Institute for Language, Logic and Information

Σ-COMPLETENESS AND BOUNDED ARITHMETIC

Rineke Verbrugge

ITLI Prepublication Series
for Mathematical Logic and Foundations ML-89-05

University of Amsterdam

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

Σ-COMPLETENESS AND BOUNDED ARITHMETIC

Rineke Verbrugge
Department of Mathematics and Computer Science
University of Amsterdam

Received October 1989

Research Supported by N.W.O.

Chapter 1. Introduction and preliminaries

This paper contains some results obtained in the course of our quest to prove or disprove the extension of Solovay's completeness theorem to bounded arithmetic. In the standard proofs of both Solovay's theorem and Rosser's theorem, the provability of Σ-completeness is essential. In Chapter 2 we will show that, under the compexity theoretic hypothesis NP$\neq$co-NP, Σ-completeness is *not* provable in the system of bounded arithmetic that we investigate, $I\Delta_0+\Omega_1$.
However, both Rosser's theorem and a very restricted version of Solovay's completeness theorem can be proved using a weak reflection principle introduced in another context by Švejdar (Švejdar[83]). In Chapter 3, we will present a proof of Švejdar's principle in $I\Delta_0+\Omega_1$, and we will give Švejdar's (short) proof that Rosser's theorem follows from his reflection principle. A discussion of Solovay's theorem will be postponed to a subsequent paper; a preliminary version can be found in Verbrugge[88].
In order to be able to explain some of the concepts occurring in this paper, we will first, by way of a few definitions, introduce some of the more popular fragments of Peano arithmetic that fall under the name of bounded arithmetic.

Bounded arithmetic.

The language of bounded arithmetic consists of:

0	zero constant symbol
S	successor
+	addition
$\cdot$	multiplication
$\lfloor \frac{1}{2}x \rfloor$	"shift right function", i.e. the entier of $\frac{1}{2}x$
$\lvert x \rvert$	$= \lceil {}^2\log(x+1) \rceil$, the length of the binary representation of x
$x \# y$	$= 2^{\lvert x \rvert \cdot \lvert y \rvert}$, the "smash" fuction
$\leqslant$	less than or equal to

(The notation $\lceil a \rceil$ denotes the least integer $\geqslant$ a.)

In Chapter 3, we will be more parsimonious and use a language containing just 0, S, +, $\cdot$, and $\leqslant$.

We call quantifiers of the form $\forall x$ or $\exists x$ unbounded quantifiers. Bounded quantifiers are of the form $\forall x \leqslant t$ or $\exists x \leqslant t$, where t is any term not involving x. The meaning of $\forall x \leqslant t A$ is $\forall x(x \leqslant t \rightarrow A)$, and, likewise, $\exists x \leqslant t A$ means $\exists x(x \leqslant t \wedge A)$. Sharply bounded quantifiers are of the form $\forall x \leqslant |t|$ or $\exists x \leqslant |t|$. A formula is bounded iff it contains no unbounded quantifiers.
The principal feature distinguishing bounded arithmetic from Peano arithmetic is that the induction axioms of the former are restricted to bounded formulas. For some theories of bounded arithmetic, induction is even restricted to a special class of bounded formulas from the hierarchy of bounded arithmetic formulas; we will now define this hierarchy.

(1) $\Sigma_0^b = \Pi_0^b = \Delta_0^b$ is the set of formulas with only sharply bounded quantifiers
(2) Σ_{k+1}^b is defined inductively by:
- (a) $\Sigma_{k+1}^b \supseteq \Pi_k^b$
- (b) If A is in Σ_{k+1}^b then so are $\exists x \leqslant t A$ and $\forall x \leqslant |t| A$
- (c) If $A,B \in \Sigma_{k+1}^b$ then $A \wedge B$ and $A \vee B$ are in Σ_{k+1}^b
- (d) If $A \in \Sigma_{k+1}^b$ and $B \in \Pi_{k+1}^b$ then $\neg B$ and $B \rightarrow A$ are in Σ_{k+1}^b.

(3) Π_{k+1}^b is defined inductively by:
- (a) $\Pi_{k+1}^b \supseteq \Sigma_k^b$
- (b) If A is in Π_{k+1}^b then so are $\forall x \leqslant t A$ and $\exists x \leqslant |t| A$
- (c) If $A,B \in \Pi_{k+1}^b$ then $A \wedge B$ and $A \vee B$ are in Π_{k+1}^b
- (d) If $A \in \Pi_{k+1}^b$ and $B \in \Sigma_{k+1}^b$ then $\neg B$ and $B \rightarrow A$ are in Π_{k+1}^b.

(4) Σ_{k+1}^b and Π_{k+1}^b are the smallest sets which satisfy (2),(3).

If R is a theory and A a formula, we say that A is Δ_i^b with respect to R iff there are formulas $B \in \Sigma_i^b$ and $C \in \Pi_i^b$ such that $R \vdash A \leftrightarrow B$ and $R \vdash A \leftrightarrow C$.

The bounded arithmetical hierarchy is related to the polynomial hierarchy of complexity theory (for a definition, see e.g. Buss

[86], Ch. 1) in the following way: if $k \geqslant 1$, then Σ_k^p (respectively, Π_k^p) is the class of predicates which are defined by formulas in Σ_k^b (respectively, Π_k^b). In particular, NP is the class of predicates which are defined by formulas in Σ_1^b , and co-NP is the class of predicates defined by Π_1^b-formulas (see Buss [86],Thm. 1.8).

Each theory of bounded arithmetic which we consider here contains (a subset of) BASIC, a finite set of true open formulas of arithmetic defining the basic properties of the function and predicate symbols contained in the language of bounded arithmetic. See Buss (Buss [86], pg. 30/31) for a list of these 32 formulas.

The different theories of bounded arithmetic are individuated by their induction axioms. Moreover, some of them contain an axiom stating that certain functions are total. At this point, we are ready to introduce the theories relevant in the context of this paper.

S_2^i

These theories have been introduced by Buss [86]. For every i, S_2^i contains the following scheme of induction, called Σ_i^b -PIND:

$$A(0) \wedge \forall x(A(\lfloor \tfrac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x),$$

where A is a Σ_i^b-formula (note the unusual form of the antecedent). The theory most extensively used in Buss [86], and in fact the only one of the S_2^i-theories mentioned in the remainder of this paper, is S_2^1 .

$I\Delta_0 + \Omega_1$

$I\Delta_0 + \Omega_1$, a system introduced by Paris and Wilkie [87], will be the leading theory in this paper. In Chapter 2 we use a "generous" version, which contains, in addition to the BASIC axioms, the scheme of bounded induction

$$A(0) \wedge \forall x(A(x) \rightarrow A(Sx)) \rightarrow \forall x A(x),$$

where A is a bounded formula.

In this version, $I\Delta_0 + \Omega_1$ is the union of the S_2^i (see Buss [86] Thm. 2.11).

The definition of $I\Delta_0+\Omega_1$ given above does not coincide with the version of Paris-Wilkie [87], which we will follow in Chapter 3. Their language L contains just $0,S,+,\cdot$ and $\leqslant$; in particular, $\#$ is not included. The theory $I\Delta_0+\Omega_1$ as defined by Paris and Wilkie contains the BASIC axioms for $0,S,+,\cdot$ and $\leqslant$, but not those in which $\#$ occurs; also, their system only contains induction axioms over Δ_0-formulas without $\#$. Paris and Wilkie did however introduce a function ω_1 defined by

$$\omega_1(x) = x^{|x|}$$

with a growth rate approximately equal to that of $\#$. The relation $\omega_1(x) = y$ can be expressed by a Δ_0-formula φ in which $\#$ does not occur. Therefore, the axiom $\forall x \exists y \varphi(x,y)$ (called Ω_1), stating that ω_1 is total, can be expressed in the $\#$-less language L. Paris and Wilkie include this axiom in their theory $I\Delta_0 + \Omega_1$.

Because $\#$ grows approximately as slowly as ω_1, we can conservatively add $\#$ to the language L, add the extra BASIC axioms containing $\#$, and allow induction for $\Delta_0(\#)$-formulas; thus, our name of $I\Delta_0+\Omega_1$ for the extended system, as we use it in Chapter 2, is legitimized.

Another difference between Buss and Paris and Wilkie is that the latter use a different classification of formulas. The R_1^+ -formulas which play an important part in Paris-Wilkie [87] define exactly the same class of predicates as Buss's Σ_1^b-formulas, namely NP.

$I\Delta_0$+EXP

$I\Delta_0$+EXP is a stronger extension of $I\Delta_0+\Omega_1$. It contains the axiom $EXP \equiv \forall x \forall y \exists z\, \psi(x,y,z)$, where ψ is a Δ_0-formula expressing the relation $x^y = z$ (see Pudlák[83], for such a Δ_0-formula).

$I\Sigma_1$

$I\Sigma_1$ is the strongest system that could reasonably be called a theory of bounded arithmetic. Its induction scheme is

$$A(0) \wedge \forall x(A(x) \rightarrow A(Sx)) \rightarrow \forall x A(x),$$

where A is a Σ^0_1-formula. Because $I\Sigma_1$ proves every primitive recursive function to be total, $I\Sigma_1$ is sometimes called **PRA** for primitive recursive arithmetic.

In order to prove Gödel's incompleteness theorems for S^1_2, Buss arithmetizes the usual notions of metamathematics (Buss [86], Ch. 7). It turns out that all predicates and functions needed can be Δ^b_1-defined in S^1_2; moreover, these definitions are intensionally correct in the sense of Feferman [60], i.e. the usual connections between these predicates can be proved in S^1_2. Here follows a list of some predicates used in the sequel.

Seq(w) $\Longleftrightarrow$ "w encodes a sequence"

Len(w)=a $\Longleftrightarrow$ "if w encodes a sequence, than the length of that sequence is a; otherwise a=0.

Term(v) $\Longleftrightarrow$ "v is the Gödel number of a term"

Fmla(v) $\Longleftrightarrow$ "v is the Gödel number of a formula"

Prf(u,v) $\Longleftrightarrow$ Fmla(v) and "u is the Gödel number of an $I\Delta_0+\Omega_1$-proof of the formula or sequent with Gödel number v"

$\text{Prf}^i(u,v)$ $\Longleftrightarrow$ Fmla(v) and "u is the Gödel number of an S^i_2-proof of the formula or sequent with Gödel number v"

Thm(v) $\Longleftrightarrow$ $\exists u\,\text{Prf}(u,v)$

$\text{Thm}^i(v)$ $\Longleftrightarrow$ $\exists u\,\text{Prf}^i(u,v)$

Instead of the usual numerals S^k0 of Peano arithmetic, Buss introduces the canonical term I_k to denote the natural number k. I_k is defined inductively by:

$I_0 = 0$

$I_{2k+1} = I_{2k} + (S0)$

$I_{2(k+1)} = (SS0)\cdot(I_{k+1})$

Note that the length of the term I_k is linear in the length of the binary representation of k (a fact which obviously does not hold for S^k0). The "shortness" of the canonical terms plays a crucial rôle in the proof of Σ^b_1-completeness.

Buss proves a property even stronger than Σ_1^b-completeness for S_2^1 (see Buss [86],Thm. 7.4), but we will follow the usual definition:

For any $A \in \Sigma_1^b$, with $a_1,\ldots,a_k$ all free variables occurring in A, there is a term $t_A(a_1,\ldots,a_k)$ such that

$S_2^1 \vdash A(a_1,\ldots,a_k) \to \exists w \leqslant t_A(a_1,\ldots,a_k)\mathrm{Prf}^1(w,\ulcorner A(I_{a_1},\ldots,I_{a_k})\urcorner)$.

In particular, because Prf^1 can be Δ_1^b-(and thus Σ_1^b-)defined in S_2^1, this result implies that the third Löb condition holds for S_2^1:

$S_2^1 \vdash \mathrm{Thm}^1(\ulcorner A\urcorner) \to \mathrm{Thm}^1(\ulcorner \mathrm{Thm}^1(I_{\ulcorner A\urcorner})\urcorner)$.

It is not difficult to see that all three Löb conditions hold for S_2^1 and for the extensions we consider. Because we also have Gödel's diagonalization lemma for S_2^1 and its extensions, we can prove Gödel's first and second incompleteness theorems in the usual way.

So far, it seems as if S_2^1 and $I\Delta_0+\Omega_1$ do not differ greatly from their stronger extensions $I\Delta_0$+EXP and $I\Sigma_1$: Löb's provability logic L is arithmetically sound with respect to all of them. However, there are considerable differences already between $I\Delta_0+\Omega_1$ and $I\Delta_0$+EXP, especially in the realm of interpretability (see Nelson [86], Paris and Wilkie[87], Visser [88]).

At this point, we will ramify our remarks about Σ-completeness which we made at the beginning of the introduction.

It is well-known that Σ_1^0 -completeness is provable in $I\Sigma_1$,, i.e.

If $A \in \Sigma_1^0$, then $I\Sigma_1 \vdash A \to \mathrm{Thm}_{I\Sigma_1}(\ulcorner A\urcorner)$, and in fact

$I\Sigma_1 \vdash A \to \mathrm{Thm}_Q(\ulcorner A\urcorner)$

and it is clear that essentially the same proof can be executed in $I\Delta_0$ + EXP, thus we have

If $A \in \Sigma_1^0$, then $I\Delta_0 + \mathrm{EXP} \vdash A \to \mathrm{Thm}_{I\Delta_0+\mathrm{EXP}}(\ulcorner A\urcorner)$ and

$I\Delta_0 + \mathrm{EXP} \vdash A \to \mathrm{Thm}_Q(\ulcorner A\urcorner)$ (folklore).

On the other hand, we will prove in Chapter 2 of this paper that:

If NP $\neq$ co-NP, then

$I\Delta_0+\Omega_1 \nvdash \forall b,c\,(\exists a(\mathrm{Prf}(a,c) \wedge \forall z \leqslant a\, \neg\mathrm{Prf}(z,b)) \to$

$\mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a,I_c) \wedge \forall z \leqslant a\, \neg\mathrm{Prf}(z,I_b))\urcorner))$.

Although we haven't yet done so, it seems highly probable that this result can be strengthened to:

If NP $\neq$ co-NP, then there are sentences φ,ψ such that

$$I\Delta_0+\Omega_1 \nvdash \exists a(Prf(a,\ulcorner\varphi\urcorner) \wedge \forall z \leqslant a\, \neg Prf(z,\ulcorner\psi\urcorner)) \rightarrow Thm(\ulcorner\exists a(Prf(a,I\ulcorner\varphi\urcorner) \wedge \forall z \leqslant a\, \neg Prf(z,I\ulcorner\psi\urcorner))\urcorner),$$

or abbreviated:

$$I\Delta_0+\Omega_1 \nvdash \Box\varphi \prec \Box\psi \rightarrow \Box(\Box\varphi \prec \Box\psi).$$

As the reader may have noticed, some notions from complexity theory keep cropping up in this discussion of bounded arithmetic. In fact, the two areas are so tightly knit together that many open problems in bounded arithmetic are equivalent to famous open questions in complexity theory (cf. Krajíček, Pudlák, Takeuti).
At this moment, we will turn our attention to the main problems considered by us.

Is Rosser's Theorem provable in $I\Delta_0+\Omega_1$?

Define R by Gödel's diagonalization theorem as follows:

$I\Delta_0+\Omega_1 \vdash R \leftrightarrow \exists a(Prf(a,\ulcorner\neg R\urcorner) \wedge \forall p < a\, \neg Prf(p,\ulcorner R\urcorner)),$

or, abbreviated, as:

$I\Delta_0+\Omega_1 \vdash R \leftrightarrow \Box\neg R \preccurlyeq \Box R.$

We would like to prove the formalized version of Rosser's theorem in $I\Delta_0+\Omega_1$. Thus, we want to prove for R defined above:

$I\Delta_0+\Omega_1 \vdash (\Box R \rightarrow \Box\bot) \wedge (\Box\neg R \rightarrow \Box\bot).$

The usual proof of Rosser's theorem in **PA** hinges on the fact that Guaspari and Solovay's logic R^- is sound with respect to **PA**.
R^- is the extension of **L** in which the language is augmented with witness comparison symbols, i.e. binary modalities $\preccurlyeq, \prec$ which are applicable only to those formulas having $\Box$ as the principal connective. Here follows a list of the additional axiom schemata of R^- over **L**:

(01) $\Box\varphi \rightarrow (\Box\varphi \preccurlyeq \Box\psi) \vee (\Box\psi \preccurlyeq \Box\varphi)$

(02) $\Box\varphi \preccurlyeq \Box\psi \rightarrow \Box\varphi$

(03) $(\Box\varphi \preccurlyeq \Box\psi) \wedge (\Box\psi \preccurlyeq \Box\chi) \rightarrow (\Box\varphi \preccurlyeq \Box\chi)$

(04) $(\Box\varphi \prec \Box\psi) \leftrightarrow (\Box\varphi \preccurlyeq \Box\psi) \wedge \neg(\Box\psi \preccurlyeq \Box\varphi)$

(Σ) $(\Box\varphi \preccurlyeq \Box\psi) \rightarrow \Box(\Box\varphi \preccurlyeq \Box\psi)$

(Σ) $(\Box\varphi \prec \Box\psi) \rightarrow \Box(\Box\varphi \prec \Box\psi).$

The arithmetical analogues of all but one of the principles of R^- can straightforwardly be proved in any theory of bounded arithmetic from S^1_2 upwards. The only principle which presents difficulties is (Σ). For $I\Delta_0 + EXP$ and $I\Sigma_1$, we do have the arithmetical analogue of (Σ), and thus we can prove Rosser's theorem in these stronger systems. However, as we argued before, it is highly unlikely that Σ-completeness could be proved in $I\Delta_0+\Omega_1$. Therefore, we cannot straightforwardly adapt the usual proof of Rosser's theorem to the case of $I\Delta_0+\Omega_1$.

One course of action we can take in order to remedy this problem is to look for a weaker theory than R^- which *is* arithmetically sound with respect to $I\Delta_0 + \Omega_1$, but can still prove Rosser's theorem for $I\Delta_0 + \Omega_1$. A subtheory of R^- that comes to mind is Z^-, a system introduced by Švejdar [83] in the context of generalized Rosser sentences. Z^- almost coincides with R^-, but instead of the troublesome Σ-completeness axioms it contains the scheme

(Šv) $\Box\varphi \to \Box(\Box\psi \preccurlyeq \Box\varphi \to \psi)$.

One can think of these axioms as saying that we can prove reflection (i.e. $\vdash \Box\psi \to \psi$) for "very short" proofs. Albert Visser conceived of the idea to use partial truth predicates (as described in Pudlák [86],[87]) to prove Švejdar's principle (Šv) in $I\Delta_0+\Omega_1$. We work out his idea in Chapter 3. As Z^- proves the formalized version of Rosser's theorem, the result of Chapter 3 implies that this theorem holds for $I\Delta_0+\Omega_1$.

Solovay's first incompleteness theorem and $I\Delta_0+\Omega_1$

We will make a few remarks about the more difficult- and as yet not solved- problem of extending Solovay's completeness theorem to bounded arithmetic. Proofs for some of the remarks can be found in Verbrugge[88].

In order to state our problem formally, we need one definition.

An <u>interpretation</u> $(\ )^*$ of the language of modal logic into the language of $I\Delta_0 + \Omega_1$ is a function which assigns to each modal formula φ a sentence φ^* in the language of $I\Delta_0 + \Omega_1$, and which satisfies the following requirements:

1) $(\bot)^* \equiv \; 0=1$
2) $(\;)^*$ commutes with the propositional connectives, i.e. $(\varphi \to \psi)^* \equiv \varphi^* \to \psi^*$, etc.
3) $(\Box\varphi)^* \equiv Thm(\ulcorner \varphi^* \urcorner)$. (When we consider arithmetical theories T other than $I\Delta_0 + \Omega_1$, this becomes: $(\Box\varphi)^* \equiv Thm_T(\ulcorner \varphi^* \urcorner)$.)

We are concerned with the question whether the following statement holds:

For any modal formula χ,

$\vdash_L \chi$ if and only if $I\Delta_0 + \Omega_1 \vdash \chi^*$ for every interpretation $(\;)^*$.

Or, less formally, is Löb's provability logic **L** arithmetically sound and complete with respect to $I\Delta_0 + \Omega_1$?

One part of the question has already been answered: as every theory of bounded arithmetic from S^1_2 upwards satisfies Löb's conditions, **L** is arithmetically sound with respect to each of them, and to $I\Delta_0 + \Omega_1$ in particular.

For the other direction, we will investigate whether we can adapt Solovay's proof of arithmetical completeness of **L** with respect to **PA**. We assume that the reader is familiar with the method of proof as described in e.g. Solovay [76] or Smoryński [85]. The only feature of the proof we need at the moment is the following. The proof uses the theorem stating that if $\mathbf{L} \nvdash \chi$, then there exists a finite tree-like Kripke model against χ. This model is used to construct an interpretation $(\;)^*$ for which $\mathbf{PA} \nvdash \chi^*$; the interpretation in turn is dependent on a specially constructed function h from $\mathbb{N}$ to the nodes (numbered 1,...,n) of this countermodel. The fact that certain conditions on the "limit" l of the function h can be proved in **PA** (e.g. $\mathbf{PA} \vdash l=i \to Prov(\ulcorner \neg\, l=j \urcorner)$, if $i,j \in \{1,\dots,n\}$ and not iRj), is crucial for the proof that the interpretation works.

Solovay's proof as he presented it does not make clear how much of **PA** is actually needed for the result. Recently however, Jumelet, following an idea of Franco Montagna and Dick de Jongh, (de Jongh, Jumelet, Montagna [89]) provided a formalized version of the proof in which the fixed point theorem is used to construct sentences which play the rôle of the expressions $l=i$ of Solovay's proof, and whose defining equations exactly mimic the conditions governing Solovay's function h. (The precise definitions can be found in Chapter 2 of this paper.) The alternative proof of Solovay's first completeness theorem shows that for L to be arithmetically complete with respect to some theory of arithmetic, it is sufficient that Guaspari and Solovay's logic R^- be sound with respect to the arithmetical theory in question (see Guaspari-Solovay [79]).

As in the case of Rosser's theorem, the usual proof of Solovay's completeness theorem can thus be adapted to $I\Delta_0 + EXP$ and $I\Sigma_1$. Also, just as before, the unprovability of Σ-completeness in $I\Delta_0+\Omega_1$ prevents adaptation of the proof to the case of $I\Delta_0+\Omega_1$. However, if we use Švejdars principle, we can find a proof of Solovay's completeness theorem only for a very limited class of Kripke countermodels (Verbrugge[88]).

Chapter 2. Σ-completeness and the NP = co-NP problem

In this chapter we will prove that, under the assumption that NP ≠ co-NP, the following holds:

$$I\Delta_0 + \Omega_1 \nvdash \forall b,c\, (\exists a(Prf(a,c) \wedge \forall z \leqslant a\ \neg Prf(z,b)) \rightarrow$$
$$Thm(\ulcorner \exists a(Prf(a,I_c) \wedge \forall z \leqslant a\ \neg Prf(z,I_b))\urcorner)) .$$

In the proofs of the lemmas leading up to this result we will frequently, often without mention, make use of the following fact and its corollary.

2.1 Fact (Buss [86])
Suppose A is a closed, bounded formula in the language of S^1_2, and let R be a consistent theory extending S^1_2.
Then $R \vdash A$ iff $\mathbb{N} \models A$.

2.2. Corollary (Buss [86], Prop. 8.3)
Suppose $A(\vec{a})$ is a bounded formula in the language of S^1_2,and let R be a consistent theory extending S^1_2.
If $R \vdash \forall \vec{x} A(\vec{x})$, then $\mathbb{N} \models \forall \vec{x} A(\vec{x})$.

In order to prove the main theorem of this chapter, we need to prove a few seemingly far-fetched lemmas. Their proofs borrow heavily from the formalization carried out in Buss. To make these lemmas understandable, we will go a little bit more into the formalization of the predicate Prf than we did in the introduction. Buss uses a sequent calculus akin to Takeuti's (see Takeuti [75]), and considers a proof to be formalized as a tree, of which the root corresponds to the end sequent, and the leaves to the initial sequents of the proof. Every node of the proof tree is labeled by an ordered pair <a,b>. The second member of this pair codes a sequent, and the first member codes the rule of inference by which this sequent has been derived from the sequents corresponding to the sons of the node in question (for leaves, the first member of the corresponding ordered pair codes the axiom of which the initial sequent is an instantiation).

The only extra fact we need here is that logical axioms are all numbered 0; in particular, for all terms t, the tree containing just one node labeled $<0, \ulcorner \rightarrow t=t \urcorner>$ is a proof for $\rightarrow t=t$. Because of a peculiarity in the encoding of trees, by which 0 and 1 are reserved as codes for brackets, the proof just mentioned is encoded by $<0, \ulcorner \rightarrow t=t \urcorner> +2$.

In the sequel, we will sometimes abuse Buss's conventions in order to keep the formulas legible. Thus, we will write $<0, \ulcorner \rightarrow I_d = I_d \urcorner>$ for $<0, (0 * \overline{Arrow}) ** (\ulcorner I_d \urcorner * \overline{Equals}) ** \ulcorner I_d \urcorner> +2$.

2.3. Definition.

Let $\psi(d,b)$ be the formula

$\forall z \leqslant <0, \ulcorner \rightarrow I_d = I_d \urcorner> \neg Prf(z,b)$.

2.4. Lemma.

The predicate represented by ψ is co-NP complete.

Proof.

Straightforwardly, ψ is a Π^b_1-formula, hence it represents a co-NP predicate (Buss [86], Thm. 1.8)

For the other side, viz. co-NP hardness, begin by supposing $A(a_1,\ldots,a_k) \in \Pi^b_1$. By Σ^b_1-completeness (see Ch. 1, pg. 5 or Buss[86], theorem 7.4), there is a term $r(\vec{a})$ such that

$I\Delta_0 + \Omega_1 \vdash \neg A(\vec{a}) \rightarrow \exists z \leqslant r(\vec{a}) \, Prf(z, \ulcorner \neg A(I_{a_1},\ldots,I_{a_k}) \urcorner)$,

and thus

$\mathbb{N} \models \neg A(\vec{a}) \rightarrow \exists z \leqslant r(\vec{a}) \, Prf(z, \ulcorner \neg A(I_{a_1},\ldots,I_{a_k}) \urcorner)$.

Because $r(\vec{a}) \leqslant \ulcorner I_{r(\vec{a})} \urcorner \leqslant <0, \ulcorner \rightarrow I_{r(\vec{a})} = I_{r(\vec{a})} \urcorner>$, we also have

(1) $\mathbb{N} \models \neg A(\vec{a}) \rightarrow \exists z \leqslant <0, \ulcorner \rightarrow I_{r(\vec{a})} = I_{r(\vec{a})} \urcorner> Prf(z, \ulcorner \neg A(I_{a_1},\ldots,I_{a_k}) \urcorner)$.

On the other hand,

(2) $\mathbb{N} \models \exists z \leqslant <0, \ulcorner \rightarrow I_{r(\vec{a})} = I_{r(\vec{a})} \urcorner> Prf(z, \ulcorner \neg A(I_{a_1},\ldots,I_{a_k}) \urcorner) \rightarrow \neg A(\vec{a})$;

this follows by the consistency of $I\Delta_0 + \Omega_1$ from Fact 2.1.

From (1) and (2), we conclude that

$\mathbb{N} \models A(\vec{a}) \leftrightarrow \forall z \leqslant <0, \ulcorner \rightarrow I_{r(\vec{a})} = I_{r(\vec{a})} \urcorner> \neg Prf(z, \ulcorner \neg A(I_{a_1},\ldots,I_{a_k}) \urcorner)$.

This means by the definition of ψ that

$\mathbb{N} \models A(\vec{a}) \leftrightarrow \psi(r(\vec{a}), \ulcorner \neg A(I_{a_1},\ldots,I_{a_k}) \urcorner)$.

As both $\ulcorner \neg A(Ia_1,\ldots,Ia_k)\urcorner$ and $r(\vec{a})$ can be computed from $\vec{a}$ by polynomial time functions, we have reduced the co-NP predicate A to ψ. ⊠

2.5. Lemma.
Let $B(a_1,\ldots,a_k)$ be a Π^b_1-formula representing a co-NP complete predicate.
If NP $\neq$ co-NP, then
$I\Delta_0+\Omega_1 \nvdash \forall \vec{a}[B(\vec{a}) \rightarrow Thm(\ulcorner B(Ia_1,\ldots,Ia_k)\urcorner)]$

Proof.
(The proof of this theorem is similar to a part of the proof of theorem 8.6 of Buss.)
Suppose NP $\neq$ co-NP, and suppose
$I\Delta_0+\Omega_1 \vdash \forall \vec{a}[B(\vec{a}) \rightarrow Thm(\ulcorner B(Ia_1,\ldots,Ia_k)\urcorner)]$.

Then by Parikh's theorem, there is a term $t(\vec{a})$ such that
$I\Delta_0+\Omega_1 \vdash \forall \vec{a}[B(\vec{a}) \rightarrow \exists w \leqslant t(\vec{a}) Prf(w,\ulcorner B(Ia_1,\ldots,Ia_k)\urcorner)]$
By corollary 2.2,
$\mathbb{N} \models \forall \vec{a}[B(\vec{a}) \rightarrow \exists w \leqslant t(\vec{a}) Prf(w,\ulcorner B(Ia_1,\ldots,Ia_k)\urcorner)]$

On the other hand, by fact 2.1, we have the other direction:
$\mathbb{N} \models \forall \vec{a}[\exists w \leqslant t(\vec{a}) Prf(w,\ulcorner B(Ia_1,\ldots,Ia_k)\urcorner) \rightarrow B(\vec{a})]$

Therefore we have shown that our co-NP complete predicate $B(\vec{a})$ can be represented by a Σ^b_1-formula, and thus belongs to NP, contradicting the assumption that NP $\neq$ co-NP. ⊠

2.6. Lemma.
If NP $\neq$ co-NP, then
$I\Delta_0+\Omega_1 \nvdash \forall b \forall d[\forall z \leqslant \langle 0, \ulcorner \rightarrow I_d = I_d \urcorner \rangle \neg Prf(z,b)$
$\rightarrow Thm(\ulcorner \forall z \leqslant I_{\langle 0, \ulcorner \rightarrow I_d = I_d \urcorner \rangle} \neg Prf(z, I_b)\urcorner]$

Proof.
Directly from Lemma 2.4 and Lemma 2.5. ⊠

2.7. Lemma.

$$I\Delta_0+\Omega_1 \vdash \forall b \forall d[\mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a, I_{\ulcorner \to I_d = I_d \urcorner}) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z, I_b)\urcorner)) \to \mathrm{Thm}(\ulcorner \forall z \leqslant I_{\langle 0, \ulcorner \to I_d=I_d \urcorner \rangle}\ \neg \mathrm{Prf}(z, I_b)\urcorner)].$$

Proof.

It is not difficult to see that for Buss's formalization of Prf, we have the following:

$$I\Delta_0+\Omega_1 \vdash \forall d \forall a[\mathrm{Prf}(a, \ulcorner \to I_d=I_d \urcorner) \to a \geqslant \langle 0, \ulcorner \to I_d=I_d \urcorner \rangle],$$

and thus

$$I\Delta_0+\Omega_1 \vdash \forall b \forall d[\exists a(\mathrm{Prf}(a, \ulcorner \to I_d=I_d \urcorner) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z,b)) \to \forall z \leqslant \langle 0, \ulcorner \to I_d=I_d \urcorner \rangle \neg \mathrm{Prf}(z,b)].$$

This in turn immediately implies

$$I\Delta_0+\Omega_1 \vdash \forall b \forall d[\mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a, I_{\ulcorner \to I_d = I_d \urcorner}) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z, I_b)\urcorner)) \to \mathrm{Thm}(\ulcorner \forall z \leqslant I_{\langle 0, \ulcorner \to I_d=I_d \urcorner \rangle}\ \neg \mathrm{Prf}(z, I_b)\urcorner)].$$ ⊠

2.8. Theorem.

If NP $\neq$ co-NP, then

$$I\Delta_0+\Omega_1 \nvdash \forall b,c\ (\exists a(\mathrm{Prf}(a,c) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z,b)) \to \mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a, I_c) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z, I_b))\urcorner)).$$

Proof.

Suppose that NP $\neq$ co-NP, and suppose, in order to derive a contradiction, that

$$I\Delta_0+\Omega_1 \vdash \forall b,c\ (\exists a(\mathrm{Prf}(a,c) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z,b)) \to \mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a, I_c) \wedge \forall z \leqslant a\ \neg \mathrm{Prf}(z, I_b))\urcorner)).$$

Then, in particular,

$$(1)\quad I\Delta_0+\Omega_1 \vdash \forall b,d\ [\mathrm{Prf}(\langle 0, \ulcorner \to I_d=I_d \urcorner \rangle, \ulcorner \to I_d=I_d \urcorner) \wedge \forall z \leqslant \langle 0, \ulcorner \to I_d=I_d \urcorner \rangle \neg \mathrm{Prf}(z,b) \to \mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a, I_{\ulcorner \to I_d = I_d \urcorner}) \wedge \forall z \leqslant a \neg \mathrm{Prf}(z, I_b))\urcorner)].$$

We know that

$$I\Delta_0+\Omega_1 \vdash \forall d\ [\mathrm{Prf}(\langle 0, \ulcorner \to I_d=I_d \urcorner \rangle, \ulcorner \to I_d=I_d \urcorner)].$$

Combined with (1), this implies

$$I\Delta_0+\Omega_1 \vdash \forall b,d\ [\forall z \leqslant \langle 0, \ulcorner \to I_d=I_d \urcorner \rangle \neg \mathrm{Prf}(z,b) \to \mathrm{Thm}(\ulcorner \exists a(\mathrm{Prf}(a, I_{\ulcorner \to I_d = I_d \urcorner}) \wedge \forall z \leqslant a \neg \mathrm{Prf}(z, I_b))\urcorner)].$$

Now we apply Lemma 2.7 to derive

$$I\Delta_0+\Omega_1 \vdash \forall b,d\,[\forall z \leqslant \langle 0, \ulcorner \rightarrow\ I_d=I_d \urcorner\rangle \neg Prf(z,b) \rightarrow$$
$$Thm(\ulcorner \forall z \leqslant I_{\langle 0, \ulcorner \rightarrow\ I_d=I_d \urcorner \rangle}\ \neg Prf(z,I_b)\urcorner)],$$

in contradiction with Lemma 2.6. ⊠

We can prove that provable Σ^0_1-completeness fails already for a much simpler Π^b_1-formula $\chi(a,b,c)$ defined as
$\forall x \leqslant c \forall y \leqslant c(ax^2 + by \neq c)$.
For the proof of this fact, we use the following lemma, which was pointed out to us by A. Wilkie.

2.9. Lemma. (Manders-Adelman[78])
The set of equations of the form $ax^2 + by=c$ $(a,b,c\in \mathbb{N}_{>0})$, solvable in natural numbers, is NP-complete.

Note that this result means that the formula
$\exists x \leqslant c \exists y \leqslant c(ax^2 + by=c)$ represents an NP-complete predicate, and thus that χ as defined above represents a co-NP complete predicate.

2.10. Theorem.
If NP $\neq$ co-NP, then

$$I\Delta_0+\Omega_1 \nvdash \forall a,b,c[\forall x \leqslant c \forall y \leqslant c(ax^2 + by\neq c) \rightarrow$$
$$Thm(\ulcorner \forall x \leqslant I_c \forall y \leqslant I_c(I_a x^2 + I_b y \neq I_c)\urcorner)]$$

Proof.
Directly from Lemma 2.9 and Lemma 2.5. ⊠

Chapter 3. Švejdar's principle is provable in $I\Delta_0 + \Omega_1$

In this chapter, we will present a proof of the fact that $I\Delta_0 + \Omega_1$ proves Švejdar's principle, i.e. for all φ,ψ:

$I\Delta_0+\Omega_1 \vdash Thm(\ulcorner\varphi\urcorner)\rightarrow$

$Thm(\ulcorner\exists a(Prf(a,\ulcorner\psi\urcorner)\wedge\forall z<a\neg Prf(z,\ulcorner\varphi\urcorner))\rightarrow\psi\urcorner)$, in this chapter abbreviated as $I\Delta_0+\Omega_1 \vdash \Box\varphi \rightarrow \Box(\Box\psi \preccurlyeq \Box\varphi \rightarrow \psi)$.

The idea of the proof is Albert Visser's. In the proof, we will use the existence of a partial truth (or satisfaction) predicate Sat_n for formulas of length $\leqslant$ n. The intended meaning of $Sat_n(x,w)$ will be "the formula of length $\leqslant$ n with Gödel number x is satisfied by the assignment sequence coded by w". Similarly, we will need a predicate $Sat_{n,\Delta}$ with as intended meaning: " the Δ_0-formula of length $\leqslant$ n with Gödel number x is satisfied by the assignment sequence coded by w".

Pudlák [86] has constructed partial truth predicates much like the ones we need . (An analogous construction, where Sat_n is related to quantifier depth instead of length, can be found in Pudlák [87].)

In order to be able to adapt his construction, we need a few more assumptions and definitions.

First of all, when formalizing, we view $I\Delta_0+\Omega_1$ in a restricted way more akin to Paris and Wilkie [87] than to Buss [86]. Thus, our language contains symbols 0, S, +, $\cdot$, but not $\#$. Additionally, it contains relation symbols = and $\leqslant$, logical symbols $\neg$, $\rightarrow$, $\leftrightarrow$ and $\forall$, and variables $v_1, v_2, \ldots$. (The at first sight superfluous appearance of $\leftrightarrow$ will be explained in the proof of Lemma 3.6.)

With regard to logical axioms, we will use a Hilbert-type system as in Paris and Wilkie [87], including extra axioms to relate $\leftrightarrow$ to $\rightarrow$ and $\neg$. As non-logical axioms we will consider a set containing: a finite number of open formulas defining the basic properties of the function and predicate symbols of the language; a formula $\forall x\forall y\exists z\varphi(x,y,z)$, where φ is the Δ_0-formula properly expressing the <u>relation</u> $x\#y=z$; and finally the scheme of induction for Δ_0-formulas.

For this adapted system, we can define the appropriate Δ_1^b-predicates Term(v), Fmla(v), Sentence(v), Prf(u,v) as in S_2^1, using Buss's Gödel numbering.
In this chapter, we denote concatenation of sequences sloppily by juxtaposition, and we leave out some outer parentheses; thus, for example, $y\ulcorner\rightarrow\urcorner z$ stands for Buss's
$(0*\overline{\text{LParen}})**(y*\overline{\text{Implies}})**(z*\overline{\text{RParen}})$.

3.1. Definition.
$w =_i w' \equiv \forall t(t \leqslant Len(w) \wedge t \neq i \rightarrow \beta(t,w) = \beta(t,w'))$ (where $\beta(t,w)$ denotes the t-th value of the sequence coded by w)

$Fmla_n(v) \equiv$ "v is the Gödel number of a formula of length $\leqslant$ n" i.e.
$Fmla(v) \wedge Len(v) \leqslant n$

$Fmla_{n,\Delta}(v) \equiv$ "v is the Gödel number of a Δ_0-formula of length $\leqslant$ n"

$Evalseq(w,x) \equiv Seq(w) \wedge (Fmla(x) \vee Term(x)) \wedge$
$\forall i$("the variable v_i occurs in the term or formula with Gödel number x" $\rightarrow Len(w) \geqslant i$)

We can, by the method of p-inductive definitions, define a function Val such that, if $t(v_{i_1},\ldots,v_{i_n})$ is a term of the (restricted) language of $I\Delta_0+\Omega_1$ and w codes a sequence evaluating all variables $v_{i_1},\ldots,v_{i_n}$ appearing in t, then $Val(\ulcorner t\urcorner,w)$ gives the value of $t(\beta(i_1,w),\ldots,\beta(i_n,w))$.

3.2. Definition.
Let Val satisfy the following conditions:

$\neg Term(t) \vee \neg Evalseq(w,t) \rightarrow Val(t,w)=0$

$$
\begin{aligned}
&Term(t,w) \wedge Evalseq(w,x) \rightarrow \\
&\qquad (t=\ulcorner 0 \urcorner \wedge Val(t)=0) \vee \\
&\qquad \exists i(t=\ulcorner v_i \urcorner \wedge Val(t,w)=\beta(i,w)) \vee \\
&\qquad \exists t_1 \exists t_2(Term(t_1) \wedge Term(t_2) \wedge \\
&\qquad ((t=\ulcorner S \urcorner t_1 \wedge Val(t,w)=S(Val(t_1,w))) \vee \\
&\qquad (t=t_1 \ulcorner + \urcorner t_2 \wedge Val(t,w)=Val(t_1,w)+Val(t_2,w)) \vee \\
&\qquad (t=t_1 \ulcorner . \urcorner t_2 \wedge Val(t,w)=Val(t_1,w).Val(t_2,w))))
\end{aligned}
$$

By induction, we can show that $t\#w$ will be a bound for $Val(t,w)$. Thus, by Theorem 7.3 of Buss[86], Val is Σ_1^b-definable in S_2^1; furthermore, the definition of Val in S_2^1 is intensionally correct in that properties of Val can be proved in S_2^1 (and thus also in $I\Delta_0+\Omega_1$) by the use of induction.
In the sequel, we will freely make use of induction for $\Delta_0(Val)$-formulas in $I\Delta_0+\Omega_1$, as is justified by the $I\Delta_0+\Omega_1$-analogues of Buss's Theorem 2.2 and Corollary 2.3.
We will especially need the following lemma.

3.3. Lemma.
If t is a term with free variables among $v_{i_1},\dots,v_{i_m}$, then
$I\Delta_0+\Omega_1 \vdash Evalseq(w,\ulcorner t \urcorner) \rightarrow Val(\ulcorner t \urcorner,w)=t[\beta(i_1,w),\dots,\beta(i_m,w)]$.

Proof.
Straightforward by induction on the build up of t.

3.4. Definition.
$s(i,t,w) = (Subseq(w,1,i)*Val(t,w))**Subseq(w,i+1,Len(w)+1)$
Thus, if w is a sequence of length $\geqslant i$, $s(i,t,w)$ denotes the sequence which is identical to w, except that $Val(t,w)$ appears in the i-th place.

3.5. Definition.
We say that $Sat_n(x,w)$ is a <u>partial definition of truth for formulas of length $\leqslant n$</u> in $I\Delta_0+\Omega_1$ iff

$$I\Delta_0+\Omega_1 \vdash \mathrm{Fmla}_n(x) \wedge \mathrm{Evalseq}(w,x) \rightarrow \{\mathrm{Sat}_n(x,w) \leftrightarrow$$
$$[\exists t,t' \leqslant x(\mathrm{Term}(t) \wedge \mathrm{Term}(t') \wedge x = t^{\ulcorner} = {}^{\urcorner}t' \wedge \mathrm{Val}(t,w) = \mathrm{Val}(t',w)) \vee$$
$$\exists t,t' \leqslant x(\mathrm{Term}(t) \wedge \mathrm{Term}(t') \wedge x = t^{\ulcorner} \leqslant {}^{\urcorner}t' \wedge \mathrm{Val}(t,w) \leqslant \mathrm{Val}(t',w)) \vee$$
$$\exists y \leqslant x(x = {}^{\ulcorner}\neg{}^{\urcorner}y \wedge \neg \mathrm{Sat}_n(y,w)) \vee$$
$$\exists y,z \leqslant x(x = y^{\ulcorner} \rightarrow {}^{\urcorner}z \wedge (\mathrm{Sat}_n(y,w) \rightarrow \mathrm{Sat}_n(z,w))) \vee$$
$$\exists y,z \leqslant x(x = y^{\ulcorner} \leftrightarrow {}^{\urcorner}z \wedge (\mathrm{Sat}_n(y,w) \leftrightarrow \mathrm{Sat}_n(z,w))) \vee$$
$$\exists y,i \leqslant x(x = {}^{\ulcorner}\forall v_i{}^{\urcorner}y \wedge \forall w'(w =_i w' \rightarrow \mathrm{Sat}_n(y,w'))) \vee$$
$$\exists y,i,t \leqslant x(\mathrm{Term}(t) \wedge x = {}^{\ulcorner}(\forall v_i \leqslant {}^{\urcorner}t^{\ulcorner}){}^{\urcorner}y \wedge$$
$$\forall w' \leqslant s(i,t,w)(w =_i w' \wedge \beta(i,w) \leqslant \mathrm{Val}(t,w) \rightarrow \mathrm{Sat}_n(y,w')))]\}$$

We denote the part between brackets [] on the right hand side of the equivalence by $\Sigma(\mathrm{Sat}_n,x,w)$; note that these are just Tarski's conditions.

Similarly, we say that $\mathrm{Sat}_{n,\Delta}(x,w)$ is a <u>partial definition of truth for Δ_0-formulas of length $\leqslant n$</u> in $I\Delta_0+\Omega_1$ iff

$$I\Delta_0+\Omega_1 \vdash \mathrm{Fmla}_{n,\Delta}(x) \wedge \mathrm{Evalseq}(w,x) \rightarrow \{\mathrm{Sat}_{n,\Delta}(x,w) \leftrightarrow$$
$$[\exists t,t' \leqslant x(\mathrm{Term}(t) \wedge \mathrm{Term}(t') \wedge x = t^{\ulcorner} = {}^{\urcorner}t' \wedge \mathrm{Val}(t,w) = \mathrm{Val}(t',w)) \vee$$
$$\exists t,t' \leqslant x(\mathrm{Term}(t) \wedge \mathrm{Term}(t') \wedge x = t^{\ulcorner} \leqslant {}^{\urcorner}t' \wedge \mathrm{Val}(t,w) \leqslant \mathrm{Val}(t',w)) \vee$$
$$\exists y \leqslant x(x = {}^{\ulcorner}\neg{}^{\urcorner}y \wedge \neg \mathrm{Sat}_{n,\Delta}(y,w)) \vee$$
$$\exists y,z \leqslant x(x = y^{\ulcorner} \rightarrow {}^{\urcorner}z \wedge (\mathrm{Sat}_{n,\Delta}(y,w) \rightarrow \mathrm{Sat}_{n,\Delta}(z,w))) \vee$$
$$\exists y,z \leqslant x(x = y^{\ulcorner} \leftrightarrow {}^{\urcorner}z \wedge (\mathrm{Sat}_{n,\Delta}(y,w) \leftrightarrow \mathrm{Sat}_{n,\Delta}(z,w))) \vee$$
$$\exists y,i,t \leqslant x(\mathrm{Term}(t) \wedge x = {}^{\ulcorner}(\forall v_i \leqslant {}^{\urcorner}t^{\ulcorner}){}^{\urcorner}y \wedge$$
$$\forall w' \leqslant s(i,t,w)(w =_i w' \wedge \beta(i,w) \leqslant \mathrm{Val}(t,w) \rightarrow \mathrm{Sat}_{n,\Delta}(y,w')))]\}$$

We denote the part between brackets [] on the right hand side of the equivalence by $\Sigma_\Delta(\mathrm{Sat}_{n,\Delta},x,w)$. Note that the only difference between $\Sigma(\mathrm{Sat}_n,x,w)$ and $\Sigma_\Delta(\mathrm{Sat}_{n,\Delta},x,w)$ is that in the latter the disjunct for the unbounded quantifier $\forall$ is left out.

In the proof of the main theorem of this chapter, we will reason inside $I\Delta_0+\Omega_1$, and we will need the existence of Gödel numbers standing for formulas Sat_n that provably satisfy the conditions of the preceding definition.
Therefore, in the proofs below, which are given in an unformalized way, we take care that the formulas Sat_n and the proofs that they have the right properties be bounded by suitable terms. The following lemmas provide us with such formulas.

Pudlák [86] proves similar lemmas for a language without function symbols; cf. also Pudlák [87]. Below, we sketch the adaptation of his method to our case. The parallel construction of a $\Delta_0(Val)$-formula $Sat_{n,\Delta}$ which works for Δ_0-formulas is peculiar to this paper. We use the formula $Sat_{n,\Delta}$ only in our proof that Sat_n preserves the Δ_0-induction axioms, but there its use is essential.

3.6. Lemma

There exist formulas $Sat_n(x,w)$ for n=0,1,2,... of lengths linear in n, and such that $I\Delta_0+\Omega_1$ proves by a proof of length linear in n that $Sat_{n+1}(x,w) \leftrightarrow \Sigma(Sat_n,x,w)$.

Proof.

Sat_n is constructed by recursion. We can define Sat_0 arbitrarily, as there are no formulas of length $\leqslant 0$. If we have the formula Sat_k, we obtain Sat_{k+1} by substituting Sat_k for Sat_n in the formula $\Sigma(Sat_n,x,w)$ defined above.

Remember that we have to ensure that the length of the formula Sat_n grows only linearly in n. However, if we straightforwardly used Σ as defined above, the length of Sat_n would grow exponentially in n, as $\Sigma(Sat_n,x,w)$ contains more than one occurrence of Sat_n.

Therefore, we use a general technique described in Ferrante-Rackoff [79, Chapter 7] to replace $\Sigma(Sat_n,x,w)$ by a formula $\Sigma'(Sat_n,x,w)$ equivalent to $\Sigma(Sat_n,x,w)$ in predicate logic, which contains only one occurrence of Sat_n. (In our case, we actually need a little bit more than predicate logic, e.g. we need $S0\neq0$; this is so because we want to take care that all newly introduced bound quantifiers are bounded by the term $S0$, in contrast to Ferrante-Rackoff. We assume in the sequel that all proofs of Ferrante-Rackoff are adapted to the bounded quantifier case.) The idea behind the technique can be exhibited by a simple example.

Suppose we want to find an equivalent with only one occurrence of Sat_n for the following formula:

$$Sat_n(u,w) \wedge \neg Sat_n(v,w).$$

This formula is easily seen to be equivalent to

$$\exists y_1, y_1', y_2, y_2' \leqslant S0\,((y_1 = y_1' \wedge y_2 \neq y_2') \wedge (y_1 = y_1' \leftrightarrow Sat_n(u,w)) \wedge (y_2 = y_2' \leftrightarrow Sat_n(v,w))),$$

which formula we can in turn replace by

$$(*)\ \exists y_1, y_1', y_2, y_2' \leqslant S0\,((y_1 = y_1' \wedge y_2 \neq y_2') \wedge \forall y, y' \leqslant S0, \forall z_1, z_2 \leqslant \max(u,v,w)\ (((y = y_1 \wedge y' = y_1' \wedge z_1 = u \wedge z_2 = w) \vee (y = y_2 \wedge y' = y_2' \wedge z_1 = v \wedge z_2 = w)) \rightarrow (y = y' \leftrightarrow Sat_n(z_1, z_2))))$$

Notice that we have introduced eight new bound variables (namely $y_1, y_1', y_2, y_2', y, y', z_1, z_2$) in the construction of the formula (*) containing only one occurrence of Sat_n. At first sight, it may seem that we have to introduce new bound variables at every step from $Sat_n(x,w)$ to $\Sigma(Sat_n,x,w)$ in order to avoid clashes of variables. However, if we introduced new variables at every step from $Sat_n(x,w)$ to $\Sigma(Sat_n,x,w)$, then the length of Sat_n would be at least of the order of $n.{}^2\log n$, because the length of variables increases as ${}^2\log n$. Let's look at an example to see how we can be thrifty and "recycle" our bound variables.

If $\exists u \exists v(*)$ were our $\Sigma(Sat_n,x,w)$, we would have to substitute $Sat_k(z_1,z_2)$ in constructing Sat_{k+1} from Sat_k. Suppose, still as an example, that for a certain k Sat_k is the formula $\forall z_1 \forall z_2 (z_1 \leqslant x \vee z_2 \leqslant w)$. By the usual methods, we would have to take an alphabetical variant of Sat_k in which z_1, z_2 are free for x,w in order to be able to use the substitution instance $Sat_k(z_1,z_2)$. However, we use an economical technique from Ferrante-Rackoff [79, Chapter 7], taking for $Sat_k(z_1,z_2)$ in the example above the formula $\forall x \forall w (x \leqslant z_1 \vee w \leqslant z_2)$.

More general, we substitute, instead of $Sat_k(z_1,z_2)$, the logically equivalent formula $Sat_k{}^{z_1,z_2|x,w}(x,w)$, obtained by replacing all free *and* bound occurrences of z_1, resp. z_2, by x, resp. w, and vice versa. In this way, clashes of variables are avoided without introducing new bound variables. Thus, the only variables that will occur (free or bound) in any of the alternative Sat_n's are $x, w, u, v, y_1, y_1', y_2, y_2', y, y', z_1, z_2$ and the variables occurring in Sat_0.

Remark. Perhaps surprisingly, the above proof uses the inclusion of $\leftrightarrow$ in the language in an essential way. There is no way to rewrite the formula (*) in such a way that $\leftrightarrow$ is replaced by an equivalent using only $\rightarrow, \neg$, and such that Sat_n still appears only once.

We will write $\Sigma'(Sat_n,x,w)$ for the equivalent of $\Sigma(Sat_n,x,w)$ resulting from an application of the techniques described above. The length of Sat_n thus constructed via iterated application of Σ' to Sat_0 is indeed linear in n (see Ferrante-Rackoff [79, Chapter 7]); moreover, for all n, the *shape* of the proof of $\Sigma(Sat_n,x,w) \leftrightarrow \Sigma'(Sat_n,x,w)$ is the same. Thus, the proofs of $\Sigma(Sat_n,x,w) \leftrightarrow \Sigma'(Sat_n,x,w)$ grow linearly in n. Hence, as $Sat_{n+1}(x,w) \equiv \Sigma'(Sat_n,x,w)$, we have

(A) $I\Delta_0+\Omega_1 \vdash Sat_{n+1}(x,w) \leftrightarrow \Sigma(Sat_n,x,w)$ by a proof of length linear in n. ⊠

3.7. Lemma.

$I\Delta_0+\Omega_1$ proves by a proof of length of the order of n^2 that the formula $Sat_n(x,w)$ as constructed in Lemma 3.6 is a partial definition of truth for formulas of length $\leqslant$ n.

Proof.

We want to prove that Sat_n is a partial definition of truth for formulas of length $\leqslant$ n in $I\Delta_0+\Omega_1$, i.e. that

$I\Delta_0+\Omega_1 \vdash Fmla_n(x) \wedge Evalseq(w,x) \rightarrow (Sat_n(x,w) \leftrightarrow \Sigma(Sat_n,x,w))$.

By (A) above (in the proof of Lemma 3.6), it suffices to show that

$I\Delta_0+\Omega_1 \vdash Fmla_n(x) \wedge Evalseq(w,x) \rightarrow (Sat_n(x,w) \leftrightarrow Sat_{n+1}(x,w))$

by a proof of length of the order of n^2.

.

This can be proved by induction on n (see Pudlák [86]). In fact, when we define

$\Phi_n \equiv \forall x \forall w(Fmla_n(x) \wedge Evalseq(w,x) \rightarrow (Sat_n(x,w) \leftrightarrow Sat_{n+1}(x,w)))$,

the length of the proofs of $\Phi_n \rightarrow \Phi_{n+1}$ in $I\Delta_0+\Omega_1$ will have a *shape* which does not depend on n. This will be elucidated by an example. Suppose we want to prove $I\Delta_0 + \Omega_1 \vdash \Phi_n \rightarrow \Phi_{n+1}$. We reason inside $I\Delta_0+\Omega_1$, and we assume Φ_n, $Fmla_{n+1}(x)$ and $Evalseq(w,x)$.

Now we have to show that $Sat_{n+1}(x,w) \leftrightarrow Sat_{n+2}(x,w)$. By (A) above, we have proofs of length linear in n of

(1.a) $Sat_{n+1}(x,w) \leftrightarrow \Sigma(Sat_n,x,w)$ and

(1.b) $Sat_{n+2}(x,w) \leftrightarrow \Sigma(Sat_{n+1},x,w)$.

Thus, we can proceed by distinguishing the cases.

Atomic formulas provide no difficulties.

If $x = y \ulcorner\rightarrow\urcorner z$ we reason as follows. By (1.a) and (1.b) we have proofs of length linear in n of

(2.a) $Sat_{n+1}(x,w) \leftrightarrow (Sat_n(y,w) \rightarrow Sat_n(z,w))$ and

(2.b) $Sat_{n+2}(x,w) \leftrightarrow (Sat_{n+1}(y,w) \rightarrow Sat_{n+1}(z,w))$.

Because $Fmla_{n+1}(x)$ and $Evalseq(w,x)$, we have $Fmla_n(y)$, $Fmla_n(z)$, $Evalseq(w,y)$ and $Evalseq(w,z)$. Therefore, we may apply Φ_n twice to conclude

(3.a) $Sat_n(y,w) \leftrightarrow Sat_{n+1}(y,w)$ and

(3.b) $Sat_n(z,w) \leftrightarrow Sat_{n+1}(z,w)$.

Combining (2) and (3), we see that the right hand sides of (2) are equivalent, and thus the left hand sides are equivalent as well.

The other cases are analogous. We can observe that every proof in $I\Delta_0+\Omega_1$ of $\Phi_n \rightarrow \Phi_{n+1}$ is really the instantiation of a single proof scheme; Thus, the length of the proofs of $\Phi_n \rightarrow \Phi_{n+1}$ increases only linearly in n, so that the length of the proof of

$\forall x \forall w(Fmla_n(x) \wedge Evalseq(w,x) \rightarrow (Sat_n(x,w) \leftrightarrow Sat_{n+1}(x,w)))$

in $I\Delta_0+\Omega_1$ is of the order n^2. ⊠

3.8. Lemma.

There exist formulas $Sat_{n,\Delta}(x,w)$ for $n=0,1,2,\ldots$ of lengths linear in n, and such that $I\Delta_0+\Omega_1$ proves by a proof of length linear in n that $Sat_{n+1,\Delta}(x,w) \leftrightarrow \Sigma_\Delta(Sat_{n,\Delta},x,w)$. The resulting formulas $Sat_{n,\Delta}(x,w)$ are $\Delta_0(Val)$-formulas.

Proof.

Completely analogous to the proof of Lemma 3.6. Because $\Sigma_\Delta(Sat_{n,\Delta},x,w)$ contains only bounded quantifiers, and because all bound quantifiers introduced by the Ferrante-Rackoff method are bounded as well, the resulting formulas are indeed Δ_0-Val.

3.9. Lemma.
$I\Delta_0+\Omega_1$ proves by a proof of length of the order of n^2 that the formula $Sat_{n,\Delta}(x,w)$ as constructed in Lemma 3.8 is a partial definition of truth for Δ_0-formulas of length $\leqslant$ n.

Proof.
We adapt the proof of Lemma 3.7, incorporating the fact that we are concerned with Δ_0-formulas only. Thus instead of Φ_n, we define

$$\Phi_{n,\Delta} \equiv \forall x \forall w(Fmla_{n,\Delta}(x) \wedge Evalseq(w,x) \rightarrow (Sat_{n,\Delta}(x,w) \leftrightarrow Sat_{n+1,\Delta}(x,w))).$$

The proof of $\Phi_{n,\Delta} \rightarrow \Phi_{n+1,\Delta}$ runs along the same lines as the proof of $\Phi_n \rightarrow \Phi_{n+1}$, using the extra fact that if $x = y^{\ulcorner} \rightarrow {}^{\urcorner}z$ and $Fmla_{n+1,\Delta}(x)$, then $Fmla_{n,\Delta}(y)$ and $Fmla_{n,\Delta}(z)$, etc. ⊠

We now show that the partial definition of truth can be proven to be really a partial truth definition in the standard sense, by proofs of quadratic length.

3.10. Lemma (cf. Pudlák [86],[87])
There exists a constant K such that for every formula φ with free variables among $v_{i_1},\ldots,v_{i_m}$ and for every n with $Len(\ulcorner\varphi\urcorner) \leqslant n$:

a) $I\Delta_0+\Omega_1 \vdash \forall w(Evalseq(w,\ulcorner\varphi\urcorner) \rightarrow (Sat_n(\ulcorner\varphi\urcorner,w) \leftrightarrow \varphi[\beta(i_1,w),\ldots,\beta(i_m,w)]))$

by a proof of length $\leqslant K.n^2$.

b) Moreover, if φ is a Δ_0-formula, we also have

$I\Delta_0 + \Omega_1 \vdash \forall w(Evalseq(w,\ulcorner\varphi\urcorner) \rightarrow (Sat_{n,\Delta}(\ulcorner\varphi\urcorner,w) \leftrightarrow \varphi[\beta(i_1,w),\ldots,\beta(i_m,w)]))$

by a proof of length $\leqslant K.n^2$.

Proof.
By cases. If φ is an atomic formula $t \leqslant t'$ of length $\leqslant n$ and with free variables among $v_{i_1},\ldots,v_{i_m}$, Lemma 3.3.1 gives

$$I\Delta_0+\Omega_1 \vdash \forall w(Evalseq(w,\ulcorner t \leqslant t'\urcorner) \rightarrow (Sat_n(\ulcorner t \leqslant t'\urcorner,w) \leftrightarrow Val(\ulcorner t\urcorner,w) \leqslant Val(\ulcorner t'\urcorner,w))$$

by a proof of length linear in n. By Lemma 3.3, we can then conclude that

$I\Delta_0+\Omega_1 \vdash \forall w(\mathrm{Evalseq}(w,\ulcorner t \leqslant t' \urcorner) \rightarrow$

$(\mathrm{Sat}_n(\ulcorner t \leqslant t' \urcorner, w) \leftrightarrow t \leqslant t'[\beta(i_1,w),\ldots,\beta(i_m,w)]))$

by a proof of length linear in n. Similarly if φ is $t=t'$.

For the non-atomic cases, we define

$\Psi_k(\psi) \equiv \forall w(\mathrm{Evalseq}(w,\ulcorner \psi \urcorner) \rightarrow$

$(\mathrm{Sat}_k(\ulcorner \psi \urcorner, w) \leftrightarrow \psi[\beta(i_1,w),\ldots,\beta(i_m,w)]))$.

Every formula φ of length $\leqslant n$ is built up from atomic formulas in at most n steps. Therefore, if we can prove by proofs of length linear in k that

$\Psi_{k-1}(\psi) \rightarrow \Psi_k(\neg\psi)$ if $\mathrm{Len}(\ulcorner \neg\psi \urcorner) \leqslant k$

$\Psi_{k-1}(\psi) \wedge \Psi_{k-1}(\chi) \rightarrow \Psi_k(\psi \rightarrow \chi)$ if $\mathrm{Len}(\ulcorner \psi \rightarrow \chi \urcorner) \leqslant k$

$\Psi_{k-1}(\psi) \wedge \Psi_{k-1}(\chi) \rightarrow \Psi_k(\psi \leftrightarrow \chi)$ if $\mathrm{Len}(\ulcorner \psi \leftrightarrow \chi \urcorner) \leqslant k$

$\Psi_{k-1}(\psi) \rightarrow \Psi_k(\forall v_i \psi)$ if $\mathrm{Len}(\ulcorner \forall v_i \psi \urcorner) \leqslant k$

$\Psi_{k-1}(\psi) \rightarrow \Psi_k((\forall v_i \leqslant t)\psi)$ if $\mathrm{Len}(\ulcorner (\forall v_i \leqslant t)\psi \urcorner) \leqslant k$,

then we have for every formula φ of length $\leqslant n$ a proof of $\Psi_n(\varphi)$ of length of the order of n^2, and we are done.

We will give the proof for the first case only; the other three are proved in a similar way.

Suppose $\mathrm{Fmla}_k(\neg\psi) \wedge \mathrm{Evalseq}(w,\ulcorner \neg\psi \urcorner)$, and suppose $\Psi_{k-1}(\psi)$. By Lemma 3.6, we have a proof of length linear in k of

(1) $\mathrm{Evalseq}(w,\ulcorner \neg\psi \urcorner) \rightarrow (\mathrm{Sat}_k(\ulcorner \neg\psi \urcorner, w) \leftrightarrow \neg \mathrm{Sat}_{k-1}(\ulcorner \psi \urcorner, w))$.

Because $\mathrm{Evalseq}(w,\ulcorner \neg\psi \urcorner) \rightarrow \mathrm{Evalseq}(w,\ulcorner \psi \urcorner)$, we have, by $\Psi_{k-1}(\psi)$,

(2) $\mathrm{Evalseq}(w,\ulcorner \neg\psi \urcorner) \rightarrow (\neg \mathrm{Sat}_{k-1}(\ulcorner \psi \urcorner, w) \leftrightarrow \neg\psi[\beta(i_1,w),\ldots,\beta(i_m,w)])$.

Combining (1) and (2), we have a proof of length linear in k of

$\forall w(\mathrm{Evalseq}(w,\ulcorner \neg\psi \urcorner) \rightarrow$

$(\mathrm{Sat}_k(\ulcorner \neg\psi \urcorner, w) \leftrightarrow \neg\psi[\beta(i_1,w),\ldots,\beta(i_m,w)])$, i.e. $\Psi_k(\neg\psi)$. ⊠

3.11. Lemma.

$I\Delta_0+\Omega_1$ proves by a proof of length of the order of n^2 that Sat_n preserves the logical rules (Modus Ponens and Generalization) for formulas of length $\leqslant n$, i.e.

$I\Delta_0+\Omega_1 \vdash \mathrm{Fmla}_n(y \ulcorner \rightarrow \urcorner z) \wedge \mathrm{Evalseq}(w, y \ulcorner \rightarrow \urcorner z) \wedge \mathrm{Sat}_n(y,w) \wedge$

$\mathrm{Sat}_n(y \ulcorner \rightarrow \urcorner z, w) \rightarrow \mathrm{Sat}_n(z,w)$

$I\Delta_0+\Omega_1 \vdash \mathrm{Fmla}_n(\ulcorner \forall v_i \urcorner y) \wedge \mathrm{Evalseq}(w, \ulcorner \forall v_i \urcorner y) \wedge$

$\forall w'(w =_i w' \rightarrow \mathrm{Sat}_n(y,w')) \rightarrow \mathrm{Sat}_n(\ulcorner \forall v_i \urcorner y, w)$

Proof.
Immediately from Lemma 3.7. ⊠

3.12. Lemma.
$I\Delta_0+\Omega_1$ proves by a proof of length of the order of n^2 that Sat_n preserves the logical axioms and the equality axioms for formulas of length $\leqslant n$, e.g. axiom scheme (1) of Paris-Wilkie[87]:

$$(1) I\Delta_0+\Omega_1 \vdash Fmla_n(y\ulcorner \rightarrow (\urcorner z \ulcorner \rightarrow \urcorner y \ulcorner)\urcorner) \wedge$$
$$Evalseq(w,y\ulcorner \rightarrow (\urcorner z \ulcorner \rightarrow \urcorner y \ulcorner)\urcorner) \rightarrow$$
$$Sat_n(y\ulcorner \rightarrow (\urcorner z \ulcorner \rightarrow \urcorner y \ulcorner)\urcorner, w)$$

Similarly for the other propositional axiom schemes (2) and (3) and the extra axioms relating $\leftrightarrow$ to $\rightarrow$ and $\neg$.
Corresponding to axiom schemes (4), (5) and (6) we have:

$$(4) I\Delta_0+\Omega_1 \vdash Fmla_n(\ulcorner \forall v_i \urcorner y \rightarrow Sub(y,\ulcorner v_i \urcorner,t)) \wedge$$
$$Evalseq(w,\ulcorner \forall v_i \urcorner y \rightarrow Sub(y,\ulcorner v_i \urcorner,t) \wedge SubOK(y,\ulcorner v_i \urcorner,t) \rightarrow$$
$$Sat_n(\ulcorner \forall v_i \urcorner y \rightarrow Sub(y,\ulcorner v_i \urcorner,t),w)$$

(where $SubOK(y,\ulcorner v_i \urcorner,t)$ is Buss's formalization of "the term with Gödel number t is free for the variable v_i in the (term or) formula with Gödel number y")

$$(5) I\Delta_0+\Omega_1 \vdash Fmla_n(\ulcorner \forall v_i(\urcorner y \ulcorner \rightarrow \urcorner z \ulcorner) \rightarrow (\urcorner y \ulcorner \rightarrow \forall v_i \urcorner z \ulcorner)\urcorner) \wedge$$
$$Evalseq(w,\ulcorner \forall v_i(\urcorner y \ulcorner \rightarrow \urcorner z \ulcorner) \rightarrow (\urcorner y \ulcorner \rightarrow \forall v_i \urcorner z \ulcorner)\urcorner) \wedge$$
"v_i does not appear free in the formula with Gödel number y" $\rightarrow$
$$Sat_n(\ulcorner \forall v_i(\urcorner y \ulcorner \rightarrow \urcorner z \ulcorner) \rightarrow (\urcorner y \ulcorner \rightarrow \forall v_i \urcorner z \ulcorner)\urcorner,w).$$

$$(6) I\Delta_0+\Omega_1 \vdash Fmla_n(v_1\ulcorner = \urcorner v_1) \wedge Evalseq(w,v_1\ulcorner = \urcorner v_1) \rightarrow Sat_n(v_1\ulcorner = \urcorner v_1,w)$$

and

$$I\Delta_0+\Omega_1 \vdash Fmla_n(v_i\ulcorner = \urcorner v_j \ulcorner \rightarrow (\urcorner y \ulcorner \rightarrow \urcorner z \ulcorner)\urcorner) \wedge$$
$$Evalseq(w,v_i\ulcorner = \urcorner v_j \ulcorner \rightarrow (\urcorner y \ulcorner \rightarrow \urcorner z \ulcorner)\urcorner) \wedge$$
$$SubOK(y,\ulcorner v_i \urcorner,\ulcorner v_j \urcorner) \wedge Somesub(z,y,\ulcorner v_i \urcorner,\ulcorner v_j \urcorner) \rightarrow$$
$$Sat_n(v_i\ulcorner = \urcorner v_j \ulcorner \rightarrow (\urcorner y \ulcorner \rightarrow \urcorner z \ulcorner)\urcorner,w)$$

(where $Somesub(z,y,\ulcorner v_i \urcorner,\ulcorner v_j \urcorner)$ is the formalization of "the formula with Gödel number z is the result of substituting the term v_j for some of the occurrences of v_i in the formula with Gödel number y")

Proof.

For the propositional axiom schemes (1),(2) and (3) and the extra ones, the results follow almost immediately from Lemma 3.7.

For (4), we need proofs in $I\Delta_0+\Omega_1$ of length of the order of n^2 of

$$Fmla_n(\ulcorner\forall v_i\urcorner y\to Sub(y,\ulcorner v_i\urcorner,t))\wedge$$
$$Evalseq(w,\ulcorner\forall v_i\urcorner y\to Sub(y,\ulcorner v_i\urcorner,t)\wedge SubOK(y,\ulcorner v_i\urcorner,t)\to$$
$$Sat_n(Sub(y,\ulcorner v_i\urcorner,t),w)\leftrightarrow Sat_n(y,s(i,t,w))$$

("Call by name / call by value"). This can be proved by induction on n, in a way similar to the proofs of Lemma 3.7. The rest of (4) then follows by Lemma 3.7 itself.

For (5), we need proofs in $I\Delta_0+\Omega_1$ of length of the order of n^2 of

$$Fmla_n(\ulcorner\forall v_i(\urcorner y\ulcorner\to\urcorner z\ulcorner)\to(\urcorner y\ulcorner\to\forall v_i\urcorner z\ulcorner)\urcorner)\wedge$$
$$Evalseq(w,\ulcorner\forall v_i(\urcorner y\ulcorner\to\urcorner z\ulcorner)\to(\urcorner y\ulcorner\to\forall v_i\urcorner z\ulcorner)\urcorner)\wedge$$
"v_i does not appear free in the formula with Gödel number y"$\wedge$
$$w=_i w'\to[Sat_n(y,w)\leftrightarrow Sat_n(y,w')].$$

This can also be proved by induction on n; again, the rest of (5) follows by Lemma 3.7.

The first equality axiom of (6) is proved immediately by Lemma 3.7. The second one has a proof similar to that of (4). ⊠

3.13. Lemma.

$I\Delta_0+\Omega_1$ proves by a proof of length of the order of n^2 that Sat_n preserves the basic non-logical axioms for formulas of length $\leqslant n$, e.g.

$$I\Delta_0+\Omega_1\vdash Fmla_n(\ulcorner 0\leqslant 0\wedge\neg S0\leqslant 0\urcorner)\wedge Evalseq(w,\ulcorner 0\leqslant 0\wedge\neg S0\leqslant 0\urcorner)$$
$$\to Sat_n(\ulcorner 0\leqslant 0\wedge\neg S0\leqslant 0\urcorner).$$

Similarly for the other 5 basic axioms relating the symbols $0, S, +, \cdot$ and $\leqslant$ of the language.

Proof.

Immediately by Lemma 3.7 and Lemma 3.3. ⊠

3.14. Lemma.

$I\Delta_0+\Omega_1$ proves by a proof of length of the order of n^2 that $Sat_{n,\Delta}$ agrees with Sat_n on Δ_0-formulas of length $\leqslant n$, i.e.

$$I\Delta_0+\Omega_1\vdash Fmla_{n,\Delta}(x)\wedge Evalseq(w,x)\to[Sat_{n,\Delta}(x,w)\leftrightarrow Sat_n(x,w)]$$

Proof.

By induction on n as in the proof of Lemma 3.9. Here, we take $\Phi_n \equiv \forall x \forall w(\mathrm{Fmla}_{n,\Delta}(x) \wedge \mathrm{Evalseq}(w,x) \rightarrow (\mathrm{Sat}_{n,\Delta}(x,w) \leftrightarrow \mathrm{Sat}_n(x,w)))$.
As in Lemma 3.3.2.a., we use the fact that if $x = y^{\ulcorner} \rightarrow {}^{\urcorner} z$ and $\mathrm{Fmla}_{n+1,\Delta}(x)$, then $\mathrm{Fmla}_{n,\Delta}(y)$ and $\mathrm{Fmla}_{n,\Delta}(z)$, etc. ⊠

3.15. Definition.

$s^*(i,x,w) = (\mathrm{Subseq}(w,1,i) * x) ** \mathrm{Subseq}(w,i+1,\mathrm{Len}(w)+1)$

Thus, if w is a sequence of length $\geqslant$ i, $s^*(i,x,w)$ denotes the sequence which is identical to w, except that x appears in the i-th place (cf. Definition 3.4.).

3.16. Lemma.

$I\Delta_0 + \Omega_1$ proves by a proof of length of the order of n^2 that Sat_n preserves the Δ_0-induction axioms of length $\leqslant n$, i.e.

$I\Delta_0 + \Omega_1 \vdash \mathrm{Fmla}_\Delta(y) \wedge$
$\mathrm{Fmla}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0)^{\ulcorner} \wedge \forall v_1({}^{\urcorner}y^{\ulcorner} \rightarrow {}^{\urcorner}\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1)^{\ulcorner}) \rightarrow \forall v_1{}^{\urcorner}y) \wedge$
$\mathrm{Evalseq}(w, \mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0)^{\ulcorner} \wedge \forall v_1({}^{\urcorner}y^{\ulcorner} \rightarrow {}^{\urcorner}\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1)^{\ulcorner}) \rightarrow \forall v_1{}^{\urcorner}y) \rightarrow$
$\mathrm{Sat}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0)^{\ulcorner} \wedge \forall v_1({}^{\urcorner}y^{\ulcorner} \rightarrow {}^{\urcorner}\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1)^{\ulcorner}) \rightarrow \forall v_1{}^{\urcorner}y, w)$.

Proof.

We work in $I\Delta_0 + \Omega_1$ and assume
$\mathrm{Fmla}_\Delta(y) \wedge$
$\mathrm{Fmla}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0)^{\ulcorner} \wedge \forall v_1({}^{\urcorner}y^{\ulcorner} \rightarrow {}^{\urcorner}\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1)^{\ulcorner}) \rightarrow \forall v_1{}^{\urcorner}y) \wedge$
$\mathrm{Evalseq}(w, \mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0)^{\ulcorner} \wedge \forall v_1({}^{\urcorner}y^{\ulcorner} \rightarrow {}^{\urcorner}\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1)^{\ulcorner}) \rightarrow \forall v_1{}^{\urcorner}y)$.

Because Sat_n is a partial satisfaction predicate for formulas of length $\leqslant n$, we can, using a proof of length of the order of n^2, prove that $\mathrm{Sat}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0)^{\ulcorner} \wedge \forall v_1({}^{\urcorner}y^{\ulcorner} \rightarrow {}^{\urcorner}\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1)^{\ulcorner}) \rightarrow \forall v_1{}^{\urcorner}y)$ is equivalent to the following formula:
$\mathrm{Sat}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0), w) \wedge$
$\forall w'(w' =_1 w \rightarrow (\mathrm{Sat}_n(y,w') \rightarrow \mathrm{Sat}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1), w'))) \rightarrow$
$\forall w'(w' =_1 w \rightarrow \mathrm{Sat}_n(y,w'))$.
This formula in turn is equivalent to:
$\mathrm{Sat}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, 0), w) \wedge$
$\forall x(\mathrm{Sat}_n(y, s^*(1,x,w)) \rightarrow \mathrm{Sat}_n(\mathrm{Sub}(y, {}^{\ulcorner}v_1{}^{\urcorner}, Sv_1), s^*(1,x,w))) \rightarrow$
$\forall x\, \mathrm{Sat}_n(y, s^*(1,x,w))$,

where s*(1,x,w) is as defined in Definition 3.15.
This last formula is then, by a proof of length of the order of n^2 of a call by name / call by value lemma analogous to the one proved in Lemma 3.12(4), equivalent to:

$Sat_n(y,s^*(1,0,w)) \wedge \forall x(Sat_n(y, s^*(1,x,w)) \rightarrow Sat_n(y,s^*(1,Sx,w))) \rightarrow$
$\forall x(Sat_n(y,s^*(1,x,w))$.

This looks almost like an instance of induction. However, because Sat_n is not Δ_0, we replace it by its Δ_0(Val)-equivalent $Sat_{n,\Delta}$, as is allowed by Lemma 3.14 and the assumption $Fmla_\Delta(y)$, and we obtain the equivalent formula

$Sat_{n,\Delta}(y,s^*(1,0,w)) \wedge$
$\forall x(Sat_{n,\Delta}(y, s^*(1,x,w)) \rightarrow Sat_{n,\Delta}(y,s^*(1,Sx,w)) \rightarrow$
$\forall x(Sat_{n,\Delta}(y,s^*(1,x,w))$.

As a true instance of Δ_0(Val)-induction, the formula above is at last provable from the assumptions. ⊠

Now that we have the partial truth predicates in hand, we can proceed with the proof proper of the main theorem of this chapter. We need only a few more definitions and lemmas.

3.17. Definition.
An <u>$I\Delta_0 + \Omega_1$-cut</u> is a formula J which defines a set of natural numbers such that

$I\Delta_0 + \Omega_1 \vdash J(0) \wedge \forall y \forall z(J(z) \wedge y \leqslant z \rightarrow J(y)) \wedge \forall y(J(y) \rightarrow J(Sy))$.

Sometimes we will write $x \in J$ for $J(x)$ and $K \subseteq J$ for

$I\Delta_0 + \Omega_1 \vdash \forall x(K(x) \rightarrow J(x))$

3.18. Lemma (Shortening lemma, Solovay).
Every $I\Delta_0+\Omega_1$-cut can be closed under addition and multiplication, i.e., if J is an $I\Delta_0+\Omega_1$-cut, then there is an $I\Delta_0+\Omega_1$-cut K such that

$I\Delta_0 + \Omega_1 \vdash \forall y(K(y) \rightarrow J(y)) \wedge \forall y \forall z(K(y) \wedge K(z) \rightarrow K(y+z) \wedge K(y \cdot z))$

Proof.
Define $P(y) \equiv \forall z(J(z) \rightarrow J(y+z))$, and subsequently
$K(y) \equiv \forall z(P(z) \rightarrow P(y \cdot z))$.
It is easy to verify that K is a cut closed under addition and multiplication. ⊠

3.19. Lemma (Paris-Wilkie, Pudlák)

If K is an <u>$I\Delta_0+\Omega_1$-initial segment</u>, i.e. if

$I\Delta_0+\Omega_1 \vdash K(0)\wedge\forall y\forall z(K(y)\wedge K(z)\rightarrow K(Sy)\wedge K(y+z)\wedge K(y\cdot z))$, then

$I\Delta_0+\Omega_1 \vdash \forall x\, Thm(\ulcorner K(\dot{x})\urcorner)$,

where $\dot{x}$ stands for the "efficient numeral" I_x defined on page 5 (we change notation to improve ease of reading).

Proof.

The complete proof can be found in Kalsbeek[89, Lemma 4.5].
Essentially, in the proof of $K(\dot{x})$, we follow the $|x|$ steps it takes to build $\dot{x}$ from $\dot{0}$. At every step, we instantiate either the proof of $\forall y(K(y)\rightarrow K(Sy))$ or the proof of $\forall y(K(y)\rightarrow K(SS0\cdot y))$ with the appropriate efficient numeral. By using Modus Ponens a total of $|x|$ times, we derive $K(\dot{x})$. The length of the proof can be bounded by a polynomial in $|x|$.
(Remark: in this case, the proof will be of length of the order $|x|^2$. In the formalized context in which we will use the result, the length of the formula K and the length of the proofs of $\forall y(K(y)\rightarrow K(Sy))$ and $\forall y(K(y)\rightarrow K(SS0\cdot y))$ also play a part in the computation of the length of the total proof, thereby making the length of the total proof of the order $|x|^3$.) ⊠

3.20. Definition.

$Prf_v(u,\ulcorner\chi\urcorner)\equiv$"u codes a proof of χ in $I\Delta_0+\Omega_1$ involving only formulas of length $\leqslant v$".

3.21. Lemma.

$I\Delta_0+\Omega_1\vdash\forall x\, Thm(\ulcorner\forall y\leqslant\dot{x}\,(Prf(y,\ulcorner\dot{\varphi}\urcorner)\leftrightarrow Prf_{|x|}(y,\ulcorner\dot{\varphi}\urcorner))\urcorner)$

Proof.

A formalization of the following observation: if a formula v occurs in a proof y where $y\leqslant x$, then $Len(v)\leqslant|v| \leqslant|x|$. ⊠

3.22. Theorem.

For all sentences φ:

$I\Delta_0+\Omega_1\vdash\forall x\, Thm(\ulcorner\forall y\leqslant\dot{x}\,(Prf(y,\ulcorner\dot{\varphi}\urcorner)\rightarrow\varphi)\urcorner)$

Proof.

By Lemma 3.21, it suffices to prove

$I\Delta_0+\Omega_1 \vdash \forall x\ Thm(\ulcorner \forall y \leqslant \dot{x}\ (Prf_{|x|}(y,\ulcorner \dot{\varphi} \urcorner) \rightarrow \varphi)\urcorner)$

We reason inside $I\Delta_0+\Omega_1$, and we take an x.

The idea behind the proof is to find a Gödel number K_x standing for a formalized "Thm-initial segment" such that we have

$Thm(K_x(\dot{x})\ulcorner \rightarrow \forall y \leqslant \dot{x}\ (Prf(y,\ulcorner \dot{\varphi} \urcorner) \rightarrow \varphi)\urcorner)$

(by abuse of notation we write $K_x(\dot{x})$ for the Gödel number that results by the appropriate application of the substitution function to K_x).

In the construction of the Thm-initial segment K_x, we will need the formalized versions of the lemmas which we proved above about the existence and the properties of partial satisfaction predicates for formulas of length smaller than some standard numeral n. In our formalized context, $|x|$ plays the rôle of "standard numeral", as will become clear when we define K_x. Again by abuse of notation, we let $Sat_{|x|}(v,w)$ stand for a Gödel number instead of a formula; we will use the appropriate formalizations of lemmas we proved about the formulas $Sat_n(v,w)$ to derive formalized facts about the Gödel number $Sat_{|x|}(v,w)$.

Keeping these cautionary remarks in mind, we start the proof by defining the Gödel number J_x of a formalized "Thm-cut" (later to be shortened to the Thm-initial segment K_x that we need) as follows:

$J_x(s) \equiv \ulcorner \forall y,v \leqslant s(Prf_{|x|}(y,v) \rightarrow \forall w(Evalseq(w,v) \rightarrow \urcorner Sat_{|x|}(v,w)\ulcorner))\urcorner.$

By the formalized version of Lemma 3.6, we may assume that this Gödel number exists, because the length of $Sat_{|x|}(v,w)$ is linear in $|x|$. (Notice that we are reasoning inside $I\Delta_0+\Omega_1$ all the time!)

It is not difficult to prove directly from the definition of J_x (and from the fact that J_x is small enough) that:

$Thm(J_x(\dot{0})\ulcorner \wedge \forall y \forall z(\urcorner J_x(z)\ulcorner \wedge y \leqslant z \rightarrow \urcorner J_x(y)\ulcorner)\urcorner).$

To prove that J_x is closed under successor, we remark that

$Thm(Prf_{|x|}(y,v) \rightarrow Len(v) \leqslant |x|).$

Therefore, we can formalize Lemmas 3.11,12,13 and 3.16 to conclude by a proof of length of the order $|x|^2$ that $Sat_{|x|}(v,w)$

preserves all logical and non-logical axioms and rules for formulas of length $\leqslant |x|$, and thus indeed, $Thm(\ulcorner\forall y(\urcorner J_x(y)\ulcorner \to \urcorner J_x(Sy))$, proving J_x to be a Thm-cut.

By a formalization of the proof of Lemma 3.18, we can shorten the Thm-cut J_x to a Thm-initial segment K_x of length linear in $|x|$ such that, by a proof of length of the order $|x|^2$,

$$Thm(\ulcorner\forall y(\urcorner K_x(y)\ulcorner \to \urcorner J_x(y)\ulcorner)\wedge \urcorner J_x(\dot{0})\ulcorner \wedge$$
$$\forall y\forall z(\urcorner J_x(z)\ulcorner \wedge y\leqslant z\to \urcorner J_x(y)\ulcorner)\wedge$$
$$\forall y\forall z(\urcorner J_x(y)\ulcorner \wedge \urcorner J_x(z)\ulcorner \to \urcorner J_x(Sy)\ulcorner \wedge \urcorner J_x(j+z)\ulcorner \wedge \urcorner J_x(y\cdot z)\ulcorner)\urcorner).$$

Carefully formalizing the proof of Lemma 3.19, we find, by proofs of length of the order $|x|^3$,

$$Thm(K_x(\dot{x}))\wedge Thm(K_x(\ulcorner\dot{\varphi}\urcorner)).$$

And thus, because we have $Thm(\ulcorner\forall y(\urcorner K_x(y)\ulcorner \to \urcorner J_x(y)\ulcorner)\urcorner)$, we conclude that, by definition of J_x,

$$Thm(\ulcorner\forall y\leqslant \dot{x}\ (Prf_{|x|}(y,\ulcorner\dot{\varphi}\urcorner)\to$$
$$\forall w(Evalseq(w,\ulcorner\dot{\varphi}\urcorner)\to \urcorner Sat_{|x|}(\ulcorner\dot{\varphi}\urcorner,w)\ulcorner))\urcorner).$$

Because we have $Thm(\ulcorner\forall y\leqslant \dot{x}\ (Prf_{|x|}(y,\ulcorner\dot{\varphi}\urcorner)\to Fmla_{|x|}(\ulcorner\dot{\varphi}\urcorner)$, we can apply the formalized version of lemma 3.10, taking note that φ is a sentence. Therefore,

$$Thm(\ulcorner\forall y\leqslant \dot{x}\ (Prf_{|x|}(y,\ulcorner\dot{\varphi}\urcorner)\to\forall w(Evalseq(w,\ulcorner\dot{\varphi}\urcorner)\to\varphi))\urcorner).$$

This in turn is equivalent to the desired

$$Thm(\ulcorner\forall y\leqslant \dot{x}\ (Prf_{|x|}(y,\ulcorner\dot{\varphi}\urcorner)\to\varphi)\urcorner).$$

Stepping out of $I\Delta_0+\Omega_1$ again, we conclude that indeed

$$I\Delta_0+\Omega_1\vdash\forall x\, Thm(\ulcorner\forall y\leqslant \dot{x}\ (Prf_{|x|}(y,\ulcorner\dot{\varphi}\urcorner)\to\varphi)\urcorner).$$ ⊠

Remark. Looking carefully at the proof of Theorem 3.22, we notice that it is also possible to derive the following result, which is a little bit stronger:

$$I\Delta_0+\Omega_1\vdash\forall v(Sentence(v)\to\forall x\, Thm(\ulcorner\forall y\leqslant \dot{x}\ (Prf_{|x|}(y,\dot{v})\to \urcorner v\ulcorner)\urcorner)).$$

Theorem 3.22 and its proof can also be adapted for the case that φ is a formula instead of a sentence (or in the stronger result mentioned above: Fmla(v) instead of Sentence(v))

3.23. Corollary (Švejdar's principle is provable in $I\Delta_0+\Omega_1$).
For all sentences φ,ψ
$I\Delta_0+\Omega_1 \vdash \Box\varphi \rightarrow \Box(\Box\psi \preccurlyeq \Box\varphi \rightarrow \psi)$, i.e.
$I\Delta_0+\Omega_1 \vdash \forall x(Prf(x,\ulcorner\varphi\urcorner)\rightarrow$
$$Thm(\ulcorner\exists y(Prf(y,\ulcorner\dot{\psi}\urcorner)\wedge\forall z\leqslant y\ \neg Prf(z,\ulcorner\dot{\varphi}\urcorner))\rightarrow\psi\urcorner))$$

Proof.
We work inside $I\Delta_0+\Omega_1$ and suppose $Prf(x,\ulcorner\varphi\urcorner)$. This implies $Thm(\ulcorner Prf(\dot{x},\ulcorner\dot{\varphi}\urcorner)\urcorner)$ (by provable Σ^b_1-completeness). Hence, we have $Thm(\ulcorner\exists y(Prf(y,\ulcorner\dot{\psi}\urcorner)\wedge\forall z\leqslant y\ \neg Prf(z,\ulcorner\dot{\varphi}\urcorner))\rightarrow\exists y\leqslant\dot{x}Prf(y,\ulcorner\dot{\psi}\urcorner)\urcorner)$.
Theorem 3.22 gives $Thm(\ulcorner\exists y\leqslant\dot{x}Prf(y,\ulcorner\dot{\psi}\urcorner)\rightarrow\psi\urcorner)$; therefore, we have
$Thm(\ulcorner\exists y(Prf(y,\ulcorner\dot{\psi}\urcorner)\wedge\forall z\leqslant y\ \neg Prf(z,\ulcorner\dot{\varphi}\urcorner))\rightarrow\psi\urcorner))$.
Jumping outside $I\Delta_0+\Omega_1$ again, we conclude that
$I\Delta_0+\Omega_1 \vdash \forall x(Prf(x,\ulcorner\varphi\urcorner)\rightarrow$
$$Thm(\ulcorner\exists y(Prf(y,\ulcorner\dot{\psi}\urcorner)\wedge\forall z\leqslant y\ \neg Prf(z,\ulcorner\dot{\varphi}\urcorner))\rightarrow\psi\urcorner))\ \boxtimes$$

The proof of the soundness of Švejdar's system Z^- (and of Z^-_F for appropriate frames F) with respect to $I\Delta_0+\Omega_1$ has now been completed (see Theorem 2.5).
Švejdar introduced his system Z^- in order to study generalized Rosser sentences, and he derived the formalized version of Rosser's theorem in it. As a welcome byproduct of the soundness of Z^- with respect to $I\Delta_0+\Omega_1$, Rosser's theorem thus holds for $I\Delta_0+\Omega_1$. Because Švejdar's proof is not very long, we will give (a variant of) it here.

3.24. Theorem (formalized Rosser, Švejdar[83]
$I\Delta_0+\Omega_1\vdash\boxdot(R\leftrightarrow\Box\neg R\preccurlyeq\Box R)\rightarrow(\Box R\rightarrow\Box\bot)\wedge(\Box\neg R\rightarrow\Box\bot)$.

Proof.
We reason inside $I\Delta_0+\Omega_1$, and assume that $\boxdot(R\leftrightarrow\Box\neg R\preccurlyeq\Box R)$. Then $\Box R\rightarrow\Box(\Box\neg R\preccurlyeq\Box R)$. Corollary 3.23 gives
$\Box R\rightarrow\Box(\Box\neg R\preccurlyeq\Box R\rightarrow\neg R)$. Combined, these two yield
$\Box R\rightarrow\Box\neg R$, i.e. $\Box R\rightarrow\Box\bot$.

Working under the same assumption $\boxdot(R \leftrightarrow \Box\neg R \preccurlyeq \Box R)$, we have $\Box\neg R \rightarrow \Box\Box\neg R$; and thus by (01) (see Ch. 2, above def. 2.3) and soundness of Švejdar's system Z^- with respect to $I\Delta_0+\Omega_1$, $\Box\neg R \rightarrow \Box(\Box\neg R \preccurlyeq \Box R \vee \Box R \preccurlyeq \Box\neg R)$. By the initial assumption, $\Box\neg R \rightarrow \Box\neg(\Box\neg R \preccurlyeq \Box R)$, and therefore we have $\Box\neg R \rightarrow \Box(\Box R \preccurlyeq \Box\neg R)$. Corollary 3.23 gives $\Box\neg R \rightarrow \Box(\Box R \preccurlyeq \Box\neg R \rightarrow R)$, and thus, as above, $\Box\neg R \rightarrow \Box R$ i.e. $\Box\neg R \rightarrow \Box\bot$. ⊠

References

Buss, S., 1986, Bounded Arithmetic, Bibliopolis, Napoli.

Feferman, S., 1960, Arithmetization of metamathematics in a general setting, Fund. Math. 49, 33-92.

Ferrante, J. and C.W. Rackoff, 1979, The Computational Complexity of Logical Theories, Springer-Verlag, Berlin.

Guaspari, D. and R.M. Solovay, 1979, Rosser sentences, Annals of Math. Logic 16, 81-99.

Jongh, D.H.J. de, 1987, A simplification of a completeness proof of Guaspari and Solovay, Studia Logica 46, 187-192.

Jongh, D.H.J. de, M. Jumelet and F. Montagna, 1989, On the proof of Solovay's theorem, ITLI Prepublication Series for Mathematical Logic and Foundations ML-89-04, University of Amsterdam, Amsterdam. To appear in Studia Logica.

Jongh, D.H.J. and F. Montagna, 1989, Rosser orderings and free variables, ITLI Prepublication Series for Mathematical Logic and Foundations ML-89-05, University of Amsterdam, Amsterdam. To appear in Studia Logica.

Jongh, D.H.J. de and F. Veltman, 1988, Intensional Logic, lecture notes, Philosophy Department, University of Amsterdam, Amsterdam.

Kalsbeek, M., 1989, An Orey Sentence for Predicative Arithmetic, ITLI Prepublication Series X-89-01 < University of Amsterdam, Amsterdam.

Krajíček, J., P. Pudlák and G. Takeuti, in preparation, Bounded arithmetic and the polynomial hierarchy.

Manders, K. and L. Adleman, 1978, NP-complete decision problems for binary quadratics, J. of Computer System Sciences 15, 168-184.

Nelson, E., 1986, Predicative Arithmetic, Math. Notes 32, Princeton University Press, Princeton.

Paris, J. and A. Wilkie, 1987, On the scheme of induction for bounded arithmetic formulas, Annals of Pure and Applied Logic 35, 261-302.

Pudlák, P., 1983, A definition of exponentiation by a bounded arithmetical formula, Commentationes Mathematicae Universitatis Carolinae 24, 667-671.

Pudlák, P., 1985, Cuts, consistency statements and interpretability, J. of Symbolic Logic 50, 423-441.

Pudlák, P., 1986, On the length of proofs of finitistic consistency statements in first order theories, in: Paris, J.B. et al. eds., Logic Colloquium '84, North Holland, Amsterdam.

Pudlák, P., 1987, Improved bounds on the length of finitistic consistency statements, in: Simpson, S.G., ed., Logic and Combinatorics, Contemporary Mathematics 35, AMS, Providence.

Smoryński, C., 1985, Self-reference and Modal Logic, Springer-Verlag, New York.

Švejdar, V., 1983, Modal analysis of generalized Rosser sentences, J. of Symbolic Logic 48, 986-999.

Solovay, R.M., 1976, Provability interpretations of modal logic, Israel J. of Mathematics 25, 287-304.

Takeuti, G., 1975, Proof Theory, North Holland, Amsterdam.

Verbrugge, L.C., 1988, Does Solovay's Completeness Theorem Extend to Bounded Arithmetic?, Master's thesis, University of Amsterdam, Amsterdam.

Visser, A., 1988, Interpretability Logic, Logic Group Preprint Series nr. 40, University of Utrecht, Utrecht.

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, Forward looking Operators
86-06 Johan van Benthem	Logical Syntax

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

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

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 Solutions
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

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