\,A(v) \rightarrow A(u)) \rightarrow \forall u A(u)$,

where $\prec$ is a primitive recursive well-ordering. It is easy to convince oneself that this schema is valid in a sheaf model, so what remains to prove is the following:

Proposition 3.1. *For every instance* F *of* $TI_{\prec}$, $\mathbf{HA}^{+}+TI_{\prec} \vdash \exists n\,(n\,\mathbf{r}\,F)$, *where* **r** *means realisability with* $\bullet$.

Proof. This is a slight adaptation of the proof given in Troelstra [1973], 3.2.23. Let F be $\forall u\,(\forall v{<}u\,A(v) \rightarrow A(u)) \rightarrow \forall u A(u)$ for some formula A, and suppose w realises the premiss. This means:

($\oplus$) $\forall u \forall w'\,(\forall v\,(v{<}u \rightarrow \forall k\,(w'\bullet v)\bullet k\,\mathbf{r}\,A(v)) \rightarrow (w\bullet u)\bullet w'\,\mathbf{r}\,A(u))$.

We want a g that realises $\forall u A(u)$ or $\forall u\,(g\bullet u\ \mathbf{r}\ A(u))$ or, with $TI_{\prec}$,

$\forall u\,(\forall v{<}u\ g\bullet v\ \mathbf{r}\ A(v) \ \rightarrow g\bullet u\ \mathbf{r}\ A(u))$.

Take a number G such that for all g,u:

$G\bullet\langle g,u\rangle \simeq (w\bullet u)\bullet(\Lambda v.\ \Lambda k.\ g\bullet v)$,

and find with the recursion theorem for $\bullet$, a number g such that for all u:

$g\bullet u \simeq G\bullet\langle g,u\rangle$.

Now $\forall v{<}u\ g\bullet v\ \mathbf{r}\ A(v)$ implies $\forall v{<}u\,\forall k\,((\Lambda v.\ \Lambda k.\ g\bullet v)\bullet v)\bullet k\ \mathbf{r}\ A(v)$, so with ($\oplus$): $(w\bullet u)\bullet(\Lambda v.\ \Lambda k.\ g\bullet v)\ \mathbf{r}\ A(u)$, which is $g\bullet u\ \mathbf{r}\ A(u)$. Note, that $\mathbf{HA}^{+}$ need not prove anything about $\prec$! ⊠

References

H. Barendregt, *The Lambda Calculus*, North Holland (Amsterdam) 1981

N.D. Goodman, Relativized realizability in intuitionistic arithmetic of all finite types, *Journal of Symb. Logic* **43**(1978), 1, pp.23-44

D.H.J. de Jongh, *The Maximality of the Intuitionistic Predicate Calculus with respect to Heyting's Arithmetic*, typed manuscript, Amsterdam 1969

S.C. Kleene & E.L. Post, *The upper semilattice of degrees of recursive unsolvability*, Ann. Math. **59** (1951),3, pp.379-407

D. Leivant, *Absoluteness of intuitionistic logic*, thesis, Amsterdam 1975

P. Odifreddi, *Classical Recursion Theory* , North Holland (Amsterdam) 1989

A.S. Troelstra & D. van Dalen, *Constructivism in Mathematics*, North Holland (Amsterdam) 1988

A.S Troelstra (ed.), *Metamathematical Investigation in Intuitionistic Arithmetic and Analysis*, Springer (Berlin) 1973 (LNM 344)

The ITLI Prepublication Series

1990