AN INSIDE VIEW OF EXP
or
The closed fragment of the provability logic of $I\Delta_0+\Omega_1$ with a propositional constant for EXP

Albert Visser
Department of Pilosophy, University of Utrecht

Logic Group
Preprint Series
No. 57
September 1990

Department of Philosophy
University of Utrecht
Heidelberglaan 2
3584 CS Utrecht
The Netherlands

AN INSIDE VIEW OF EXP
or
The closed fragment of the provability logic of $I\Delta_0+\Omega_1$ with a propositional constant for EXP

Albert Visser

University of Utrecht, Department of Pilosophy,
Heidelberglaan 2, 3584CS Utrecht
The Netherlands

Abstract:
We characterize the closed fragment of the provability logic of $I\Delta_0$+EXP with a propositional constant for EXP. In three appendices the details of various results in Arithmetic needed for our characterization are provided.

MSC-1980 classification 03B 15/03F30
Key words and phrases: Provability Logic, Interpretability, Fragments of Arithmetic

AN INSIDE VIEW OF EXP
or
The closed fragment of the provability logic of $I\Delta_0+\Omega_1$ with a propositional constant for EXP

Albert Visser

ABSTRACT: in this paper I give a characterization of the closed fragment of the provability logic of $I\Delta_0$+EXP with a propositional constant for EXP.

1 Introduction

Paris & Wilkie, in their paper *On the scheme of induction for bounded arithmetic formulas* (Paris & Wilkie[87]), paint a gripping picture of the interrelations between $I\Delta_0+\Omega_1$ and $I\Delta_0$+EXP. Two of their most memorable results are their Corollary 8.14: $I\Delta_0+\text{EXP}\nvdash\text{Con}(I\Delta_0+\Omega_1)$, and their Theorem 8.19: $I\Delta_0+\text{EXP}+\text{Con}(I\Delta_0+\Omega_1)\nvdash\text{Con}(I\Delta_0+\text{EXP})$. In this paper I give a generalization of theorems in this style. Consider the closed modal language generated by $\bot,\top$, the propositional connectives and $\Box$, with an additional logical constant EXP. We interpret the propositional constants as themselves, $\Box$ as provability in $I\Delta_0+\Omega_1$ and EXP as the arithmetical axiom EXP. In this language Paris and Wilkie's results can be reformulated as $I\Delta_0+\Omega_1\nvdash(\text{EXP}\to\Diamond\top)$ [as usual $\Diamond$ abbreviates $\neg\Box\neg$] and $I\Delta_0+\Omega_1\nvdash((\text{EXP}\wedge\Diamond\top)\to\Diamond\text{EXP})$. In this paper I characterize all principles of the closed modal language under the given interpretation that are provable in $I\Delta_0+\Omega_1$. One special case of our result of a distinctly different flavour than the theorems of Paris and Wilkie discussed above is: $I\Delta_0+\Omega_1\vdash(\Diamond\Diamond\top\to\Diamond\text{EXP})$.

Our result can be described as a solution of a variant for a special case of Friedman's 35th problem. Friedman original problem is to give a characterization of the formulas of the closed fragment of the language of modal propositional logic which are provable under the standard provability interpreta- tion in reasonable arithmetical theories like PA. Friedman's problem was solved independently by van Benthem, Boolos (see Boolos[76]) and Magari (see Magari[75]). Their result works (modulo a slight refinement in case a theory proves its own n-iterated inconsistency for some n) for all $\Delta_1{}^b$- axiomatized theories containing a sufficiently large fragment of $I\Delta_0+\Omega_1$ or even better Buss's $S_2{}^1$. The reason that the result goes through so easily in weak theories is that it doesn't require Rosser style arguments: to formalize Rosser style arguments one seems to need EXP. In contrast Solovay's proof of his arithmetical completeness theorem for Provability Logic doesn't work in $I\Delta_0+\Omega_1$. (For an elaboration of this theme see Verbrugge[88,89].) A solution of Friedmans problem for the case of Heyting's Arithmetic was given in Visser[85].

Hájek and Svejdar in Hajék & Svejdar[198?] prove a characterization of the closed fragment of (all extensions of) a modal system ILF. ILF is a system of interpretability logic: the logic one gets by adding an operator $\rhd$ for relative interpretability to the language. For a given arithmetical theory T, $A \rhd B$ means: T+B is relatively interpretable in T+A. An immediate consequence of Hájek and Svejdar's result is, that their characterizion describes the closed fragment of all logics for interpretability and provability valid in $\Delta_1{}^b$-axiomatized extensions of $I\Delta_0+\Omega_1$ (again modulo a slight refinement in case T proves its own n-iterated inconsistency). In section 6 of this paper I prove a similar generalization of our main result.

The contents of the paper are as follows: in section 3 the necessary conventions and elementary facts are introduced. Section 4 contains our main technical lemma. The lemma is a variant of the main lemma of Visser[90]. It is the result of formalizing a model theoretical argument due to Paris and Wilkie. In Section 5 our main result is proved and section 6 gives the generalization to the language also involving interpretability. Section 7 is an extended appendix containing sketches of the calculations needed to provide the estimates that are essential for the proof of one of the most important lemmas.

I thank the anonymous referee for spotting a gap in my earlier presentation.

2 Prerequisites

We presuppose some knowledge of either Boolos[79] or Smoryński[85], and of either Buss[85] or Paris & Wilkie[87]. At a few places results from Pudlák[85],[86] and from Visser[90,89] are used.

The reader who is not familiar with Buss[85] or Paris & Wilkie[87] and who is interested in the modal material could try to understand the statement of lemma 4.1 and then proceed immediately to section 5.

3 Facts, notions and conventions

In $I\Delta_0+\Omega_1$ we can define all the apparatus of coding needed for the purpose of arithmetization. See Buss[85] or Paris & Wilkie[87]. The aim of this subsection is give a few definitions and to state a few elementary points.

J.H. Bennett shows that there is a Δ_0-formula exp(x)=y, such that $I\Delta_0$ verifies $((\exp(x)=y \wedge \exp(x)=z) \rightarrow y=z)$, $\exp(\underline{0})=\underline{1}$ and $\exp(Sx)=2.\exp(x)$. It is easy to see that $I\Delta_0$ verifies such familiar facts as:

$$((x<y \wedge \exp(y)=z) \rightarrow \exists u\ \exp(x)=u),$$

$$((\exp(x)=u \wedge \exp(y)=v) \rightarrow \exp(x+y)=u.v\ .$$

(Similar remarks hold for x^y.)

We define $|x|:=\text{entier}({}^2\log(x+1))$, $x\#y:=2^{|x|.|y|}$, $\omega_1(x):=x\#x$. Ω_1 is the axiom "ω_1 is total". As is easily seen $I\Delta_0$ does not prove Ω_1. $I\Delta_0+\Omega_1$ is just right for treating syntax: e.g. Ω_1 guarantees that substitution of a term in a formula is possible.

We will code strings of symbols in an alphabet adequate for the language of arithmetic, with some extras like several kinds of brackets. The function n(x) giving the number of symbols of the string coded by x is Δ_0-definable in $I\Delta_0+\Omega_1$. We have: $n(x)\leq|x|$ and $|x|\leq k.n(x)$ for some standard number k.

To every number x we can assign an efficient numeral num(x): assign to 0 and 1 (the codes of) $\underline{0}$ and $S\underline{0}$; if we have assigned to $x\neq 0$ numeral t, assign to 2.x: $SS\underline{0}.t$, and to 2x+1: $(SS\underline{0}.t+S\underline{0})$. Num(x) is Δ_0-definable in $I\Delta_0+\Omega_1$. We have $n(\text{num}(x))\leq k.|x|$, for some standard k.

A crucial fact about adding functions to $I\Delta_0$ is the following:

Theorem: (Gaifman & Dimitracopoulos[82]): If f has Δ_0-graph than $I\Delta_0$+"f is total and weakly monotonically increasing"$\vdash I\Delta_0(f)$.

Here $\Delta_0(f)$ is the class of (translations of) formulas with only bounded quantifiers, where f is allowed to occur in the bounding terms.

It follows that $I\Delta_0+\Omega_1\vdash I\Delta_0(\omega_1)$, so in $I\Delta_0+\Omega_1$ we can work as if ω_1 were a function symbol in the language.

A sequence of syntactical objects (like formulas or terms) is coded as the string describing the sequence as a syntactical object: e.g. <0=0,⊥> is coded as $\ulcorner<\urcorner*\ulcorner 0=0\urcorner*\ulcorner,\urcorner*\ulcorner\bot\urcorner*\ulcorner>\urcorner$. A sequence of numbers is coded as the sequence of the numerals of those numbers, e.g. <0,2,3> is coded by: $\ulcorner<\urcorner*\text{num}(0)*\ulcorner,\urcorner*\text{num}(2)*\ulcorner,\urcorner*\text{num}(3)*\ulcorner>\urcorner$. Length(x), the length of x, considered as a sequence is Δ_0-definable in $I\Delta_0+\Omega_1$. Note that if x is a sequence of numbers and z is the maximum number occuring in x, then $n(x)\leq\text{length}(x).(n(\text{num}(z))+2)\leq k.\text{length}(x).(|z|+1)$ for some standard number k.

3.2 Theories and Provability

Our basic theory in this paper is $I\Delta_0+\Omega_1$. It is (modulo some translation work) the same as Buss's theory S_2 (see Buss[85]). The language of $I\Delta_0+\Omega_1$ has constant 0 and function symbols S,+,. . Sometimes, especially in subscripts, we will call $I\Delta_0+\Omega_1$ simply Ω. We will also be looking at $I\Delta_0$+EXP, which we will call sometimes -if no confusion is possible- simply EXP.

We will assume that the axiom-set of a theory T is given by a Δ_1^b-predicate (see Buss[1985]). We take this predicate to be part of the identity conditions of the theory. $Proof_T$ is the Δ_1^b proof predicate based on the predicate defining T's axiom set.

We write par abus de langage '$Proof_T(u, \phi(\underline{x}_1,...,\underline{x}_n))$' for: $Proof_T(u, \ulcorner\phi(\dot{x}_1,...,\dot{x}_n)\urcorner)$, here:

i) all free variables of ϕ are among those shown.

ii) $\ulcorner\phi(\dot{x}_1,...,\dot{x}_n)\urcorner$ is the "Gödelterm" for $\phi(x_1,...,x_n)$ as defined in Smoryński[85], p43. Here we use instead of the usual numerals the efficient numerals of section 3.1, so that: $I\Delta_0+\Omega_1\vdash\forall x_1,...,x_n\exists y\ \ulcorner\phi(\dot{x}_1,...,\dot{x}_n)\urcorner=y$.

$\Box_T\phi(\underline{x}_1,...,\underline{x}_n)$ will stand for: $Prov_T(\ulcorner\phi(\dot{x}_1,...,\dot{x}_n)\urcorner)$.

Occurrences of terms inside $\Box_T$ should be treated with some care. Is $\Box_T(\phi[t/x])$ intended $(\Box_T\phi(x))[t/x]$? We will always use the first, i.e. the small scope reading. In cases where: proves that t is total and $U\vdash t=x\rightarrow\Box_V t=\underline{x}$, the scope distinction may be ignored within U w.r.t. $\Box_V$. We have: $U\vdash (\Box_V\phi(x))[t/x]\leftrightarrow\Box_V(\phi[t/x])$.

We will use the same convention for occurrences of variables inside the interpretability predicate. For some uses in section 4 our conventions are not sufficient. Rather than introducing a heavier notational apparatus I prefer to explain what is going on there in words.

Some alternative notions of provability will be used in this paper: first we write $Tabproof_U(x,A)$ for "x is a tableaux proof of inconsistency from a finite subset of the axioms of U and $\neg A$". Here tableaux proofs are defined as in Paris & Wilkie[87]. Define $\Delta_U A :\Leftrightarrow \exists x\ Tabproof_U(x,A)$.

Let $\nu(A)$ be defined as follows: $\nu(A):=0$ if A is atomic, $\nu(A\wedge B):=\nu(A\vee B):=\nu(A\rightarrow B):=\max(\nu(A),\nu(B))+1$, $\nu(A\leftrightarrow B):=\max(\nu(A),\nu(B))+2$, $\nu(\forall xA):=\nu(\exists xA):=\nu(A)+1$, $\nu(\neg A):=\nu(A)$. (Note that our ν modulo the conventional translations of the connectives coincides with Schwichtenberg's $|.|$ (see Schwichtenberg[77], p871).) Let p be a proof. Define $\nu(p):=\max\{\nu(B)|B \text{ occurs in } p\}$. Put:

$$Proof_{U,x}(p,A) :\Leftrightarrow Proof_U(p,A)\wedge\nu(p)\leq x,$$
$$\Box_{U,x}A :\Leftrightarrow \exists p\ Proof_{U,x}(p,A).$$

Our notion of restricted provability is a little bit more flexible than that of Paris & Wilkie[87], but serves the same purposes.

3.3 Cuts

We follow the discussion of cuts of Paris & Wilkie[87]. For reasons of convenience we use a slightly idiosyncratic notion of cut: a cut I is given by an arithmetical predicate, is downwards closed w.r.t. the standard ordering of the natural numbers, is closed under successor, addition, multiplication and ω_1. The attentive reader of Paris & Wilkie[87] will easily see that our restricted notion is not really restrictive, because any cut in the usual sense can be shortened to a cut in our sense. We will say that I is a T-cut if T proves the arithmetization of "I is a cut".

We write A^I for the result of relativizing the quantifiers of A to I. We will see in section 3.5 that relativization to a cut can be considered as a special case of interpretation. Put: $\Box_T{}^I A := (\Box_T A)^I$.

3.4 Some crucial facts

We state some of the vitally important arithmetical facts needed in this paper.

3.4.1 Fact: Let A range over (codes of) sentences of the language of arithmetic, we have:

$$I\Delta_0+\Omega_1 \vdash \forall I \in \Omega\text{-cuts}\ \forall A\ (\Box_\Omega A \to \Box_\Omega A^I).$$

Reference: See the proof of Corollary 7.5 in Paris & Wilkie[87]. □

3.4.2 The Big Outside, Small Inside Lemma: $I\Delta_0+\Omega_1 \vdash \forall I \in U\text{-cuts}\ \exists u\ \forall x\ \Box_{U,u}\underline{x} \in I$.

Elaboration: The idea is sketched in the proof of Lemma 8.1 of Paris & Wilkie[87]. Suppose p is the U-proof that I is a cut. We find that we can take u:=v(p). Let x be given. The U-proof q of $\underline{x} \in I$ can be estimated by $|q| \leq |x|.(a|p|+b|x|)$, where a and b are fixed small standard numbers. □

Define $\exp(x) := 2^x$, $\mathrm{itexp}(x,0) := x$, $\mathrm{itexp}(x,y+1) := \exp(\mathrm{itexp}(x,y))$. The graph of itexp can be Δ_0-defined in $I\Delta_0+\Omega_1$ in such a way that the recursive clauses for itexp can be verified.

3.4.3 Facts (Pudlák):

i) $I\Delta_0+\Omega_1 \vdash \forall y\ ((\mathrm{itexp}(y,\underline{2})\text{ exists}) \to \exists I \in \Omega\text{-cuts}\ \Box_\Omega \forall x \in I\ (\mathrm{itexp}(x,\underline{y})\text{ exists})),$

ii) If the language of Ω contains the connective $\leftrightarrow$, then:

$I\Delta_0+\Omega_1 \vdash \forall y\ ((\exp(y)\text{ exists}) \to \exists I \in \Omega\text{-cuts}\ \Box_\Omega \forall x \in I\ (\mathrm{itexp}(x,\underline{y})\text{ exists})),$

Proof-sketch & Remarks:

Part of the idea of the proof can be found in the proof of Lemma 8.1 of Paris & Wilkie[87]. We need however careful estimates on cuts as given in the proof of Lemma 2.2 of Pudlák[86].

A brief sketch: first extend the language of $I\Delta_0+\Omega_1$ with a predicate variable X. Let $\Phi(X)$ be the formula: $\forall y(\exp(y) \in X \to \exp(x\#y) \in X)$. It is easy to find an $I\Delta_0+\Omega_1$-proofs $\pi(X)$ of (X cut $\to$ $\Phi(X)$ cut) and $\pi'(y,X)$ of $\mathrm{itexp}(x,y+\underline{1}) \in X$ from the assumption $\mathrm{itexp}(x,y) \in \Phi(X)$. Let $I_0 := \{x|x=x\}$, $I_{n+1} := \Phi(I_n)$. Note that $|I_{n+1}| = \underline{2}.|I_n| + \underline{k}$, for some standard k. So $|I_y| \leq \underline{m}.\exp(y)+\underline{n}$, for standard m and n. So the code of I_y is $\leq \underline{p}.(\mathrm{itexp}(y,\underline{2})\#\underline{q})$ for some standard p,q. Let π_0 be the proof of $\{x|x=x\}$ cut. Then the proof π_y of (I_y cut) looks like this:

$\pi_0, \pi(I_0),\ldots,\pi(I_{y-1})$.

Note $|\pi_y| \le y.|\pi(I_y)|+\underline{r} \le y.(\underline{s}.|I_y|+\underline{t})+\underline{a} \le \underline{b}.y.\exp(y)+\underline{c}$ for some standard r,s,t,a,b,c. So the code of π_y will be $\le$ itexp(y,$\underline{2}$)#exp(y)#$\underline{d}$ for some standard d.

Consider the following proof π'_y:

$x\in I_y,\ldots,\text{itexp}(x,\underline{0})\in I_y,\pi'(I_{y-1}),\ldots,\pi(I_0),\text{itexp}(x,\underline{y})$ exists.

Clearly the code of π'_y can be estimated in a similar way as the code of π_y.

These estimates suffice for the proof of (i). To get the sharpening (ii) it is sufficient to reduce the double occurrence of X in $\Phi(X)$ to a single one. This can be done using a trick due to Ferrante & Rackoff. In our case this trick works out like this: let $F(x,y,z):=\exp(x\#y)$ if $z=0$, $F(x,y,z):=\exp(y)$ if $z\neq 0$. Take $\Psi(X):=\forall y\exists z(F(x,y,z)\in X\leftrightarrow z=0)$. It is easy to see that $I\Delta_0+\Omega_1$ shows $\Phi(X)\leftrightarrow\Psi(X)$. The rest of the proof is similar to the one above, but with better estimates.

Note: it is essential for estimates in (ii) that our language contains $\leftrightarrow$. I don't know of any way to get rid of this restriction for a standard language. One strategy to get the efficient definitions would be to enrich the language with λ-abstraction and represent formulas by acyclic graphs, which are not necessarily trees. (In this way we get a syntax which allows sharing. See Barendregt &alii[86] for a treatment of syntax using graphs in a somewhat different context.)

Since it is somewhat unpleasant to work in a language with $\leftrightarrow$ we will use (i). □

3.4.4 Fact:

i) $I\Delta_0+\Omega_1 \vdash \forall x,y$ ((itexp(y,$\underline{2}$) exists) $\rightarrow \Box_\Omega$ (itexp($\underline{x}$,$\underline{y}$) exists))

ii) If the language of $I\Delta_0+\Omega_1$ contains the connective $\leftrightarrow$:
$I\Delta_0+\Omega_1 \vdash \forall x,y$ ((exp(y) exists) $\rightarrow \Box_\Omega$ (itexp($\underline{x}$,$\underline{y}$) exists))

Proof: By 3.4.2, 3.4.3. □

Our next fact is a direct adaptation of Pudlák's strengthening of Gödels Second Incompleteness Theorem in Pudlák[85]. Let's say that a T-cut I is T-reasonable if according to T we have enough instances of Δ_0-induction in I to verify the various metamathematical principles formalized by Paris and Wilkie in $I\Delta_0+\Omega_1$. Clearly every T-cut can be shortened to a T-reasonable T-cut. Moreover if T proves 'enough' instances of $I\Delta_0$ then automatically every T-cut is T-reasonable (by downwards preservation of Π_1-sentences).

3.4.5 The Strengthened Löb's Principle (SLP): Let T extend Q. We have:

$I\Delta_0+\Omega_1 \vdash$ for all T-reasonable T-cuts I $\Box_T(\Box_T{}^I A\rightarrow A) \rightarrow \Box_T A$

Proof: Reason in $I\Delta_0+\Omega_1$: Let I be a T-reasonable T-cut and suppose $\Box_T(\Box_T{}^I A\rightarrow A)$. By the

Diagonalization Lemma we can find a sentence λ such that $\Box_T(\lambda \leftrightarrow (\Box_T{}^I\lambda \to A))$. We also have $\Box_T\Box_T{}^I(\lambda \leftrightarrow (\Box_T{}^I\lambda \to A))$ and hence: $\Box_T(\Box_T{}^I\lambda \to \Box_T{}^I(\Box_T{}^I\lambda \to A))$ (because in I we have 'enough' axioms of $I\Delta_0+\Omega_1$). Moreover: $\Box_T(\Box_T{}^I\lambda \to \Box_T{}^I\Box_T{}^I\lambda)$. Ergo $\Box_T(\Box_T{}^I\lambda \to \Box_T{}^I A)$ and hence $\Box_T(\Box_T{}^I\lambda \to A)$. We may conclude: $\Box_T\lambda$. It follows that for some x $\Box_T\mathrm{Proof}_T(x,\lambda)$. By 3.4.2: $\Box_T x \in I$, hence $\Box_T\Box_T{}^I\lambda$ and so: $\Box_T A$. □

3.4.5 Cut Elimination Theorem: Let $\rho(p)$ be the cut-rank of proof p, as defined in Schwichtenberg[77]. For some standard k, we have:

$$I\Delta_0+EXP \vdash \forall x,p,A\ (\mathrm{Proof}_U(p,A) \wedge \mathrm{itexp}(p,2.\rho(p)+k)=x) \to \exists p^* \leq x\ \mathrm{Tabproof}_U(p^*,A).$$

Discussion: In Paris & Wilkie[87] a theorem like this is claimed twice. First on page 293 in effect our 3.4.5 is given with the restriction that $\rho(p)$ is standard. Secondly there is lemma 8.18. This, however, uses an estimate that is to large for our purposes: we need that the iteration is of order $2.\rho(p)+k$ rather than of order p. In appendix 7.1 we sketch how the proof of cut elimination in Schwichtenberg[77] should be adapted to get our result. □

There is an $I\Delta_0+EXP$-cut $\mathfrak{I}$ such that $I\Delta_0+EXP \vdash \forall x \forall y \in \mathfrak{I}$ itexp(x,y) exists. We have:

3.4.6 Fact: $I\Delta_0+EXP \vdash \forall A \forall x \in \mathfrak{I}\ (\Box_{U,x}A \to \Delta_U A)$.

Proof: Immediate by 3.4.5 and the fact that $\rho(p) \leq v(p)+1$. Note that A need not be in $\mathfrak{I}$! □

3.4.7 Reflection Principle I: For all formulas $A(x) \in \Pi_2$:

$$I\Delta_0+EXP \vdash \forall x(\ \Delta_\Omega A(\underline{x}) \to A(x)\ ).$$

Discussion: This is lemma 8.10 of Paris & Wilkie[87] formulated for a functional language. In appendix 7.2 it is shown how to adapt the proof from Paris & Wilkie[87] for this case. □

3.4.8 Reflection Principle II: For all formulas $A(x) \in \Pi_2$:

$$I\Delta_0+EXP \vdash \forall x \forall y \in \mathfrak{I}(\ \Box_{\Omega,y}A(\underline{x}) \to A(x)\ ).$$

Proof: Immediate by 3.4.6 and 3.4.7. Note that x need not be in $\mathfrak{I}$.

3.5 Interpretability

Consider two languages L and N. We assume for the moment N is relational, i.e. it contains no functionsymbols or constants.

Interpretations are in this paper: one dimensional global relative interpretations without parameters (for a discussion see Pudlak [83] or Visser[89]). An interpretation M of N in L is given by (i) a function F from the relation symbols of N to formulas of the language of L and (ii) a formula $\delta(a)$ of L having just a free. The image of a relation symbol has precisely $a_1,...,a_n$ free, where n is the arity of the relation symbol. The image of = need not be $a_1=a_2$. The function F is canonically extended in the following way: $(R(b_1,...,b_n))^M:=A(b_1,...,b_n)$, where A=F(R). (To make substitution of the b's possible we rename bound variables in A if necessary. In fact it would be neater to set apart bound variables for the F(R) and for δ that do not occur in the original N) $(.)^M$ commutes with the propositional connectives. $(\forall bB)^M:=\forall b(\delta(b)\rightarrow B^M)$. Similarly for $\exists$.

We can easily extend $(.)^M$ again to map proofs π (from assumptions) in N to proofs π^M from the translated assumptions in L in the obvious way. As is easily seen for a given interpretation M the lengths of the translated objects are given by a fixed polynomial in the lengths of the originals. The graphs of B^M (considered as a function in B and M) and of π^M (considered as a function in π and M) can be arithmetized by $\Delta_1{}^b$-formulas in such a way that the recursive clauses are verifiable in $I\Delta_0+\Omega_1$. Using the polynomial bound on the lengths of the values it is easy to verify that $I\Delta_0+\Omega_1$ proves that these functions are total. (This is verified in detail in Kalsbeek[89].)

The demand that N is relational is unnecessarily restrictive. To extend the notion of interpretation we employ certain standard translations from the language with function symbols to an associated relational language and back. The main problem is to see, whether the obvious properties of these translations can be verified in $I\Delta_0+\Omega_1$. The details of working with these translations are given in appendix 7.3. In the main body of the paper we will simply ignore the subtleties involved in going from functional to relational and back.

Consider theories U (with language L) and V (with language N). What does it mean to say that V is interpretable in U via M? I think the obvious definition is this: for every $B\in\alpha_V$ there is a proof in U of B^M. (I assume in this discussion that we are dealing with sentences, in the case of formulas one should consider: $(\delta[B]\rightarrow B^M)$, where $\delta[B]$ is the conjunction of $\delta(b)$'s, for all free variables b of B.) Given this definition the next step is to show: if V is interpretable in U via M and if V proves C, say by π, then there is a proof π^* in U of C^M. Roughly π^* is π^M with proofs of the translated T'-axioms plugged in at the relevant places. Now here is a problem: in a theory like $I\Delta_0+\Omega_1$ we cannot exclude that the proofs of the translated V-axioms are cofinal in the natural numbers. In other words we cannot prove that there is a bound for these proofs. The axiom that would provide such bounds is Σ_1-collection. (So we would get this basic property in $B\Sigma_1+\Omega_1$, where $B\Sigma_1:=I\Delta_0+\Sigma_1$-collection.)

We evade the problem by making a definitional move. We change the definition of interpretability in such a way that the basic properties we want are guaranteed even in $I\Delta_0+\Omega_1$, but also in such a way that our definition and the usual one collapse in the presence of $B\Sigma_1+\Omega_1$.

Define $(\forall x\exists y)^*A(x,y)$ by: $\forall u\exists v\forall x<u\exists y<vA(x,y)$. Similarly for more variables. We also write:

$(\forall x\in \alpha\exists y\in \beta)^*A(x,y)$ for: $\forall u\exists v\forall x<u(x\in\alpha\rightarrow\exists y<v(y\in\beta\wedge A(x,y)))$

Note that if $(\forall x\exists y)^*A(x,y)$ and $(\forall y\exists z)^*B(y,z)$, then: $(\forall x\exists y,z)^*(A(x,y)\wedge B(y,z))$.

Define:

$$K{:}U\rhd_a V \;:\Leftrightarrow\; \forall x\in \alpha_V \mathrm{Prov}_U(x^K).$$
$$K{:}U\rhd_s V \;:\Leftrightarrow\; (\forall x\in \alpha_V\exists p)^*\mathrm{Proof}_U(p,x^K).$$
$$K{:}U\rhd_t V \;:\Leftrightarrow\; \forall x\in \mathrm{Sent}_N(\mathrm{Prov}_V(x)\rightarrow\mathrm{Prov}_U(x^K)).$$

Our first notion is *axioms interpretability*; our second notion is *smooth interpretability*, our third notion is *theorems interpretability*. Axioms interpretability is the naive notion. One can easily show that in $B\Sigma_1+\Omega_1$ both smooth and theorems interpretability are equivalent to axioms interpretability.

For our purposes both theorems interpretability and smooth interpretability are good choices. So by interpretability we will simply mean either theorems or smooth interpretability.

$K{:}U\rhd V$ can be arithmetized in such a way that K occurs in the arithmetization as a number, so it is possible to quantify over K in the theory. Define:

$$U\rhd V \;:\Leftrightarrow\; \exists K\, K{:}\, U\rhd V$$
$$K{:}A\rhd_U B \;:\Leftrightarrow\; K{:}(U+A)\rhd(U+B)$$
$$A\rhd_U B \;:\Leftrightarrow\; (U+A)\rhd(U+B)$$
$$U\equiv V \;:\Leftrightarrow\; U\rhd V\wedge V\rhd U$$
$$A\equiv_U B \;:\Leftrightarrow\; (U+A)\equiv(U+B)$$

In Visser[90 or 89] It is shown that the following principles are valid in any sequential theory U extending $I\Delta_0+\Omega_1$. (Here $\Box{:=}\Box_U$, $\rhd{:=}\rhd_U$.)

L1	$\vdash A\Rightarrow\ \vdash\Box A$
L2	$\vdash\Box(A\rightarrow B)\rightarrow(\Box A\rightarrow\Box B)$
L3	$\vdash\Box A\rightarrow\Box\Box A$
L4	$\vdash\Box(\Box A\rightarrow A)\rightarrow\Box A$
J1	$\vdash\Box(A\rightarrow B)\rightarrow A\rhd B$
J2	$\vdash(A\rhd B\wedge B\rhd C)\rightarrow A\rhd C$
J3	$\vdash(A\rhd C\wedge B\rhd C)\rightarrow(A\vee B)\rhd C$
J4	$\vdash A\rhd B\rightarrow(\Diamond A\rightarrow\Diamond B)$
J5	$\vdash\Diamond A\rhd A$
W	$\vdash A\rhd B\rightarrow A\rhd(B\wedge\Box\neg A)$

The principles L1-J5 make up the theory IL. IL+W=:ILW. (In Visser[89] it is shown that this set of principles is incomplete for interpretations in any $\Delta_1{}^b$-axiomatized theory extending $I\Delta_0+\Omega_1$.)

4 Doing some simple model theory in $I\Delta_0+\Omega_1$

In this section we formalize a model theoretic argument from Paris and Wilkie[87]. The result will be our main technical tool in sections 5 and 6.

4.1 Main Lemma: For every $A(x,y)\in\Delta_0$ with only x,y free:

$I\Delta_0+\Omega_1\vdash(\forall I\in\Omega\text{-cuts}\Diamond_\Omega\exists x\in I\,\forall y\,A(x,y))\equiv_\Omega(EXP\wedge\exists x\forall y\,A(x,y))$.

So in more traditional terms this lemma states that $I\Delta_0+\Omega_1$ verifies the following:

$$I\Delta_0+\Omega_1+\forall I\in\Omega\text{-cuts}\ Con(I\Delta_0+\Omega_1+\exists x\in I\forall yA(x,y))$$
is equi-interpretable with
$$I\Delta_0+EXP+\exists x\forall yA(x,y).$$

Proof: Some details of the proof not given here are presented in Visser[90]. Let me first remark that it is sufficient to prove our theorem for axioms interpretability: by Parikh's theorem we automatically will have a bound on the length of the proof of the interpretation of an axiom C, which is given by a polynomial in the length of C. The presence of this bound is sufficient to guarantee both smooth and theorems interpretability (see also Visser[89]). We reason in $I\Delta_0+\Omega_1$.

"$\rhd$" Let J be a (standard) Ω-cut such that $\Box_\Omega(\forall x\in J\ itexp(x,\underline{2})\ exists)$.

Reason in $I\Delta_0+\Omega_1$ (so this is really in $I\Delta_0+\Omega_1$ in $I\Delta_0+\Omega_1$):

Suppose that for every Ω-cut I: $\Diamond_\Omega\exists x\in I\forall y\,A(x,y)$. By 3.4.3:

$\forall u\in J\,\exists I\in\Omega\text{-cuts}\ \Box_\Omega(\forall v\in I\ itexp(v,\underline{u})\ exists)$.

It follows that: $\forall u\in J\ \Diamond_\Omega\exists x\,(itexp(x,\underline{u})\ exists\wedge\forall y\,A(x,y))$. Let c be a new constant and let $V{:=}I\Delta_0+\Omega_1+\forall y\,A(c,y)+\{itexp(c,\underline{u})\ exists\mid u\in J\}$. As is easily seen V is consistent.

We want to formalize the following more or less trivial model theoretical argument (keeping in mind that model≈interpretation). For the moment read 'ω' for J. Pick a model K of V. Say D is the domain of K. Let $D^*=\{d\in D\mid \text{for some } n\in\omega\ K\models d\leq itexp(c,\underline{n})\}$. Let K^* be the restriction of K to D^*. Clearly $K^*\models EXP$. Because the $I\Delta_0$-axioms are Π_1: $K^*\models I\Delta_0$; similarly $K^*\models\forall y\,A(c,y)$. We may conclude that $K^*\models I\Delta_0+EXP+\exists x\forall y\,A(x,y)$.

We formalize the Henkin construction to produce an internal model K of V.

We proceed as follows: first define the usual Henkin tree for formulas in the language extended with Henkin constants. The formula treated at depth x will be precisely the formula with code x (if there is such a formula). So, roughly, if σ is in the tree $(\sigma)_A$ tells us whether we want A or not. Some care should be taken to make the Henkin constants not too big. We pick the leftmost path π in the tree. We cannot prove that our path is infinite in the usual sense, but we can produce an Ω-cut I_0 such that for each x in I_0 there is a sequence in π with length x. Without loss of generality we may assume that $I_0 \subseteq J$. Let K be the set of formulas given by elements of π with length in I_0. Note that if $\sigma \in \pi$, and if A 'occurs' in σ, then $A \leq |\sigma| \in I_0$, hence $A \in I_0$. It follows that $K \subseteq I_0$. Let D be the set of Henkin constants in I_0. It can be arranged that if (the code of) $\exists x B(x)$ is in K and b is the Henkin constant of $\exists x B(x)$, then b is in D. We can show: $\forall x \in I_0\, Prov_V(x) \rightarrow K(x)$.

We use d,d', e,.. to range over D. We write e.g. K(B(d,d')) for K(b(d,d')), where b(d,d') is a term for: the code of the sentence obtained by substituting the Henkin constants coded by d and d' for u and v in B(u,v). We write for x in I_0 e.g. K(C($\underline{x}$)) for K(c(x)), where c(x) is a term for: the code of the sentence obtained by substituting the efficient numeral of x for u in C(u).

K is one form of appearance of the 'model K' we are looking for. Its other form of appearence is as an interpretation $(.)^K$. The domain of this interpretation is going to be D. Let R be a relation of the language of V, we have: $R^K(d,...) :\leftrightarrow K(R(d,...))$. For arbitrary formulas B(d,...) $B^K(d,...)$ is defined as usual. For vividness we will write $K \models B(d,...)$ for $B^K(d,...)$.

As usual we can show $\forall x\, K(conj(x,y)) \leftrightarrow (K(x) \wedge K(y))$, etc. . By an *external* induction we can show:

*   For d,... in D: $K(B(d,...)) \leftrightarrow K \models B(d,...)$.

More on the meaning of * and its proof below: see the discussion on **.

Finally we can define a homomorphism f from I_0 to the natural numbers of the 'internal model' K. Consider x in I_0, f(x) will be the code of the Henkin constant of $\ulcorner \exists u\, u=\underline{x} \urcorner$. We will have: $K(f(x)=\underline{x})$. We can arrange it so (by shortening I_0 if necessary) that the range of f is downwards closed in K.

Let c* be the Henkin constant of $\exists x\, x=c$. We have $K(c^*=c)$. Moreover: $\forall x \in I_0 \Box_V(itexp(c,\underline{x})$ exists), ergo $\forall x \in I_0\, K(itexp(c,\underline{x})$ exists), so $\forall x \in I_0\, K(itexp(c^*,f(x))$ exists). We may conclude: $\forall x \in I_0\, K \models (itexp(c^*,f(x))$ exists). Let $D^* := \{d \in D \mid \exists x \in I_0\, K \models d \leq itexp(c^*,f(x))\}$. Clearly: $c^* \in D^*$ and $\forall d \in D^* \exists e \in D^*\, K \models exp(d)=e$.

Let $(.)^{K^*}$ be like $(.)^K$ exept that we use D* instead of D. We write for d,... in D*: $K^* \models B(d,...)$ for $B^{K^*}(d,...)$. Because the graph of exp is Δ_0 it follows by a simple argument that $K^* \models EXP$. Moreover $K \models \forall y\, A(c^*,y)$, A is Δ_0, hence $K^* \models \forall y\, A(c^*,y)$ and thus $K^* \models \exists x \forall y\, A(x,y)$.

Finally we have for all codes z of instances Z of Δ_0-induction: $\Box_\Omega \underline{z} \in I_0$ and $\Box_\Omega \mathrm{Prov}_V(\underline{z})$, hence $\Box_\Omega K(\underline{z})$, so $\Box_\Omega(K \models Z)$. Because these Z have Π_1 form we may conclude: $\Box_\Omega(K^* \models Z)$.

Let's look at this last argument a bit more carefully. As is well known (see e.g. Paris & Wilkie [87]) the proofs of $\ulcorner \underline{z} \in I_0 \urcorner$ and $\ulcorner \mathrm{Prov}_V(\underline{z}) \urcorner$ can be explicitily bounded by terms in z involving the usual arithmetical operations and ω_1 (ω_1-terms for short). (A moment's reflection shows that I_0 is given by a standard formula.) Hence the proof of $\ulcorner K(\underline{z}) \urcorner$ can be bounded by an ω_1-term in z.

Next we move to $\Box_\Omega(K \models Z)$ using (momentarily confusing formulas and their codes):

** $\quad \forall C \Box_\Omega(\forall d,\ldots \in D\ (K(C(d,\ldots)) \leftrightarrow K \models C(d,\ldots))\ )$.

We give the proof for the language without $\leftrightarrow$, and discuss an alternative strategy for the language with $\leftrightarrow$ afterwards.

Let's call the Ω-proof of $K \models C(d,\ldots)$ from assumptions $d,\ldots \in D$ and $K(C(d,\ldots)$: $\eta(C)$. Call the Ω-proof of $K(C(d,\ldots))$ from assumptions $d,\ldots \in D$ and $K \models C(d,\ldots)$: $\theta(C)$.

To prove ** we use $\Delta_0(\omega_1)$-induction, which is available in $I\Delta_0+\Omega_1$. To do this we must bound the $\eta(C)$, $\theta(C)$ with ω_1-terms in C; in other words the lengths (=number of symbols) of these proofs should be bounded by a polynomial in n(C), i.e. the length of C. Let's call the length of the $\eta(C)$: $\lambda(C)$; the length of $\theta(C)$: $\kappa(C)$.

I consider a specific example: the relative estimate of $\lambda(C)$ for $C=(F \to G)$. To construct $\eta(C)$ we give proofs $\pi(C)$, π' of respectively $C=\mathrm{impl}(F,G)$, and $\forall x\ K(\mathrm{impl}(x,y)) \leftrightarrow (K(x) \to K(y))$. The length of $\pi(C)$ is polynomially bounded in n(C) and the length of π' is standard. Now $\eta(C)$ looks as follows:

$$\dfrac{\theta(F)^{(1)} \qquad \dfrac{\pi(C) \quad \pi' \quad K(F \to G)}{K(F) \to K(G)}}{\dfrac{\eta(G)}{K \models (F \to G)}\,1}$$

Here the 1 indicates the cancelation of the assumption $K \models F$. We find for some standard polynomial P: $\lambda(F \to G) \le \kappa(F) + \lambda(G) + P(n(C))$

For each connective we find such a polynomial. Similarly for κ. Let Q be a polynomial that majorizes all polonomials corresponding to the connectives for both λ and κ. Noting that

$n(F)+n(G)<n(C)$ it is now easy to show that: $\lambda(C)\leq n(C).Q(n(C))$, e.g. in the case considered we have e.g:

$\lambda(C)\leq\kappa(F)+\lambda(G)+Q(n(C))\leq n(F).Q(n(F))+n(G).Q(n(G))+Q(n(C))\leq(n(F)+n(G)+1).Q(n(C))\leq n(C).Q(n(C))$.

In case the language contains $\leftrightarrow$ this argument doesn't work since $\eta(F)$, $\theta(F)$, $\eta(G)$, $\theta(G)$ all occur in e.g. $\eta(F\leftrightarrow G)$. This spoils our estimate. The alternative strategy is this: suppose we have proofs π, π' of $K(F)\leftrightarrow K\models F$, $K(G)\leftrightarrow K\models G$. Prove e.g. $K(F\leftrightarrow G)\leftrightarrow K\models(F\leftrightarrow G)$ in the naive way say the proof is σ. Now remove from σ the various occurrences of π,π' leaving the conclusions of π,π' as assumptions. Say the result of this operation is τ. Cancel the new assumptions that are the former conclusions of π as follows:

$$\vee E\;\frac{\pi \qquad \tau^{(1)} \qquad \tau^{(1)}}{K(C)\leftrightarrow K\models(C)}\,1$$

Cancel the former conclusions of π' similarly. This strategy is easily seen to yield the desired estimates.

Finally we move to $\Box_\Omega(K^*\models Z)$. Here we use:

*** $\quad\forall C\Box_\Omega(\,\forall d,...\in D^*\;(K^*\models C(d,...)\leftrightarrow K\models C(d,...))\,)$.

The proof shares many features with the proof of **. Again the lengths of the proofs will be polynomially bounded in $n(C)$. Let t range over ω_1-terms. An important lemma is:

+ $\quad\forall t\Box_\Omega(\,\forall d,...\in D^*\forall e\in D\;(\,(K\models e=t(d,...))\rightarrow e\in D^*\,)\,)$.

The lemma is proved by induction on t using a bound on the lengths of the proofs that is polynomial in $n(t)$.

We may conclude: let AX be the set of axioms of $I\Delta_0+EXP+\exists x\forall y\;A(x,y)$. We have for a suitable ω_1-term t: $\forall C\in AX\;\exists p<t(C)\;Proof_\Omega(p,\ulcorner K^*\models C\urcorner)$. By induction we find for a suitable ω_1-term u:

$$\forall x\forall C<x\;(Proof_{AX}(x,C)\rightarrow\exists z<u(x)\;Proof_\Omega(z,\ulcorner K^*\models C\urcorner)). \qquad \Box$$

"$\lhd$" Let $\mathfrak{I}$ be an $I\Delta_0+EXP$-cut such that $I\Delta_0+EXP\vdash\forall u\in\mathfrak{I}\forall v$ itexp(v,u) exists. We first show for B in Δ_0 having only x,y free:

$I\Delta_0+EXP\vdash\forall I\in\mathfrak{I}(\,\Box_\Omega^{\mathfrak{I}}$"I is a cut" $\rightarrow((\exists z\in\mathfrak{I}\;\Box_{\Omega,z}\forall x\in I\;\exists y\;B(x,y))\rightarrow\forall x\exists y\;\;B(x,y))\,)$.

Reason in $I\Delta_0+EXP$: Suppose $I\in\mathfrak{I}$, $\Box_\Omega^{\mathfrak{I}}$"I is a cut", $z\in\mathfrak{I}$ and $\Box_{\Omega,z}\forall x\in I\;\exists y\;B(x,y)$. Let $q\in\mathfrak{I}$ be the $I\Delta_0+\Omega_1$-proof of "I is a cut". By the elaboration of 3.4.2 there is a $u\leq v(q)\leq q$ such that $\Box_{\Omega,u}\underline{v}\in I$. Clearly $u\in\mathfrak{I}$. It follows that for some $w\in\mathfrak{I}$: $\forall x\Box_{\Omega,w}\exists y\;B(\underline{x},y)$. By 3.4.8 we may conclude: : $\forall x\exists y\;B(x,y)$.

From the above we have by Σ-completeness, contraposition and by weakening the statement a bit: for A in Δ_0 having only x,y free:

$$I\Delta_0+\Omega_1\vdash \Box_{EXP}(\exists x\forall y A(x,y) \to (\forall I\in \Omega\text{-cuts}\Diamond_\Omega\exists x\in I\,\forall y\, A(x,y))^{\mathfrak{I}}).$$

From this the result we're looking for is immediate using $\mathfrak{I}$ as our interpretation. □

4.2 Corollary: For any Σ_2-sentence B: $I\Delta_0+\Omega_1\vdash B\rhd_\Omega(B\wedge\neg EXP)$.

Proof: from 4.1 we have: $I\Delta_0+\Omega_1\vdash (B\wedge EXP)\rhd_\Omega\Diamond_\Omega B$, hence by principle W: $I\Delta_0+\Omega_1\vdash (B\wedge EXP)\rhd_\Omega((\Diamond_\Omega B)\wedge\Box_\Omega(B\to\neg EXP))$, so $I\Delta_0+\Omega_1\vdash (B\wedge EXP)\rhd_\Omega\Diamond_\Omega(B\wedge\neg EXP)$. By J5 we may conclude: $I\Delta_0+\Omega_1\vdash (B\wedge EXP)\rhd_\Omega(B\wedge\neg EXP)$. Also $I\Delta_0+\Omega_1\vdash (B\wedge\neg EXP)\rhd_\Omega(B\wedge\neg EXP)$, hence by J3: $I\Delta_0+\Omega_1\vdash B\rhd_\Omega(B\wedge\neg EXP)$. □

4.3 Corollary

i) Suppose A is Δ_0 having only x,y free, then:

$$I\Delta_0+\Omega_1\vdash \Box_{EXP}\forall x\exists y\, A(x,y) \leftrightarrow \Box_\Omega\exists\, I\in\Omega\text{-cuts}\ \Box_\Omega\forall x\in I\,\exists y\, A(x,y).$$

ii) Suppose B is a Σ_2-sentence, then $I\Delta_0+\Omega_1\vdash \Box_\Omega(B\to EXP)\to\Box_\Omega\neg B$.

Proof: (i) is immediate from 4.1 and (ii) is immediate from 4.2. □

4.4 Corollary: Suppose A is a Σ_1-sentence, then:

i) $I\Delta_0+\Omega_1\vdash \Box_{EXP}A\leftrightarrow\Box_\Omega\Box_\Omega A$

ii) $I\Delta_0+\Omega_1\vdash \Box_{EXP}(\Box_\Omega A\to A)\to\Box_{EXP}A$

Proof: (i) is immediate from 4.3(i). For (ii) we have:

$$\begin{array}{lll} I\Delta_0+\Omega_1\vdash \Box_{EXP}(\Box_\Omega A\to A) & \to\Box_\Omega\exists\, I\in\Omega\text{-cuts}\ \Box_\Omega(\Box_\Omega^I A\to A) & (4.3(i)) \\ & \to\Box_\Omega\Box_\Omega A & (SLP) \\ & \to\Box_{EXP}A & (4.3(i)) \end{array}$$

□

5 The closed fragment of the provability logic of $I\Delta_0+\Omega_1$ with a constant for EXP

Λ is the closed language of provability logic, i.e. Λ is the smallest set containing $\bot,\top$, which is closed under $\neg,\wedge,\vee,\to$ and $\Box$. If logical constants c,c',... are added to Λ we write: $\Lambda[c,c',\ldots]$. $\Diamond$ abbreviates $\neg\Box\neg$.

The degrees of falsity DF are defined as follows: $\Box^0\bot:=\bot$, $\Box^{n+1}\bot:=\Box\Box^n\bot$, $\Box^\omega\bot:=\top$. Dually the degrees of truth are defined by: $\Diamond^0\top:=\top$, $\Diamond^{n+1}\top:=\Diamond\Diamond^n\top$, $\Diamond^\omega\top:=\bot$. If X is a set of formulas we write Boole(X) for the set of Boolean combinations of elements of X.

We will only consider a fixed interpretation of our languages: the propositional connectives are interpreted as themselves, $\Box$ is interpreted as $\Box_\Omega$, EXP is interpreted as the arithmetical axiom EXP. The fact that our interpretation is constant makes that we can conveniently confuse modal formulas and their arithmetical counterparts. From now on we will do so.

The system LC[EXP] in Λ[EXP] is given by the following principles:

L1	$\vdash A \Rightarrow \vdash \Box A$
L2	$\vdash \Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$
L3	$\vdash \Box A \rightarrow \Box\Box A$
L4	$\vdash \Box(\Box A \rightarrow A) \rightarrow \Box A$
C1	$\vdash \Box(\mathrm{EXP} \rightarrow B) \leftrightarrow \Box\Box B$, for $B \in$ Boole(DF)
C2	$\vdash \Box(\neg\mathrm{EXP} \rightarrow B) \leftrightarrow \Box B$, for $B \in$ Boole(DF)

We verify the validity of LC[EXP] for interpretations in $I\Delta_0+\Omega_1$. C2 is immediate from 4.3(ii).

In our verification of C1 we will use the "some finite subset" notation: $\{A \| P(A)\}$ means approximately: some finite (possibly empty) subset of $\{A \mid P(A)\}$. When the notation is repeatedly used however it will function in an anaphoric way: so sometimes it means: the finite subset we were talking about; or even: the finite subset connected in the evident way with the finite subset we were talking about.

Verification of C1 in $I\Delta_0+\Omega_1$: Consider B in Boole(DF). Clearly B is equivalent to a sentence of the form $\bigwedge\{\Box^{\alpha}\bot \rightarrow \Box^{k}\bot \| k<\alpha\}$. (Here: α ranges over $\omega+1$.) By 4.3(i) we have that:

$$I\Delta_0+\Omega_1 \vdash \Box(\mathrm{EXP}\rightarrow B) \leftrightarrow \Box\exists I\in \Omega\text{-cuts}\ \Box\bigwedge\{\Box^{\alpha,I}\bot \rightarrow \Box^{k}\bot \| k<\alpha\}.$$

On the other hand:

$$\begin{array}{lll}
I\Delta_0+\Omega_1 \vdash \exists I\in \Omega\text{-cuts}\ \Box\bigwedge\{\Box^{\alpha,I}\bot \rightarrow \Box^{k}\bot \| k<\alpha\} & \rightarrow & \\
\quad \exists I\in \Omega\text{-cuts}\ \bigwedge\{\Box(\Box^{\alpha,I}\bot \rightarrow \Box^{k}\bot) \| k<\alpha\} & \rightarrow & \\
\quad \exists I\in \Omega\text{-cuts}\ \bigwedge\{\Box(\Box^{k+1,I}\bot \rightarrow \Box^{k}\bot) \| k<\alpha\} & \rightarrow & (\mathrm{SLP}) \\
\quad \bigwedge\{\Box^{k+1}\bot \| k\in\omega\} & \rightarrow & (\alpha^*=\inf\{k \| k\in\omega\}) \\
\quad \Box^{1+\alpha^*}\bot & \rightarrow & \\
\quad \Box\bigwedge\{\Box^{\alpha}\bot \rightarrow \Box^{k}\bot \| k<\alpha\} & \rightarrow & \\
\quad \exists I\in \Omega\text{-cuts}\ \Box\bigwedge\{\Box^{\alpha,I}\bot \rightarrow \Box^{k}\bot \| k<\alpha\}. & &
\end{array}$$

Ergo $I\Delta_0+\Omega_1 \vdash \Box(\mathrm{EXP}\rightarrow B) \leftrightarrow \Box\Box B$. $\Box$

5.1 Theorem

i) For every $A\in\Lambda$[EXP]: LC[EXP] $\vdash \Box A \leftrightarrow \Box^{\alpha}\bot$, for some $\alpha\in\omega+1$.

ii) For every $A\in\Lambda$[EXP] there is a $B\in$ Boole(DF$\cup$\{EXP\}): LC[EXP] $\vdash A \leftrightarrow B$.

iii) For every $A\in\Lambda$[EXP]: LC[EXP] $\vdash \Box A \Rightarrow$ LC[EXP] $\vdash A$.

Proof: for (i) and (ii) it is sufficient to show that for $B\in \mathrm{Boole}(DF\cup\{EXP\})$: $LC[EXP]\vdash \Box B \leftrightarrow \Box^{\alpha}\bot$, for some $\alpha\in\omega+1$. The rest of the argument is a simple induction. As is easily seen there are C,D in Boole(DF) such that $LC[EXP]\vdash B \leftrightarrow ((EXP\to C)\wedge(\neg EXP\to D))$, hence $LC[EXP]\vdash \Box B \leftrightarrow (\Box(EXP\to C)\wedge\Box(\neg EXP\to D))$, so by C1, C2: $LC[EXP]\vdash \Box B \leftrightarrow (\Box\Box C\wedge\Box D)$. So by the usual reasoning the desired result follows.

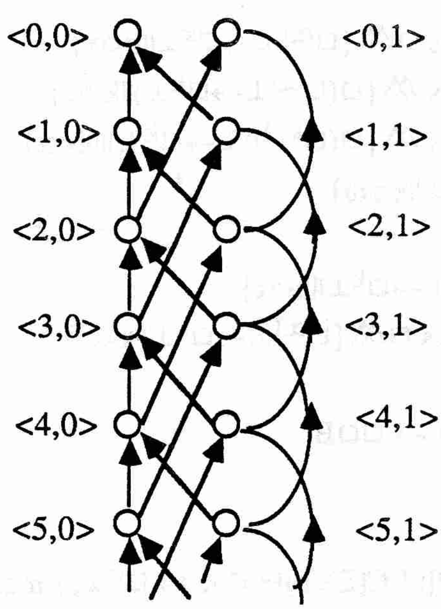
To prove (iii) suppose $LC[EXP]\vdash \Box A$. We note that by (ii): A is LC[EXP]-equivalent to: $(EXP\to \bigwedge\{\Box^{\alpha}\bot\to\Box^{k}\bot \mid k<\alpha\})\wedge(\neg EXP\to\bigwedge\{\Box^{\beta}\bot\to\Box^{n}\bot\mid n<\beta\})$. If both conjunctions are empty we are done. If not it follows that for some m $LC[EXP]\vdash \Box^{m}\bot$ and hence $I\Delta_0+\Omega_1\vdash\Box^{m}\bot$, quod non. □

Consider two Kripke models $K=\langle W,R,\Vdash\rangle$ and $K'=\langle W',R',\Vdash'\rangle$. A *Λ-bisimulation* β between K and K' is a relation between W and W' such that: (i) for every k in W there is a k' in W' with kβk'; (ii) for every k' in W' there is a k in W with kβk'; (iii) if kβk' and kRs, then there is an s' with k'R's' and sβs'; (iv) if kβk' and k'R's', then there is an s with kRs and sβs'. As is easily seen: if β is a Λ-bisimulation between K and K' and kβk', then for $A\in\Lambda$: $k\Vdash A \Leftrightarrow k'\Vdash' A$.

5.2 Theorem: $LC[EXP]\vdash A \Leftrightarrow I\Delta_0+\Omega_1\vdash A$.

Proof: "⇒" has already been checked. For "⇐" suppose $I\Delta_0+\Omega_1\vdash A$. Suppose that LC[EXP] does not prove A, then LC[EXP] does not prove □A, so □A must be LC[EXP]-equivalent to $\Box^{k}\bot$ for some k. We find $I\Delta_0+\Omega_1\vdash\Box A$, hence $I\Delta_0+\Omega_1\vdash\Box^{k}\bot$. Quod non. □

We define a Kripke model M:



The model M

The domain of M is $\{<n,i> | n\in\omega, i\in\{0,1\}\}$; M has an accessibility relation given by: $<n,i>R<m,j> :\Leftrightarrow n>m+j$. We stipulate $<n,i>\Vdash EXP :\Leftrightarrow i=1$. The forcing relation is extended to the whole language in the usual way. We show that LC[EXP] is valid in M. As is easily seen R is transitive and upwards wellfounded. Hence the principles L1-L4 are valid on M.

Let N be the model with domain ω and accessibility relation R^* given by: $nR^*m :\Leftrightarrow n>m$. Define a relation β between nodes of N and nodes of M by $n\beta<m,i> :\Leftrightarrow n=m$. It is easily seen that β is a Λ-bisimulation between N and M. We may conclude that for A in Λ: $<n,0>\Vdash A \Leftrightarrow <n,1>\Vdash A$.

Verification of C1 in M: suppose B is a Boolean combination of degrees of falsity.

First suppose $<n,i>\Vdash\Box\Box B$ and $<n,i>R<m,j>$ and $<m,j>\Vdash EXP$, i.e. $j=1$. We have: $n>m+1$, so $<n,i>R<m+1,0>R<m,0>$. Hence $<m,0>\Vdash B$. B is in Λ, so $<m,1>\Vdash B$. We may conclude: $<n,i>\Vdash\Box(EXP\rightarrow B)$.

Suppose for the converse: $<n,i>\Vdash\Box(EXP\rightarrow B)$ and $<n,i>R<m,j>R<p,k>$. Clearly $n>m+j>p+k$, so $n>p+1$ and thus $<n,i>R<p,1>$. $<p,1>\Vdash EXP$ and so $<p,1>\Vdash B$. B is in Λ so we may conclude: $<p,k>\Vdash B$. Ergo $<n,i>\Vdash\Box\Box B$ □

Verification of C2 in M: suppose B is a Boolean combination of degrees of falsity.

One direction is trivial. Suppose: $<n,i>\Vdash\Box(\neg EXP\rightarrow B)$ and $<n,i>R<m,j>$. Clearly $<n,i>R<m,0>$, so $<m,0>\Vdash B$. B is in Λ so we may conclude: $<m,j>\Vdash B$. Ergo $<n,i>\Vdash\Box B$. □

5.3 Theorem: LC[EXP]$\vdash A \Leftrightarrow$ M$\Vdash A$.

Proof: entirely analogous to the proof of 5.2. □

6 The closed fragment of the interpretability logic of $I\Delta_0+\Omega_1$ with a constant for EXP

The system ILC[EXP] is given by the following principles:

L1	$\vdash A \Rightarrow\ \vdash\Box A$
L2	$\vdash\Box(A\rightarrow B)\rightarrow(\Box A\rightarrow\Box B)$
L3	$\vdash\Box A\rightarrow\Box\Box A$
L4	$\vdash\Box(\Box A\rightarrow A)\rightarrow\Box A$
J1	$\vdash\Box(A\rightarrow B)\rightarrow A\rhd B$
J2	$\vdash(A\rhd B\wedge B\rhd C)\rightarrow A\rhd C$

J3	$\vdash (A \rhd C \wedge B \rhd C) \to (A \vee B) \rhd C$
J4	$\vdash A \rhd B \to (\Diamond A \to \Diamond B)$
J5	$\vdash \Diamond A \rhd A$
W	$\vdash A \rhd B \to A \rhd (B \wedge \Box \neg A)$
C	$\vdash (EXP \wedge B) \equiv \Diamond B$, where $B \in$ Boole(DF)

We verify the validity of ILC[EXP] for interpretations in $I\Delta_0+\Omega_1$.

Verification of C in $I\Delta_0+\Omega_1$:

Suppose $B \in$ Boole(DF). Clearly B is equivalent to a sentence of the form $\bigvee\{\Diamond^k \top \wedge \Box^\alpha \bot \| k<\alpha\}$, where α ranges over $\omega+1$. By 4.1 we have that:

$$I\Delta_0+\Omega_1 \vdash (EXP \wedge B) \equiv (\forall\, I \in \Omega\text{-cuts } \Diamond \bigvee\{\Diamond^k \top \wedge \Box^{\alpha,I} \bot \| k<\alpha\}).$$

By contraposition of the reasoning concerning the verification of C1:

$$I\Delta_0+\Omega_1 \vdash (\forall\, I \in \Omega\text{-cuts } \Diamond \bigvee\{\Diamond^k \top \wedge \Box^{\alpha,I} \bot \| k<\alpha\}) \leftrightarrow \Diamond B.$$

We may conclude: $I\Delta_0+\Omega_1 \vdash (EXP \wedge B) \equiv \Diamond B$. □

6.1 Theorem

i) For every $A \in \Lambda[\rhd, EXP]$: ILC[EXP] $\vdash \Box A \leftrightarrow \Box^\alpha \bot$, for some $\alpha \in \omega+1$.

ii) For every $A, B \in \Lambda[\rhd, EXP]$: ILC[EXP] $\vdash A \rhd B \leftrightarrow \Box^\alpha \bot$, for some $\alpha \in \omega+1$.

iii) For every $A \in \Lambda[\rhd, EXP]$ there is a $B \in$ Boole(DF$\cup\{EXP\}$): LC[EXP] $\vdash A \leftrightarrow B$.

iv) For every $A \in \Lambda[EXP]$: LC[EXP] $\vdash \Box A \Rightarrow$ LC[EXP] $\vdash A$.

Proof: for (i), (ii), (iii) it is sufficient to show that for $A, B \in$ Boole(DF$\cup\{EXP\}$): ILC[EXP] $\vdash \Box A \leftrightarrow \Box^\alpha \bot$, for some $\alpha \in \omega+1$ and ILC[EXP] $\vdash A \rhd B \leftrightarrow \Box^\alpha \bot$, for some $\alpha \in \omega+1$. The rest of the argument is a simple induction. We can restrict ourselves to the case of $\rhd$ noting that $\Box A$ is equivalent to $\neg A \rhd \bot$.

First consider C in Boole(DF). We show: ILC[EXP] $\vdash (EXP \wedge C) \equiv \Diamond^\alpha \top$, for some α. We have:

$$\text{ILC[EXP]} \vdash (EXP \wedge C) \equiv \Diamond C \equiv \Diamond^\alpha \top.$$

Next we show: ILC[EXP] $\vdash (\neg EXP \wedge C) \equiv \Diamond^\beta \top$, for some β. First note:

$$\begin{aligned} \text{ILC[EXP]} \vdash (EXP \wedge C) &\rhd \Diamond C \\ &\rhd (\Diamond C \wedge \Box(C \to \neg EXP)) \\ &\rhd \Diamond(\neg EXP \wedge C) \\ &\rhd (\neg EXP \wedge C) \end{aligned}$$

Also: ILC[EXP] $\vdash (\neg EXP \wedge C) \rhd (\neg EXP \wedge C)$, hence ILC[EXP] $\vdash C \rhd (\neg EXP \wedge C)$. We find:

$$\begin{aligned} \text{ILC[EXP]} \vdash (\neg EXP \wedge C) &\equiv C \\ &\equiv (C \vee \Diamond C) \end{aligned}$$

$\equiv\Diamond^{\beta}\top$

Consider A in Boole(DF$\cup${EXP}). Clearly A is equivalent to (EXP$\wedge$C)$\vee$($\neg$EXP$\wedge$D) for some C and D in Boole(DF). By the above: ILC[EXP]$\vdash$ (EXP$\wedge$C)$\equiv\Diamond^{\alpha}\top$, for some α and ILC[EXP]$\vdash$ ($\neg$EXP$\wedge$D)$\equiv\Diamond^{\beta}\top$, for some β. Hence ILC[EXP]$\vdash$ A$\equiv$($\Diamond^{\alpha}\top\vee\Diamond^{\beta}\top$)$\equiv\Diamond^{\gamma}\top$, for some γ. We may conclude for A,B in Boole(DF$\cup${EXP}): ILC[EXP]$\vdash$ A$\rhd$B $\leftrightarrow$ $\Diamond^{\gamma}\top\rhd\Diamond^{\delta}\top$ for some γ,δ. If $\gamma\geq\delta$: ILC[EXP]$\vdash$ A$\rhd$B $\leftrightarrow$ $\top$, and we are done. If $\gamma<\delta$:

$$\begin{aligned}\text{ILC[EXP]}\vdash A\rhd B &\leftrightarrow \Diamond^{\gamma}\top\rhd\Diamond^{\delta}\top\\ &\leftrightarrow \Diamond^{\gamma}\top\rhd(\Diamond^{\delta}\top\wedge\Box\neg\Diamond^{\gamma}\top)\\ &\leftrightarrow \Diamond^{\gamma}\top\rhd(\Diamond^{\delta}\top\wedge\Box^{\gamma+1}\bot)\\ &\leftrightarrow \Diamond^{\gamma}\top\rhd\bot\\ &\leftrightarrow \Box^{1+\gamma}\bot\end{aligned}$$

The proof of of (iv) is the same as the proof of 5.1(iii). □

6.2 Theorem: ILC[EXP]$\vdash$A $\Leftrightarrow$ IΔ_0+$\Omega_1$$\vdash$A.

Proof: the same as the proof of 5.2. □

We define a Kripke model M as follows: the domain of M is {<n,i>|n$\in\omega$,i$\in$ {0,1}}; M has an two accessibility relations R and S given by: <n,i>R<m,j> :$\Leftrightarrow$ n>m+j and <n,i>S<m,j> :$\Leftrightarrow$ n+i$\geq$m+j. We stipulate <n,i>$\Vdash$EXP :$\Leftrightarrow$ i=1. The forcing relation is extended to the whole language in the usual way using R as the accessibility relation for □ and:

x$\Vdash$A$\rhd$B :$\Leftrightarrow$ for all y: xRy and y$\Vdash$A $\Rightarrow$ there is a z with ySz and z$\Vdash$B.

As before R is transitive and upwards wellfounded. We have: R$\subseteq$S; S is reflexive and transitive; S satisfies property P, i.e.: xRySz $\Rightarrow$ xRz.

Excursion: The property 'xRySz $\Rightarrow$ xRz' makes M into an ILP-model (see Visser[88] or Visser[90] or De Jongh & Veltman[90]). This implies that the principle: A$\rhd$B $\rightarrow$ □(A$\rhd$B) is valid on M. There are a priori reasons, given the fact that M fully characterizes what is and what is not provable in the restricted language and seeing the methods we used, that this should be so. For suppose M would provide a counterexample to the principle. This shows or at least strongly suggests that IΔ_0+Ω_1 is not finitely axiomatizable. (The loophole here is that it might be the case that, yes, IΔ_0+Ω_1 is in fact finitely axiomatizable but, no, its finite axiomatizability is not verifiable in IΔ_0+Ω_1.) But the problem of finite axiomatizability of IΔ_0+Ω_1 is connected with difficult complexity theoretic problems and it seems clear that the methods used in section 4 are not 'heavy' enough to solve such problems. So a full characterization of the valid principles of Λ[EXP,$\rhd$] in IΔ_0+Ω_1 using light methods as in section 4 cannot but satisfy principle P.

Verification of C in M: suppose B is a Boolean combination of degrees of falsity.

First suppose $<n,i>\Vdash\Box\Box B$ and $<n,i>R<m,j>$ and $<m,j>\Vdash EXP$, i.e. $j=1$. We have: $n>m+1$, so $<n,i>R<m+1,0>R<m,0>$. Hence $<m,0>\Vdash B$. B is in Λ, so $<m,1>\Vdash B$. We may conclude: $<n,i>\Vdash \Box(EXP\rightarrow B)$.

Suppose for the converse: $<n,i>\Vdash\Box(EXP\rightarrow B)$ and $<n,i>R<m,j>R<p,k>$. Clearly $n>m+j>p+k$, so $n>p+1$ and thus $<n,i>R<p,1>$. $<p,1>\Vdash EXP$ and so $<p,1>\Vdash B$. B is in Λ so we may conclude: $<p,k>\Vdash B$. Ergo $<n,i>\Vdash\Box\Box B$ □

6.3 Theorem: $ILC[EXP]\vdash A \Leftrightarrow M\Vdash A$.

Proof: entirely analogous to the proof of 5.3. □

7. Appendices

7.1 Cut Elimination

In this section we provide an estimate on the rate of growth of the number of symbols of a proof when we apply cutelimination. To save space the presentation is parasitic on the one in Schwichtenberg[77]. The reader should look up Schwichtenberg's treatment: we just present the additions to his paper that are necessary to get our estimate. Locally in this section we follow Schwichtenberg's conventions, numbering of theorems, etc..

$n(\phi)$ is the number of symbols in ϕ. Similarly for $n(d)$, $n(\Gamma)$. Note that we must consider a variable as complex: we stipulate that e.g. x_5 is represented as x101 and thus $n(x_5)=4$. Because we want to Gödelize the proofs it would be more natural to take a linearized version of the system. Because linearization causes only a few inessential details we refrain from doing this.

We stipulate that sets of formulas are written: $\{\phi_1,...,\phi_n\}$. The empty set is represented by: $\{\}$. In $I\Delta_0+\Omega_1$ we have a recursive function available that eliminates repetitions from representations of sets and puts the elements of the representation in a fixed order, so we may assume that sets are always represented without repetitions and in a fixed order.

Here follow the additions to Schwichtenberg[77]: We work in the system described by Schwichtenberg with terms but without extra rules for identity. (Identity will be handled by adding finitely many axioms. These will be treated on a par with other axioms.)

2.3.1. WEAKENING LEMMA. $n(d,\Gamma)\leq n(d).(n(\Gamma)+1)$.

PROOF: d,Γ has less symbols than the result of inserting Γ after each symbol of d.

2.4.1. SUBSTITUTION LEMMA. $n(d(s))\leq n(d(x)).n(s)$

2.4.2. SUBSTITUTION-WEAKENING LEMMA. $n(d(s),\Gamma)\leq n(d(x)).(n(\Gamma)+n(s))$

2.5. INVERSION LEMMA. (i) If $d\vdash\Gamma,\phi_0\wedge\phi_1$, then we can find $d^*_i\vdash\Gamma,\phi_i$ (i=0,1) with $|d^*_i|\leq|d|$, $\rho(d^*_i)\leq\rho(d)$, $n(d^*_i)\leq n(d).n(\phi_0\wedge\phi_1)$.

(ii) If $d\vdash\Gamma,\forall x\psi(x)$, then we can find $d^*\vdash\Gamma,\psi(x)$ with $|d^*|\leq|d|$, $\rho(d^*)\leq\rho(d)$, $n(d^*)\leq n(d).n(\forall x\psi(x))$.

PROOF: We restrict ourselves to (ii). Let ϕ be $\forall x\psi(x)$. If $\phi\in\Gamma$, we take $d^*:=d,\psi(x)$. Our result follows by the weakening lemma. Assume $\phi\notin\Gamma$.

Case 1: ϕ is a not a p.f. in the last inference of d. Then this inference has the form

$$\frac{\Lambda,\phi,\psi_j \quad \text{for all } j<k}{\Lambda,\phi,\Delta}$$

With m.f. ψ_j, p.f. Δ and s.f. Λ,ϕ and $\Gamma=\Lambda,\Delta$.The case that k=0 is trivial. In case k>0 we apply the induction hypothesis. Let the immediate subproofs of d be d_i. We find $d_i^*\vdash\Lambda,\psi(x),\psi_i$ with $|d_i^*|\leq|d_i|$, $\rho(d_i^*)\leq\rho(d_i)$, $n(d_i^*)\leq n(d_i).n(\phi)$. The result follows by the inference:

$$\frac{\Lambda,\psi(x),\psi_i \quad \text{for all } i<k}{\Lambda,\psi(x),\Delta}$$

Suppose e.g. k=2. We have:
$n(d^*)\leq n(d_0^*)+n(d_1^*)+1+n(\Gamma)+n(\psi(x))+1\leq(n(d_0)+n(d_1)).n(\phi)+n(\Gamma)+n(\psi(x))+2\leq$
$\leq(n(d_0)+n(d_1)+1+n(\Gamma)+1+n(\phi)).n(\phi)$.
The last term is clearly equal to $n(d).n(\phi)$.

Case 2: ϕ is a p.f. in the last inference of d. If ϕ is not a s.f. in the last inference of d, the inference has the form:

$$\frac{\Gamma,\psi(x)}{\Gamma,\phi}$$

With m.f. $\psi(x)$, p.f. ϕ and s.f. Γ, where $\phi\notin\Gamma$. Here we can pick as d^* simply the immediate subproof of d. If ϕ is a s.f. in the last inference of d, the inference has the form:

$$\frac{\Gamma,\phi,\psi(x)}{\Gamma,\phi}$$

With m.f. $\psi(x)$, p.f. ϕ and s.f. Γ. Here we find d* by applying the Induction Hypothesis to the immediate subproof d_0 of d. Note: $n(d^*)\leq n(d_0).n(\phi)\leq n(d).n(\phi)$.

2.6. REDUCTION LEMMA. $n(d)\leq(n(d_0)+n(d_1)).n(d_0).n(d_1)$.

PROOF.

Case 1: We treat the case that k=2, the cases that k=0,1 being easier or similar. Let the immediate subproofs of d_0 be d_{00} and d_{01}. By the induction hypothesis the direct subproofs of d are going to be $\leq(n(d_{00})+n(d_1)).n(d_{00}).n(d_1)$ respectively $\leq(n(d_{01})+n(d_1)).n(d_{01}).n(d_1)$. Hence:

$$\begin{aligned}
n(d)\leq\ & (n(d_{00})+n(d_1)).n(d_{00}).n(d_1)+(n(d_{01})+n(d_1)).n(d_{01}).n(d_1)+1+n(\Lambda,\Delta,\Theta)\leq\\
\leq\ & (n(d_{00})+n(d_1)).n(d_{00}).n(d_1)+(n(d_{01})+n(d_1)).n(d_{01}).n(d_1)+1+(n(d_0)-2)+n(d_1)\leq\\
\leq\ & (n(d_0)+n(d_1)-1).(n(d_{00})+n(d_{01})).n(d_1)+n(d_0)+n(d_1)-1\leq\\
\leq\ & (n(d_0)+n(d_1)-1).(n(d_0)-1).n(d_1)+(n(d_0)+n(d_1)-1)\leq\\
\leq\ & (n(d_0)+n(d_1)).n(d_0).n(d_1)
\end{aligned}$$

Case 2.1: $n(\Gamma,\Delta)\leq n(\Gamma,\phi)+n(\Delta,\neg\phi)\leq 2.n(\Gamma,\phi).n(\Delta,\neg\phi)$.

Case 2.2: Let the immediate subproof of d_0 be d_{0i}. We split the cases that ϕ is a s.f. in the last inference of d_0 and that ϕ is not.

Suppose ϕ is not a s.f. in the last inference of d_0. The conclusion of d_{0i} is of the form Γ,ϕ_i. By weakening we get d_{0i},Δ with conclusion Γ,Δ,ϕ_i. Here $n(d_{0i},\Delta)\leq n(d_{0i}).n(d_1)$. By the inversion lemma we get a proof d_{1i} of $\Delta,\neg\phi_i$ with $n(d_{1i})\leq n(d_1).n(\phi)$. Clearly d_{1i},Γ has conclusion $\Gamma,\Delta,\neg\phi_i$ and $n(d_{1i},\Gamma)\leq n(d_{1i}).n(d_0)$. By cutelimination we combine d_{0i},Δ and d_{1i},Γ into a proof d of Γ,Δ. We have:

$$\begin{aligned}
n(d)\leq\ & n(d_{0i}).n(d_1)+n(d_{1i}).n(d_0)+1+n(d_0)+n(d_1)\leq\\
\leq\ & (n(d_0)-1).n(d_1)+n(d_1).n(\phi).n(d_0)+1+n(d_0)+n(d_1)\leq\\
\leq\ & (1+n(\phi)).n(d_0).n(d_1)+(1+n(\phi)).n(d_0)+1\leq\\
\leq\ & (3+2.n(\phi)).n(d_0).n(d_1)\leq (n(d_0)+n(d_1)).n(d_0).n(d_1)
\end{aligned}$$

(Clearly for k=0,1: $n(d_k)\geq n(\phi)+2$.)

Suppose ϕ is a s.f. in the last inference of d_0. The conclusion of d_{0i} is of the form Γ,ϕ,ϕ_i. Apply the Induction Hypothesis to d_{0i} and d_1. We obtain a proof d' of Γ,Δ,ϕ_i with $n(d')\leq (n(d_{0i})+n(d_1)).\ n(d_{0i}).n(d_1)$. By the inversion lemma we get a proof d_{1i} of $\Delta,\neg\phi_i$ with

$n(d_{1i})\leq n(d_1).n(\phi)$. Weakening gives us d_{1i},Γ with conclusion $\Gamma,\Delta,\neg\phi_i$ and:

$$n(d_{1i},\Gamma)\leq n(d_{1i}).n(d_0)\leq n(d_1).n(\phi).n(d_0).$$

We obtain our final proof d by applying cutelimination to the conclusions of d' and d_{1i},Γ. Clearly:

$$\begin{aligned}
&n(d)\leq n(d')+n(d_{1i},\Gamma)+1+n(d_0)+n(d_1)\leq\\
&\leq (n(d_{0i})+n(d_1)).n(d_{0i}).n(d_1)+n(d_1).n(\phi).n(d_0)+1+n(d_0)+n(d_1)\leq\\
&\leq (n(d_0)-n(\phi)-1+n(d_1)).(n(d_0)-n(\phi)-1).n(d_1)+n(d_1).n(\phi).n(d_0)+1+n(d_0)+n(d_1)=\\
&= (n(d_0)+n(d_1)).n(d_0).n(d_1)-(n(d_0)+n(d_1)).(n(\phi)+1).n(d_1)-(n(\phi)+1).n(d_0).n(d_1)+\\
&+ (n(\phi)+1)^2.n(d_1)+n(d_1).n(\phi).n(d_0)+1+n(d_0)+n(d_1)=\\
&= (n(d_0)+n(d_1)).n(d_0).n(d_1)-(n(d_0)+n(d_1)).(n(\phi)+1).n(d_1)-n(d_0).n(d_1)+\\
&+ (n(\phi)+1)^2.n(d_1)+1+n(d_0)+n(d_1)\leq \ldots
\end{aligned}$$

Note that $n(\phi)+1\leq n(d_1)$ and hence $(n(\phi)+1)^2.n(d_1)\leq(n(d_0)+n(d_1)).(n(\phi)+1).n(d_1)$.
So:

$$\ldots \leq (n(d_0)+n(d_1)).n(d_0).n(d_1)-n(d_0).n(d_1)+1+n(d_0)+n(d_1)\leq\ldots$$

Note that $n(d_0)\geq 3$ and $n(d_1)\geq 3$ and hence $n(d_0).n(d_1)\geq n(d_0)+n(d_1)+1$. So:

$$\ldots \leq (n(d_0)+n(d_1)).n(d_0).n(d_1)$$

Case 2.3.: Let the immediate subproof of d_0 be d_{00}. As before we split the cases that ϕ is a s.f. in the last inference of d_0 and that ϕ is not. The case that ϕ is not a s.f. in the last inference of d_0 is entirely analogous to the corresponding case in 2.2. Suppose ϕ is a s.f. in the last inference of d_0. The conclusion of d_{00} is of the form $\Gamma,\phi,\psi(s)$. Apply the Induction Hypothesis to d_{00} and d_1. We obtain a proof d' of $\Gamma,\Delta,\psi(s)$ with $n(d')\leq(n(d_{00})+n(d_1)).n(d_{00}).n(d_1)$. By the inversion lemma we get a proof $d_{10}(x)$ of $\Delta,\neg\psi(x)$, where x does not occur in Δ with $n(d_{10}(x))\leq n(d_1).n(\phi)$. We form $d_{10}(s),\Gamma$ with conclusion $\Gamma,\Delta,\neg\psi(s)$. By the Substitution-Weakening Lemma:

$$n(d_{10}(s),\Gamma)\leq n(d_{10}(x)).(n(s)+n(\Gamma))\leq n(d_1).n(\phi).n(d_0).$$

We obtain our final proof d by applying cutelimination to the conclusions of d' and $d_{10}(s),\Gamma$. Clearly:

$$\begin{aligned}
&n(d)\leq n(d')+n(d_{10}(s),\Gamma)+1+n(d_0)+n(d_1)\leq\\
&\leq (n(d_{00})+n(d_1)).n(d_{00}).n(d_1)+n(d_1).n(\phi).n(d_0)+1+n(d_0)+n(d_1) \leq\\
&\leq (n(d_0)-n(\phi)-1+n(d_1)).(n(d_0)-n(\phi)-1).n(d_1)+n(d_1).n(\phi).n(d_0)+1+n(d_0)+n(d_1)
\end{aligned}$$

From this point on the reasoning proceeds as in 2.2.

Let $\exp(x):=2^x$; $\mathrm{itexp}(x,0):=x$, $\mathrm{itexp}(x,y+1):=\exp(\mathrm{itexp}(x,y))$, $\exp^2(x):=\mathrm{itexp}(x,2)$.

2.7. CUT-ELIMINATION THEOREM. *If $d\vdash\Gamma$ and $\rho(d)>0$, then we can find $d'\vdash\Gamma$ with*

$\rho(d)<\rho(d')$ and $|d'|\leq exp(|d|)$ and $n(d')\leq exp^2(n(d))$.

PROOF. $n(d'_i)\leq exp^2(n(d_i))$. Let $m:=sup(n(d_0),n(d_1))$. We have:

$$n(d')\leq(n(d'_0)+n(d'_1)).n(d'_0).n(d'_1)\leq exp(exp(m)+1).exp^2(m+1)\leq exp^2(m+2)\leq exp^2(n(d)).$$

(Γ could be empty, but by our convention the number of symbols representing the empty set is is non-zero.)

2.7.1. COROLLARY. *If $d\vdash\Gamma$, then we can find a cut-free proof $d^*\vdash\Gamma$ with $|d^*|\leq itexp(|d|,\rho(d))$ and $n(d^*)\leq itexp(n(d),2.\rho(d))$.*

Note that, if we think of d and d* as coded as numbers we find: $d^*\leq exp(k.n(d^*))$ for some standard k. So if d* is large enough we get $d^*\leq exp^2(n(d^*))$. Hence we get:

$$d^*\leq itexp(n(d),2.(\rho(d)+1))\leq itexp(d,2.(\rho(d)+1)).$$

Our argument can be formalized in the usual way using the bounds one proves as bounds in the induction. Hence we get:

$I\Delta_0+EXP\vdash\forall d,\Gamma,x\ ((Proof^*(d,\Gamma)\wedge itexp(d,2.(\rho(d)+1))=x)\rightarrow\exists d^*\leq x\ Cutfreeproof^*(d^*,\Gamma))$.

Here Proof* and Cutfreeproof* are formalizations of the notion of proof and cutfree proof as treated above. Now note that proofs in any ordinary reasonable proofsystem can be multi-exponentially transformed in proofs in Schwichtenberg's system. (In fact, I think, one can do much better.) Moreover cutfree proofs in Schwichtenberg's system can be almost trivially transformed in tableaux proofs as in the system used by Paris & Wilkie. Hence for some standard k we get for any $\Delta_1{}^b$-axiomatized theory U:

$$I\Delta_0+EXP\vdash\forall x,p,A\ ((Proof_U(p,A)\wedge itexp(p,2.\rho(p)+k)=x)\rightarrow\exists p^*\leq x\ Tabproof_U(p^*,A)).$$

7.2 Satisfaction & Reflection

We construct a satisfaction relation SAT for Δ_0-formulas in $I\Delta_0+EXP$. SAT will be in $\Delta_0(exp)$ (this means that SAT is the translation into our official language of a formula, in our language enriched with a function symbol for exponentiation, in which all quantifiers are bounded by terms possibly involving exponentiation). The fact that $SAT\in\Delta_0(exp)$ will derive its usefulness from the well known fact that $I\Delta_0+EXP\vdash I\Delta_0(exp)$.

We work in $I\Delta_0+EXP$. Let σ code a finite partial function ϕ. By default we set $\sigma(u):=0$ if $u\notin Dom(\phi)$. $m(\sigma):=max(Range(\phi)\cup\{2\})$. Call the set of assignments ASS. We write $\sigma[i/y]$ for the unique σ' such that for all j $(i\neq j\rightarrow\sigma(i)=\sigma(j))$ and $(\sigma')_i=y$. In this section we write $\subsetneq$ for the subformula/subterm relation.

As is well known already in $I\Delta_0+\Omega_1$ we have an evaluation function VAL for terms and sequences of numbers, such that $VAL(\ulcorner t(v_i,...)\urcorner,\sigma)= t(\sigma(i),...)$. Note that $VAL(t,\sigma) \leq m(\sigma)^{n(t)} \leq 2^{(|m(\sigma)|+1).n(t)} \leq m(\sigma)\#t\#m$ for a suitable standard m.

$$
\begin{aligned}
SAT(A,\sigma) :\leftrightarrow\ & \sigma\in ASS \wedge A\in \Delta_0 \wedge \exists\tau \\
& \quad \tau \text{ is a sequence} \wedge (\tau)_{length(\tau)-1}=\langle A,\sigma\rangle \wedge \forall i<length(\tau) \\
& \quad\quad \exists s,t\subseteq A\ \exists\sigma'\in ASS \\
& \quad\quad\quad (\tau)_i=\langle\ulcorner s=t\urcorner,\sigma'\rangle \wedge VAL(s,\sigma')=VAL(t,\sigma') \\
& \quad\quad \vee \\
& \quad\quad \exists s,t\subseteq A\ \exists\sigma'\in ASS \\
& \quad\quad\quad (\tau)_i=\langle\ulcorner\neg s=t\urcorner,\sigma'\rangle \wedge VAL(s,\sigma')\neq VAL(t,\sigma') \\
& \quad\quad \vee \\
& \quad\quad \ldots\ldots\ldots\ldots\ldots \\
& \quad\quad \vee \\
& \quad\quad \exists B\subseteq A\ \exists C,t,v_k\subseteq B\ \exists\sigma'\in ASS \\
& \quad\quad\quad B=\ulcorner\forall v_k\leq t\ C\urcorner \wedge (\tau)_i=\langle B,\sigma'\rangle \wedge \forall y\leq VAL(t,\sigma')\ \exists j<i\ (\tau)_j=\langle C,\sigma'[k/y]\rangle \\
& \quad\quad \vee \\
& \quad\quad \exists B\subseteq A\ \exists C,v_k\subseteq B\ \exists\sigma'\in ASS \\
& \quad\quad\quad B=\ulcorner\neg\forall v_k\leq t\ C\urcorner \wedge (\tau)_i=\langle B,\sigma'\rangle \wedge \exists y\leq VAL(t,\sigma')\ \exists j<i \\
& \quad\quad\quad (\tau)_j=\langle\neg C,\sigma'[k/y]\rangle
\end{aligned}
$$

Clearly all quantifiers in the definition of SAT except $\exists\tau$ can be bounded by τ.

Let's give a rough estimate of τ. Let t* be the biggest term in A. First consider $\langle B,\sigma'\rangle$ in τ and an immediate predecessor $\langle C,\sigma''\rangle$ in τ of $\langle B,\sigma'\rangle$. We estimate $m(\sigma'')$ in terms of t* and $m(\sigma')$: the only interesting case is that of the quantifiers, here we find for some term t:

$$m(\sigma'')\leq \max(m(\sigma'),VAL(t,\sigma'))\leq t\#m(\sigma')\#m\leq t^*\#m(\sigma')\#m.$$

Similarly it follows that the number of immediate predecessors of $\langle B,\sigma'\rangle$ is $\leq t^*\#m(\sigma')\#m$. Hence the sequence-length of τ will be $\leq$ than

$$
\begin{aligned}
& 1+t^*\#m(\sigma)\#m+t^*\#(t^*\#m(\sigma)\#m)\#m+....= \\
& = 1+m(\sigma)\#\omega_1^{(0)}(t^*\#m)+m(\sigma)\#\omega_1^{(1)}(t^*\#m)+...+m(\sigma)\#\omega_1^{(n(A)-2)}(t^*\#m)\leq \\
& \leq n(A).(m(\sigma)\#\omega_1^{(n(A))}(t^*\#m)).
\end{aligned}
$$

How long can $\langle B,\sigma'\rangle$ be? Clearly $m(\sigma')\leq m(\sigma)\#\omega_1^{(n(A))}(t^*\#m)$. Also the codes of the elements of the domain of σ' are substrings of A. The code of $m(\sigma')$ will have length $\leq|m(\sigma)\#\omega_1^{(n(A))}(t^*\#m)|$. So the length of $\langle B,\sigma'\rangle$ considered as a string will be $\leq k.n(A).(|m(\sigma)\#\omega_1^{(n(A))}(t^*\#m)|+1)$ for some standard k. So the length of τ considered as a string will be $\leq n(A).(m(\sigma)\#\omega_1^{(n(A))}(t^*\#m)).(k.n(A).(|m(\sigma)\#\omega_1^{(n(A))}(t^*\#m)|+1)+2) =:F(A,\sigma)$.

So for some standard r: $\tau\leq \exp(r.F(A,\sigma))$. Noting that $\omega_1^{(s)}(p)\leq \text{itexp}(s+|||p|||,3)$, we see that a bound for τ in terms of A and σ is available in $I\Delta_0$+EXP.

Write $\sigma \models A$ for: SAT(A,σ)

7.2.1 Lemma: $\sigma \models (.)$ commutes with the propositional connectives and the bounded quantifiers. Moreover for every $A \in \Delta_0$ $\sigma \models A$ or $\sigma \models \neg A$.

Proof: Entirely routine. □

7.2.2 Lemma: Suppose t is substitutable for v_k in A, then: $\sigma \models A[t/v_k] \Leftrightarrow \sigma[k/VAL(t,\sigma)] \models A$.

Proof: Entirely routine. □

7.2.3 Theorem: Let $r \in \omega$ and A(x) be a Σ_2-formula, then

$$I\Delta_0+EXP \vdash \forall x\ (\ \sigma(x) \rightarrow Tabcon(I\Delta_0+\Omega_r+\sigma(\underline{x}))\ ).$$

Proof: This is just a slight variant of the proof of lemma 8.10 of Paris & Wilkie[87]. Suppose $A(x)=\exists y \forall z B(x,y,z)$, where $B \in \Delta_0$. Let M be model of $I\Delta_0$+EXP+A(a), where $a \in M$ and suppose $M \models Tabincon(I\Delta_0+\Omega_r+A(\underline{a}))$. Work in M. (Of course we also could give a straightforward formalization of the proof in $I\Delta_0$+EXP, but thinking 'in the model' is more pleasant from the heuristic point of view.)

Let p be a tableaux proof of a contradiction from $I\Delta_0+\Omega_r+A(\underline{a})$, say $p=\Gamma_1,\ldots,\Gamma_s$. Let t* be the bigest term occuring in p and let C be the biggest formula occuring in p. Note that $t^* \geq a$, because the numeral of a occurs in p. For some b we have: $\forall z B(a,b,z)$. Let m be standard such that $VAL(t,\sigma) \leq t\#m(\sigma)\#m$. Define $c:=\max(b,t^*\#m)$, $d:=\omega_r^{(2.s)}(c)$.

For each $i<s$ and $X \in \Gamma_i$ we define an assignment $\sigma_{i,X}$ with domain the free variables of X and range bounded by d, as follows:

$\sigma_{0,X}$ is empty (for clearly in X no free variables occur);

Consider $\sigma_{i+1,X}$. Suppose the predecessor of X at stage i is Y. We consider several cases:

i) (α)-(δ) do not introduce new variables. Put $\sigma_{i+1,X}:=\sigma_{i,Y}$;

ii) In case (ε) some spurious new free variables may be introduced. Put $\sigma_{i+1,X}(v):=\sigma_{i,Y}(v)$ if $v \in Dom(\sigma_{i,Y})$, $\sigma_{i+1,X}(v):=0$ otherwise;

iii) We turn to case (ζ): we get $\neg E(v_k)$ from $\neg \forall x E(x)$. Put $\sigma_{i+1,X}(v):=\sigma_{i,Y}(v)$ if $v \in Dom(\sigma_{i,Y})$. For v_k there are three possibilities: first $\neg\forall$ may stand for the first existential quantifier of A. In this case put $\sigma_{i+1,X}(v_k):=b$. Secondly $\neg\forall$ may stand for the first existential quantifier in axiom Ω_r. This means $\neg\forall x E(x)$ is a translation of: $\exists x\ \omega_r(t)=x$ for some term t. Put $\sigma_{i+1,X}(v_k):=\omega_r(VAL(t,\sigma_{i,Y}))$. Thirdly $\neg\forall$ may stand for a bounded existential quantifier, where E is Δ_0. Say $\neg\forall x E(x)=\neg\forall x \leq t' F(x)$. Put: $\sigma_{i+1,X}(v_k)$:=the least $z \leq VAL(t,\sigma_{i,Y})$ such that $\sigma_{i,Y}[k/z] \models \neg F(v_k)$, if such a z exists,

$\sigma_{i+1,X}(v_k):=0$ otherwise.

7.2.4 Lemma: For all $i<s$ $m(\sigma_{i+1,X})\leq\omega_r^{(2.i)}(c)$.

Proof: The only serious growth of the elements of Range($\sigma_{i,X}$) occurs due to clause (ζ). We treat the subcase of $\exists x\ \omega_r(t)=x$. So suppose we get $\sigma_{i+1,X}$ by applying the second subcase of (ζ). Let the predecessor stage be Y. We find (assuming $i\neq 0$):

$$\omega_r(VAL(t,\sigma_{i,Y}))\leq\omega_r(t\#m(\sigma_{i,Y})\#m)\leq\omega_r(t*\#\omega_r^{(2.i-2)}(c)\#m)\leq\omega_r(c\#\omega_r^{(2.i-2)}(c))\leq$$
$$\leq\omega_r(\omega_r^{(2.i-2)}(c)\#\omega_r^{(2.i-2)}(c))\leq\omega_r(\omega_1(\omega_r^{(2.i-2)}(c)))\leq\omega_r^{(2.i)}(c).\qquad\Box$$

Our theorem is immediate from the following lemma:

7.2.5 Lemma: For all $i\leq s$ there is an $X\in\Gamma_i$ such that

(i) For all Δ_0-formulas $C\in X$ $\sigma_{i,X}\models C$;

(ii) For all Σ_1-formulas $(\exists v,...C)\in X$ $\sigma_{i,X}\models\exists v,...\leq\underline{d}\ C$ (where $C\in\Delta_0$);

(iii) For all Π_1-formulas $(\forall v,...C)\in X$ $\sigma_{i,X}\models\forall v,...\leq\underline{d}\ C$ (where $C\in\Delta_0$).

Proof: The proof is by induction on i. (Note that our induction predicate is Δ_0(exp)!)

i=0: Here the most natural thing is to assume that there is only one X in Γ_0. The elements of X are (a) standardly finitely many identity axioms, (b) standardly finitely many axioms concerning S,+ and ., (c) non-standardly finitely many Δ_0-induction axioms, (d) A, (e) Ω_1. (a) and (b) give no problems. The claim does not apply to (d) and (e). Let's consider (c).

Suppose E is an induction axiom in X (remember: E might be non-standard!). E has the following form:

$$\forall v,...\forall w((D(0,v,...)\wedge\forall v_j{<}w(D(v_j,v...)\rightarrow D(S(v_j),v...)))\rightarrow\forall v_j{<}wD(v_j,v...)).$$

Let V be the (non-standardly) finite set of variables {v,...} of the block in the front of E (except w). Write $\sigma[V,d]\sigma'$:$\Leftrightarrow$ σ and σ' differ only on elements of V and the values assigned by σ' to the elements of V are $\leq$d. One can show using an easy induction (on the number of elements of V) that:

$$\sigma\models\forall v,...\leq\underline{d}\forall w\leq\underline{d}((D(0,v,...)\wedge\forall v_j{<}w(D(v_j,v...)\rightarrow D(S(v_j),v...)))\rightarrow\forall v_j{<}wD(v_j,v...))$$

if and only if

$$\forall\sigma'[V,d]\sigma\forall x\leq d(\sigma'[j/0]\models D(v_j,v...)\wedge\forall y{<}\underline{x}(\sigma'[j/y]\models D(v_j,v...)\rightarrow\sigma'[j/S(y)]\models D(v_j,v...)))$$
$$\rightarrow\forall y{<}\underline{x}\ \sigma'[j/y]\models D(v_j,v...)\ ).$$

This last formula is an instance of the Δ_0(exp) Induction Scheme.

i=j+1: Suppose $Y\in\Gamma_j$ satisfies the induction hypothesis. Let X be a successor of Y in Γ_i. We treat the cases that X is introduced by ε and ζ.

Let $\forall v_k\ E(v_k)$ and $E(t)$ be the premiss and the conclusion involved. There are three possibilities: $\forall v_k\ E(v_k)$ is Π_2,Π_1 or Δ_0. If it is Π_2, then $\forall v_k\ E(v_k)=\Omega_1$. So we have to check: $\sigma_{i+1,X}\models \exists v_p\underline{\leq d}\ \omega_r(t)=v_p$. This follows easily by the observation that:

$$\omega_r(VAL(t,\sigma_{i+1,X}))\leq\omega_r(t\#m(\sigma_{i+1,X})\#m)\leq\omega_r(t^*\#\omega_r^{(2.i)}(c)\#m)\leq\omega_r(c\#\omega_r^{(2.i)}(c))\leq$$
$$\leq\omega_r(\omega_r^{(2.i)}(c)\#\omega_r^{(2.i)}(c))\leq\omega_r(\omega_1(\omega_r^{(2.i)}(c)))\leq\omega_r^{(2.i+2)}(c)\leq\omega_r^{(2.s)}(c)=d.$$

In case $\forall v_k\ E(v_k)$ is Π_1 by the induction hypothesis we have: $\sigma_{i,Y}\models\forall v_k\underline{\leq d}\ E^*(v_k)$ (where E^* is the result of bounding unbounded universal quantifiers in E by $\underline{d}$). It follows that $\sigma_{i,X}\models E^*(t)$, noting that by our earlier argument $VAL(t,\sigma_{i+1,X})\leq d$. The case that $\forall v_k\ E(v_k)$ is Δ_0 is similar.

Let $\neg\forall v_k\ E(v_k)$ and $\neg E(v_p)$ be the premiss and the conclusion involved. There are three possibilities: first $\neg\forall$ may stand for the first existential quantifier of A. In this case $\sigma_{i,X}(v_p):=b$. We leave it to the reader to verify that indeed $\sigma_{i,X}\models\forall z\underline{\leq d}\ B(\underline{a},v_p,z)$. Secondly $\neg\forall$ may stand for the first existential quantifier in axiom Ω_r. This means that $\neg\forall v_k\ E(v_k)$ is a translation of: $\exists v_k\ \omega_r(t)=v_k$ for some term t. $\sigma_{i,X}(v_p):=\omega_r(VAL(t,\sigma_{j,Y}))$. As is easily seen $\sigma_{i,X}\models\neg E(v_p)$, i.e. $\sigma_{i,X}\models\omega_r(t)=v_p$. Thirdly $\neg\forall$ may stand for a bounded existential quantifier, where $\neg\forall v_k\ E(v_k)$ is Δ_0, say $\neg\forall v_k\ E(v_k)=\neg\forall v_k\leq t\ F(v_k)$. By the induction hypothesis $\sigma_{i,Y}\models\neg\forall v_k\leq t\ F(v_k)$. Hence for some $z\leq VAL(t,\sigma_{i,Y})$ $\sigma_{i,Y}[k/z]\models\neg F(v_k)$ and thus for some $z\leq VAL(t,\sigma_{i,Y})$ $\sigma_{i,Y}[p/z]\models\neg F(v_p)$. $\sigma_{i+1,X}(v_p):=$(the least $z\leq VAL(t,\sigma_{i,Y})$ such that $\sigma_{i,Y}[p/z]\models\ \neg F(v_p)$). Ergo $\sigma_{i+1,X}\models\neg F(v_p)$. □

Note: Our argument hides much more generality than explicitely stated. The reader may amuse him/herself by proving the following variants.

i) Let $r\in\omega$ and $A(x)\in\Sigma_2$, then $I\Delta_0+EXP\vdash\forall x\ (\ \sigma(x)\rightarrow Tabcon(I\Delta_0+\Omega_r+\neg EXP+\sigma(\underline{x}))\ )$.

ii) Let $A(x)\in\Sigma_2$, then $I\Delta_0+SUPEXP\vdash\forall x\ (\ \sigma(x)\rightarrow Con(I\Delta_0+EXP+\sigma(\underline{x}))\ )$.

The principle in (ii) is the uniform Π_2-Reflection Principle $UREF(I\Delta_0+EXP,\Pi_2)$. By an easy argument one can modify (ii) to:

iii) $I\Delta_0+SUPEXP$ and $I\Delta_0+\Omega_1+UREF(Q,\Pi_2)$ prove the same theorems.

7.3 From Functional to Relational and back

We write $P^n\{x\}$ for: 'some polynomial of the form $x^n+a_1.x^{n-1}+\ldots+a_{n-1}.x+a_n$'. Here the a_j are standard. Moreover n will always be standard. $P\{x\}$ will stand for: 'some $P^n\{x\}$, for standard n'.

Let L be a language with finitely many relation symbols, function symbols, constants. Let L* be the relational variant of L. I.e. L* has the same relation symbols as L; for each n-ary function symbol f in L there is an n+1-ary relation symbol F in L*; for each constant c in L there is a unary relation symbol C in L*. L* has only relation symbols corresponding to relation symbols, function symbols and constants in L. It is convenient here to treat constants as 0-ary function symbols. So we don't have to mention the case of constants separately.

Let PL be predicate logic in L and let PL* be the corresponding theory in L*, where PL* is predicate logic + $\forall x,...\exists! y\, F(x,...,y)$ (for all F corresponding to f and c in L). To fix ideas we work with a Natural Deduction System with the ordinary schematic identity rules. The reader is free to substitute his or her preferred system (with cuts!) for ours. I predict he/she will find that the proofs go through with minimal changes. (The use of schematic identity rules is an unessential simplification: if π is a proof in our system, it can be transformed in a simple way into a proof π' in the corresponding system with finitely many (concrete) identity axioms, with $n(\pi')\leq P^3\{n(\pi)\}$.) We assume that in our languages $\leftrightarrow$ is a defined symbol.

We provide a translation $(.)^*$ from L to L* and a translation $(.)^\circ$ from L* to L such that $I\Delta_0+\Omega_1$ verifies:

i) $PL\vdash A \Leftrightarrow PL^*\vdash A^*$

ii) $PL\vdash B^\circ \Leftrightarrow PL^*\vdash B$

iii) $PL\vdash (A\leftrightarrow A^{*\circ})$

iv) $PL^*\vdash (B\leftrightarrow B^{\circ *})$

Both translations will commute with the logical connectives. We will first show that to prove (i)-(iv) it suffices to show (in $I\Delta_0+\Omega_1$):

i') $PL\vdash A \Rightarrow PL^*\vdash A^*$

ii') $PL^*\vdash B \Rightarrow PL\vdash B^\circ$

iii) $PL\vdash (A\leftrightarrow A^{*\circ})$

iv) $PL^*\vdash (B\leftrightarrow B^{\circ *})$

Proof:

"(i'),(ii'),(iii) $\Rightarrow$ (i)" Suppose $PL^*\vdash A^*$, then $PL\vdash A^{*\circ}$ and hence $PL\vdash A$.

"(i'),(ii'),(iv) $\Rightarrow$ (iii)" Suppose $PL\vdash B^\circ$, then $PL^*\vdash B^{\circ *}$ and hence $PL^*\vdash B$. □

Note that by Parikh's Theorem, there are explicit bounds to the proofs whose existence is claimed in (i)-(iv). E.g. the number of symbols of the PL*- proof π^* of A^* in (i) will be bounded by $P\{n(\pi)\}$, where π is the PL-proof of A. Of course our proofs will explicitely provide such polynomials.

$(.)^\circ$ is defined as follows: replace in formulas A of L atoms of the form $F(x,...,y)$ by $f(x,...)=y$.

To define $(.)^*$, we first have to define the function $t[x]$ from terms t and variables x such that $x\notin FV(t)$ to formulas of L* as follows. We assume that our variables are $v_0,v_1,v_2,...$. Their official forms are v, v0, v1, v10, v11, v100,... . $x,x_1,y,y',z,...$ are really metavariables running over the variables. Define for $x\notin FV(t)$:

$y[x]:=(y=x)$

$f(t_1,...,t_n)[x]:=\exists x_1...\exists x_n(t_1[x_1]\wedge...\wedge t_n[x_n]\wedge F(x_1,...,x_n,x))$, where $x_1,...x_n$ are the first n variables not in $FV(f(t_1,...,t_n))\cup\{x\}$ (in ascending order).

We estimate the number of symbols $n(t[x])$ in $t[x]$ in terms of $n(t)$ and $n(x)$. Our estimate will have the form $K(n(t))+n(x)$. We have:

$n(y[x])=n(y)+n(x)+3$,

$n(f(t_1,...,t_n)[x])\le K(n(t_1))+...+K(n(t_n))+3.(n(x_1)+...+n(x_n))+5.n+3+n(x)$.

(There are: n existential quantifiers, n conjunctions, 2.n brackets corresponding to these conjunctions, n commas after 'F'. Finally there are 'F' and two brackets.)

Hence it suffices if K satisfies:

$K(n(y))\ge n(y)+3$,

$K(n(f(t_1,...,t_n)))\ge K(n(t_1))+...+K(n(t_n))+3.(n(x_1)+...+n(x_n))+5.n+3$.

We prove first that for some standard s not depending on the t_i:

$n(x_1)+...+n(x_n)\le n(t_1)+...+n(t_n)+s$.

Suppose $FV(f(t_1,...,t_n))\cup\{x\}=\{z_0,...,z_m\}$, where for $j<k$ $n(z_j)\le n(z_k)$. Clearly $n(x_i)\le n(v_{m+i})$, because x_i will be v_j for some $j\le m+i$. Now $n(z_0)+...+n(z_{m-1})\le n(t_1)+...+n(t_n)$, hence $m\le n(t_1)+...+n(t_n)$. We have: $n(x_i)\le n(v_{m+n})\le 2+\text{entier}({}^2\log(m+n+1))$, ergo $n(x_1)+...+n(x_n)\le n.(2+\text{entier}({}^2\log(n(t_1)+...+n(t_n)+n+1)))$. Because n is fixed, we find:

$n(x_1)+...+n(x_n)\le n(t_1)+...+n(t_n)+s$ for some fixed, standard s.

So we can find a standard c such that it is sufficient if:

$K(n(y))\ge n(y)+3$,

$K(n(f(t_1,...,t_n)))\ge K(n(t_1))+...+K(n(t_n))+3.(n(t_1)+...+n(t_n))+c$.

Clearly we can take $K(n):=P^2\{n\}$.

How many symbols does it take to write down a witnessing sequence σ for $t[x]=A$? The length of σ would be $\le n(t)$. Each item in σ would be a tripel $<t',x',A'>$. A moment's reflection shows that $n(t')\le n(A')$, $n(x')\le n(A')$, $n(A')\le n(A)$. Hence each item in σ counts less symbols than $3.(P^2\{n(t)\}+n(x))$. So $n(\sigma)\le 3.n(t).(P^2\{n(t)\}+n(x))$.

By inspection of our argument we see that in $I\Delta_0+\Omega_1$ we can define (the arithmetization of) the function $\lambda t,x.t[x]$ with $\Sigma_1{}^b$-graph and prove it to be total.

Define $(.)^*$ as follows:

$(R(t_1,...,t_n))^*:=\exists x_1...\exists x_n(t_1[x_1]\wedge...\wedge t_n[x_n]\wedge R(x_1,...,x_n))$, where $x_1,...x_n$ are the first n variables not in $FV(R(t_1,...,t_n))$ (in ascending order). (= is treated just as the other relations.)

$(.)^*$ commutes with the logical connectives and the quantifiers.

Let us write $t_x[y]$ for: $t[x][y/x]$. The notion "$t_x[y]$" is slightly more flexible than "$t[y]$". We need it to make some of the necessary inductions work.

7.3.1 Lemma (in $I\Delta_0+\Omega_1$):

a) For all t and all $z,z' \notin FV(t)$, z' substitutable for z in t[z]: $PL^* \vdash \forall y...\exists z'\ t(y,...)_z[z']$,

b) For all t and all $z,u \notin FV(t)$, for all z',u' such that z' is substitutable for z in t[z], and such that u' is substitutable for u in t[u]:

$$PL^* \vdash \forall y...,z',u'\ (\ t(y,...)_z[z'] \rightarrow (t(y,...)_u[u'] \leftrightarrow z'=u'))\ .$$

c) For all t and all $z \notin FV(t)$, for all u, such that u is substitutable for z in t[z]:

$$PL^* \vdash \forall y...,z,u\ (\ t(y,...)_z[u] \leftrightarrow t(y,...)[u]\ )$$

Proof: We leave it to the reader to show that $\forall y...\exists z'\ t(y,...)_z[z']$, has proof π, with $n(\pi) \leq P^3\{n(t)\}+q.n(z')$, where q is standard. (c) is an immediate consequence of (b).

We prove (b). Let's call the proof from $t_z[z']$ and $t_u[u']$ of $z'=u'$: $\eta(t,z,u,z',u')$, and the proof from $t_z[z']$ and $z'=u$ 'of $t_u[u']$: $\theta(t,z,u,z',u')$. The proof is by induction on t. The atomic case is trivial.

To simplify inesentially let us suppose that t is of the form f(v,w) for certain terms v and w. So for certain variables a,b,d,e: $f(v,w)_z[z']$ is $\exists a,b\ (v[a] \wedge w[b] \wedge F(a,b,z'))$ and $f(v,w)_u[u']$ is $\exists d,e\ (v[d] \wedge w[e] \wedge F(d,e,u'))$. Let a',b',d',e' be distinct variables not occurring in $FV(t) \cup \{z',u'\}$, such that a' is substitutable for a in v[a], b' is substitutable for b in w[b], d' is substitutable for d in v[d], e' is substitutable for e in w[e]. We can arrange it so that n(a'),n(b'),n(d'),n(e') are smaller than n(t)+k for some fixed standard k. (This can be seen by an argument analogous to the one for estimating "$n(x_1)+...+n(x_n)$" above.)

Now $\eta(t,z,u,z',u')$ will look roughly as follows: assume $\exists a,b(v[a] \wedge w[b] \wedge F(a,b,z'))$ and $\exists d,e\ (v[d] \wedge w[e] \wedge F(d,e,u'))$. By two $\exists$-eliminations and four $\wedge$-eliminations it is sufficient to prove our result from: $v_a[a']$, $w_b[b']$, $F(a',b',z')$, $v_d[d']$, $w_e[e']$, $F(d',e',u)$. $v_a[a']$ and $v_d[d']$ give by $\eta(v,a,d,a',d')$: $a'=d'$; $w_b[b']$ and $w_e[e']$ give by $\eta(w,b,e,b',e')$ $b'=e'$. From $a'=d'$, $b'=e'$, $F(a',b',z')$, $F(d',e',u')$ we have: $z'=u'$.

So for certain standard k,m,n,p:

$$\begin{aligned} n(\eta(t,z,u,z',u')) \leq\ & n(\eta(v,a,d,a',d'))+n(\eta(w,b,e,b',e')) \\ & k.(n(v[a])+n(w[b])+n(v[d])+n(w[e])+ \\ & \quad n(v_a[a'])+n(w_b[b'])+n(v_d[d'])+n(w_e[e'])) + \\ & m.(n(a)+n(b)+n(d)+n(e)+n(a')+n(b')+ n(d')+n(e')) + \\ & p.(n(z')+n(u')) +n. \end{aligned}$$

Note that $n(a)<P^1\{n(t)\}$, $n(a')<P^1\{n(t)\}$, etcetera. Moreover $n(v[a]) \leq P^2\{n(v)\}+n(a)<P^2\{n(t)\}$,

$n(v_a[a'])\leq P^2\{n(v)\}+n(a')<P^2\{n(t)\}$, etcetera. Suppose that our estimate has the form: $n(\eta(t,z,u,z',u'))\leq H(n(t))+p.(n(z')+n(u'))$: we find that it is sufficient that:

$$H(n(t))\geq H(n(v))+H(n(w))+k.P^2\{n(t)\}.$$

Hence we can take: $H(n(t)):=P^3\{n(t)\}$.

Next we do θ. Assume $\exists a,b(v[a]\wedge w[b]\wedge F(a,b,z'))$, $z'=u'$. By one $\exists$-elimination and two $\wedge$-eliminations it is sufficient to prove our conclusion from $v_a[a']$, $w_b[b']$, $F(a',b',z')$, $z'=u'$. First show: $\exists d'\ d'=a'$ and $\exists e'\ e'=b'$. By two $\exists$-eliminations it is sufficient to prove our conclusion from $v_a[a']$, $w_b[b']$, $F(a',b',z')$, $z'=u'$, $d'=a'$, $e'=b'$. From $v_a[a']$ and $d'=a'$ we get by $\theta(v,a,d,a',d')$: $v_d[d']$. Similarly we get $w_e[e']$. Clearly: $F(d',e',u')$. So by two $\wedge$-introductions and two $\exists$-introductions we find: $\exists d,e(v[d]\wedge w[e]\wedge F(d,e,u'))$.

As is easily seen we get the same estimate as for η. □

7.3.2 Lemma (in $I\Delta_0+\Omega_1$)

a) For all terms t,w of L, for all variables x,z with $z\notin FV(w)\cup FV(w[t/y])\cup\{x\}$ and $x\notin FV(t)\cup(FV(w)\setminus\{y\})$, x substitutable for y in w[z]:

$$PL^*\vdash \exists x(t[x]\wedge w[z][x/y])\leftrightarrow w[t/y][z].$$

b) For all formulas A, terms t and variables x of L, such that t is substitutable for y in A and such that x is substitutable for y in A* and $x\notin FV(t)\cup(FV(A)\setminus\{y\})$:

$$PL^*\vdash \exists x(t[x]\wedge A^*[x/y]))\leftrightarrow (A[t/y])^*.$$

Note that in (a) the condition on the variables is certainly fullfilled if $x\neq z$ and $x,z\notin FV(t)\cup FV(w)$.

Proof: (a) Induction on w. Call the proof from right to left $\eta(w,t,x,z)$ and the proof from left to right $\theta(w,t,x,z)$. First the atomic case. There are three possibilities: w is a constant, w is a variable not equal to y, w is y. In case w is a constant, say c, we have to show: $\exists x(t[x]\wedge C(z))\leftrightarrow C(z)$. θ is trivial. By 7.3.1(a) $n(\eta)$ can be estimated by: $P^3\{n(t)\}+q.(n(x)+n(z))$, for some standard q. The case that w is a variable not equal to y is similar. If w is y, we get: $\exists x(t[x]\wedge x=z)\leftrightarrow t[z]$. Clearly by 7.3.1(b) $n(\theta)$ is estimated by $P^3\{n(t)\}+r.(n(x)+n(z))$ for standard r. For η reason as follows: Clearly $\exists x\ x=z$. Suppose t[z] and x=z by 7.3.1(b): t[x], hence $\exists x(t[x]\wedge x=z)$. By $\exists$-elimination we can cancel the assumption x=z. So $n(\eta)$ can be estimated by: $P^3\{n(t)\}+s.(n(x)+n(z))$ for standard s.

Suppose e.g. that w=f(u,v) for terms u and v. We have to show that:

$$\exists x(t[x]\wedge\exists a,b\ (u[a][x/y]\wedge v[b][x/y]\wedge F(a,b,z)))\leftrightarrow \exists e,g\ (u[t/y][e]\wedge v[t/y][g]\wedge F(e,g,z)).$$

Let's first do η: Assume $\exists e,g\ (u[t/y][e]\wedge v[t/y][g]\wedge F(e,g,z))$. By one $\exists$-elimination and two $\wedge$-elimations it is sufficient to prove our result from: $u[t/y]_e[e']$, $v[t/y]_g[g']$, $F(e',g',z)$. Here e',g' are chosen in such a way that $e',g'\notin FV(w)\cup FV(t)\cup\{x,z,a,b\}$ and e' is substitutable for e in $u[t/y][e]$ and g' s substitutable for g in $v[t/y][g]$. By 7.3.1(c) we may conclude: $u[t/y][e']$ and $v[t/y][g']$. As is easily seen the conditions of the induction hypothesis are satisfied for u,t,x,e', so by $\eta(u,t,x,e')$ we may conclude $\exists x(t[x]\wedge u[e'][x/y])$. Similarly: $\exists x(t[x]\wedge u[g'][x/y])$. By two $\exists$-eliminations and two $\wedge$-eliminations it is sufficient to prove our result from: $t[x]$, $u[e'][x/y]$, $t_x[x']$, $v[g'][x'/y]$). Here x' is chosen as small as possible such that x' is substitutable for x in $t[x]$ and for y in $v[g']$, $x'\notin FV(w)\cup FV(t)\cup\{x,z,a,b,e',g'\}$. By 7.3.1(b): $x=x'$. Hence $t[x]$, $u[e'][x/y]$, $v[g'][x/y]$, $F(e',g',z)$. Clearly $\exists a\ e'=a$ and $\exists b\ g'=b$, so by two $\exists$-eliminations it is sufficient to prove our result from: $e'=a$, $g'=b$, $t[x]$, $u[e'][x/y]$, $v[g'][x/y]$, $F(e',g',z)$. By 7.3.1(b) we get: $t[x]$, $u[a][x/y]$, $v[b][x/y]$, so we may conclude: $\exists x(t[x]\wedge\exists a,b\ (u[a][x/y]\wedge v[b][x/y]\wedge F(a,b,z)))$.

We turn to θ: suppose $\exists x(t[x]\wedge\exists a,b\ (u[a][x/y]\wedge v[b][x/y]\wedge F(a,b,z)))$. By several $\exists$-eliminations and $\wedge$-eliminations it is sufficient to prove our result from: $t_x[x']$, $u_a[a'][x'/y]$, $v_b[b'][x'/y]$, $F(a',b',z)$. Here a',b',x' are distinct variables such that $a',b',x'\notin FV(w)\cup FV(t)\cup\{x,z,e,g\}$ and such that a' is substitutable for a in $u[a]$, b' is substitutable for b in $v[b]$, x' is substitutable for x in $t[x]$ and for y in $u[a']$ and $v[b']$. As is easily seen using 7.3.1(c) it easily follows that: $u[a'][x'/y]$, $v[b'][x'/y]$. Clearly we may apply the induction hypothesis so by $\theta(u,t,x',a')$ we have: $u[t/y][a']$. Similarly: $v[t/y][b']$. Clearly $\exists e\ a'=e$ and $\exists g\ b'=g$. So by two $\exists$-eliminations it is sufficient to prove our result from: $a'=e$, $b'=g$, $u[t/y][a']$, $v[t/y][b']$, $F(a',b',z)$. By 7.3.1(b): $u[t/y][e]$, $v[t/y][g]$, $F(e,g,z)$ and by a few introductions we are done.

Let us first estimate the 'local' variables of these steps. We treat one example. Consider e'. We demanded that $e'\notin FV(w)\cup FV(t)\cup\{x,z,a,b\}$ and e' is substitutable for e in $u[t/y][e]$. Let $y_1,\ldots,y_n$ be the free variables occurring in $u[t/y]$. It is easily seen that $n(y_1)+\ldots+n(y_n)\leq n(u)+n(t)$. Hence by previous reasoning the length of the variables bound by a quantifier in whose scope e occurs is $\leq n(u)+n(t)+k$ for some standard k. So clearly we may choose $e'\leq n(w)+n(t)+s$ for some standard s. Moreover e.g. the step from $u[t/y]_e[e']$ to $u[t/y][e']$ can be estimated by:

$$P^3\{n(u[t/y])\}+m.n(e') \leq P^3\{\max(n(w[t/y]),n(w)+n(t))\}.$$

So we have for some standard k:

$$n(\eta(w,t,x,z))\leq n(\eta(u,t,x,e'))+n(\eta(v,t,x,g'))+P^3\{n(w).\max(n(t),n(x))\}+k.n(z).$$

It follows that:

$$n(\eta(w,t,x,z))\leq P^4\{n(w).\max(n(t),n(x))\}+k.n(z).$$

A similar estimate holds for θ.

(b) The proof is by induction on A. Call the proof from right to left $\eta(A,t,x)$ and the proof from left to right $\theta(A,t,x)$. The proofs for the atomic case are analogous to the case of $f(u,v)$ in (a). We get the estimate: $P^4\{n(A).\max(n(t),n(x))\}$.

We treat one example of the induction step: the η-case, where $A=(B\rightarrow C)$.

Suppose $((B[t/y])^* \rightarrow (C[t/y]^*))$. By 7.3.1(a) $\exists x\, t[x]$. So it is sufficient to prove our desired conclusion from t[x]. Suppose $(B[x/y])^*$, by $\exists$-introduction: $\exists x(t[x] \wedge (B[x/y])^*)$. So by $\theta(B,t,x)$: $(B[t/y])^*$ and hence $(C[t/y])^*$. By $\eta(C,t,x)$: $\exists x(t[x] \wedge (C[x/y])^*)$, so it sufficient to prove our conclusion from: $t_x[x']$, $(C[x/y])^*[x'/x]$, where $x' \notin FV(t) \cup FV(A[t/y]) \cup \{x\}$, x' substitutable for x in t[x] and in $(C[x/y])^*$. By 7.3.1(b): x=x' and hence: $(C[x/y])^*$. Our conclusion now easily follows.

We get: $n(\eta(A,t,x)) \leq n(\theta(B,t,x)) + n(\eta(C,t,x)) + P^3\{n(A).\max(n(t),n(x))\}$.

The other cases are similar. We find that both $n(\eta(A,t,x))$ and $n(\eta(A,t,x))$ can be estimated by: $P^4\{n(A).\max(n(t),n(x))\}$. □

Now we are in the position to prove (i'),(ii'),(iii),(iv):

7.3.3 Theorem (in $I\Delta_0+\Omega_1$): We can transform each PL-proof π of A into an PL*-proof π^* of A*.

Proof: Consider for example the step moving from $\forall y\, A$ to A[t/y]. This step is transformed into the following reasoning: suppose $\forall y\, A^*$. We show by 7.3.1(a) $\exists x\, t[x]$ and from this $\exists x (t[x] \wedge A^*[x/y])$. Here $x \notin FV(t) \cup FV(A)$ and x is substitutable for y in A*. By 7.3.2 we can conclude: $(A[t/y])^*$. So the length of the transformed step will be $P^4\{n(A).\max(n(t),n(x'))\} + k.n(x)$. We can choose x' such that $n(x') \leq n(A)$. □

Finally we define $(.)^\circ$ as follows:

if F corresponds to f: $(F(x_1,...,x_n,y))^\circ := (f(x_1,...,x_n)=y)$,

if R does not correspond to a function symbol: $(R(x_1,...,x_n))^\circ := R(x_1,...,x_n)$,

$(.)^\circ$ commutes with logical connectives and quantifiers.

7.3.4 Theorem (in $I\Delta_0+\Omega_1$): We can transform each PL*-proof π^* of B into an PL-proof π of B°.

Proof: We can simply follow π^* in $(.)^\circ$-translation. We only have to add at some places the (standard!) proofs of statements of the form $\forall y,...\exists! x\, f(y,...)=x$. So $n(\pi)$ is linear in $n(\pi^*)$. □

7.3.5 Lemma (in $I\Delta_0+\Omega_1$): $PL \vdash (t[x])^\circ[t/x]$.

Proof: The proof is by induction on t. Let's consider a typical step. Say t is of the form f(v,w), where v and w are terms. $(t[x])^\circ[t/x]$ will have the form: $\exists u,z\, (v[u]^\circ \wedge w[z]^\circ \wedge f(u,z)=t)$ (*). Clearly (*) is immediate from: $(v[u])^\circ[v/u] \wedge (w[z])^\circ[w/z] \wedge f(v,w)=t$, i.e. $(v[u])^\circ[v/u] \wedge (w[z])^\circ[w/z] \wedge t=t$. So if we call our proof of $(t[x])^\circ[t/x]$: $\pi\{t,x\}$ we have:

$$n(\pi\{t,x\}) \leq n(\pi\{v,u\})+n(\pi\{w,z\})+k.n(t)+m.n(t[x]).n(t) \leq$$
$$\leq n(\pi\{v,u\})+n(\pi\{w,z\})+a.n^3(t)+b.n^2(t)+(c+m.n(x)).n(t)+d,$$
where n,m,a,b,c,d are standard.

Now assume that $n(\pi\{t,x\})$ has the form $G(n(t))+m.n(x).n(t)$, we find that it is sufficient that:
$$G(n(t)) \leq G(n(v))+G(n(w))+m.n(u).n(v)+m.n(z).n(w)+a.n^3(t)+b.n^2(t)+c.n(t)+d.$$
Note that $n(u)+n(z)\leq n(t)+e$, for certain standard e and that $n(v)+n(w)\leq n(t)$, hence:
$$G(n(t)) \leq G(n(v))+G(n(w))+f.n^3(t)+g.n^2(t)+h.n(t)+i,$$
for suitable standard f,g,h,i. So clearly we may take $G(x):=P^4\{x\}$ □

7.3.6 Theorem (in $I\Delta_0+\Omega_1$): $PL\vdash(A\leftrightarrow A^{*\circ})$.

Proof: Let $\eta(A)$ stand for the proof of $A^{*\circ}$ from A and let $\theta(A)$ stand for the proof of A from $A^{*\circ}$. Let's first consider the atomic case: we have:
$$R(t_1,\ldots,t_n)^{*\circ}=\exists x_1,\ldots,x_n(t_1[x_1]^\circ\wedge\ldots\wedge t_n[x_n]^\circ\wedge R(x_1,\ldots,x_n)).$$
$\eta(R(t_1,\ldots,t_n))$ looks as follows: first we have proofs π_j of $(t_j[x_j])^\circ[t_j/x_j]$ (j=1,...,n). A number of simple steps brings us to: $(t_1[x_1])^\circ[t_1/x_1]\wedge\ldots\wedge(t_n[x_n])^\circ[t_n/x_n]\wedge R(t_1,\ldots,t_n)$ and from there to: $\exists x_1,\ldots,x_n(t_1[x_1]^\circ\wedge\ldots\wedge t_n[x_n]^\circ\wedge R(x_1,\ldots,x_n))$. Note that: $n(x_1)+\ldots+n(x_n)\leq n(t_1)+\ldots+n(t_n)$, $n(\pi_j)\leq G(n(t_j))+m.n(x_j).n(t_j)$, $n((t_j[x_j])^\circ[t_j/x_j])\leq p.(K(n(t_j))+n(x_j)).n(t_j)$ for some standard p. From these observations it is immediate that $n(\eta(R(t_1,\ldots,t_n)))$ can be estimated by $P^4\{n(R(t_1,\ldots,t_n))\}$.

$\theta(R(t_1,\ldots,t_n))$ looks as follows: first we have proofs π_j of $(t_j[x_j])^\circ[t_j/x_j]$ (j=1,...,n). Then we have proofs λ_j from $(t_j[x_j])^\circ[t_j/x_j]$ and $(t_j[x_j])^\circ$ to $x_j=t_j$. Assume $t_1[x_1]^\circ\wedge\ldots\wedge t_n[x_n]^\circ\wedge R(x_1,\ldots,x_n)$, move to $t_1[x_1]^\circ,\ldots,t_n[x_n]^\circ,R(x_1,\ldots,x_n)$ and infer $R(t_1,\ldots,t_n)$. Finally apply the $\exists$-elimination Rule.

Note that $n(\pi_j)\leq P^4\{n(t_j)\}+m.n(x_j).n(t_j)$. $n(\lambda_j)$ is like the proofs 7.3.1(b), but a standard factor longer because of $(.)^\circ$: so it will be $\leq m.P^3\{n(t_j)\}+k.(n(x_j)+n(t_j))$. A moment's reflection will convince the reader that $n(\theta(R(t_1,\ldots,t_n)))$ can be estimated by $P^4\{n(R(t_1,\ldots,t_n))\}$

Consider a typical step: e.g. to $(C\rightarrow D)$. We have: for some standard p,q:
$$n(\eta(C\rightarrow D))\leq n(\theta(C))+n(\eta(D))+p.(n(C)+n(D))+q,$$
$$n(\theta(C\rightarrow D))\leq n(\eta(C))+n(\theta(D))+p.(n(C)+n(D))+q.$$
It follows that we can estimate: $n(\eta(A))\leq P^4\{n(A)\}$, $n(\theta(A))\leq P^4\{n(A)\}$ □

7.3.7 Theorem (in $I\Delta_0+\Omega_1$): $PL^*\vdash(B\leftrightarrow B^{\circ *})$.

Proof: The effect of $(.)^{\circ *}$ is just to replace atomic subformulas of the form $F(x_1,\ldots,x_n,y)$ by subformulas of the form $\exists u_1,\ldots,u_n,u,v(x_1=u_1\wedge\ldots\wedge x_n=u_n\wedge F(u_1,\ldots,u_n,u)\wedge y=v\wedge u=v)$. We have

$n(u_1)+...+n(u_n)+n(v)\leq n(F(x_1,...,x_n,y))+s$ for some standard s. It follows that the proof π of the equivalence of $F(x_1,...,x_n,y)$ and $\exists u_1,...,u_n,u,v(x_1=u_1\wedge...\wedge x_n=u_n\wedge F(u_1,...,u_n,u)\wedge y=v\wedge u=v)$ satisfies: $n(\pi)= P^1\{n(F(x_1,...,x_n,y))$. Let $\eta(B)$ stand for the proof of $B^{\circ *}$ from B and let $\theta(B)$ stand for the proof of B from $B^{\circ *}$, we find e.g. for some standard p,q:

$$n(\eta(C\to D))\leq n(\theta(C))+n(\eta(D))+p.(n(C)+n(D))+q,$$
$$n(\theta(C\to D))\leq n(\eta(C))+n(\theta(D))+p.(n(C)+n(D))+q.$$

It follows that: $n(\eta(B))\leq P^2\{n(B)\}$, $n(\theta(B))\leq P^2\{n(B)\}$. □

Let W be a theory (whose language may contain function symbols) in a language L. W* be the theory in L* axiomatized by PL* plus the *-translations of the non-logical-axioms of W. Evidently W* is Δ_1^b axiomatized. By the above we have:

7.3.8 Theorem: $I\Delta_0+\Omega_1\vdash\forall A\in Sent_N(\Box_W A\leftrightarrow\Box_{W*}A^*)$.

Let U and V be theories in languages L and N. Let K be an interpretation of N* in L. We define:

$K{:}U\rhd_a V \quad :\Leftrightarrow \forall y\in \alpha_{V*} Prov_U(y^K)$.
$K{:}U\rhd_s V \quad :\Leftrightarrow (\forall y\in \alpha_{V*}\exists p)^* Proof_U(p,y^K)$.
$K{:}U\rhd_t V \quad :\Leftrightarrow \forall x\in Sent_N(Prov_V(x)\to Prov_U(x^{*K}))$.

We can view $(.)^\circ$ as an interpretation of L* in L, by taking as its domain $\{x|x=x\}$. If K is an interpretation of N* in L, then K* is the interpretation of N* in L* with $(R(x,...))^{K*}:=((R(x,...))^K)^*$ and $\delta_{K*}(x)=(\delta_K(x))^*$. Similarly, when M is an interpretation of N* in L*, then M° is the interpretation of N* in L with $(R(x,...))^{M^\circ}:=((R(x,...))^M)^\circ$ and $\delta_{M^\circ}(x)=(\delta_M(x))^\circ$.

7.3.9 Theorem: Let K,M be free parameters ranging over interpretations respectively of N* in L and of N* in L*. For every $\xi\in\{a,s,t\}$:

i) $I\Delta_0+\Omega_1\vdash (.)^\circ{:}U\rhd_\xi U$
ii) $I\Delta_0+\Omega_1\vdash K{:}U\rhd_\xi V\leftrightarrow K{:}U\rhd_\xi V^*$.
iii) $I\Delta_0+\Omega_1\vdash K{:}U\rhd_\xi V\leftrightarrow K^*{:}U^*\rhd_\xi V^*$
iv) $I\Delta_0+\Omega_1\vdash M^\circ{:}U\rhd_\xi V\leftrightarrow M{:}U^*\rhd_\xi V^*$

Proof: Note that (i) follows from (iv) and the fact that $ID{:}U^*\rhd_\xi U^*$, where ID is the identity interpretation. We treat (iii) in case ξ=s and leave the other cases and (ii) and (iv) to the reader. Reason in $I\Delta_0+\Omega_1$. "$\to$" Suppose $(\forall x\in \alpha_{V*}\exists p)^* Proof_U(p,x^K)$. Let a be given and let b be the bound for the U-proofs of the x^K. We have to provide a bound c such that $\forall x<a(x\in\alpha_{V*}\to\exists q<c\ Proof_{U*}(q,x^{K*}))$. It is easy to see that $x^{K*}=(x^K)^*$. Moreover as we have seen if p is a U-proof of x^K, then there is a U*-proof q of $(x^K)^*$ with $|q|<P(|p|)$ for some standard polynomial P. So we can take $c:=exp(P(|b|)$.

"$\leftarrow$" Fully analogous. □

References:

Artemov, S.N., 1980, *Aritmeticeski polnyje modal'nyje teorii (Arithmetically complete modal theories)*, Semiotika i informatika 14, 115-113. Translation: AMS Transl. (2), vol 135, 1987, 39-54.

Artemov, 1986, *On Modal Logics axiomatizing Provability*, Math. USSR Izvestia, Vol 27, No.3, 401-429.

Barendregt, H.P., van Eekelen, M.C.J.D., Glauert, J.W.R., Kennaway, J.R., Plasmeijer, M.J., Sleep, M.R., 1986, *Term Graph Rewriting*, Internal Rapport 87, Dept. of Computer Science, University of Nijmegen. (Also Report SYS-C87-01, School of Information Systems, University of East Anglia.)

Bennet, J.H., 1962, *On spectra*, Thesis, Princeton University, Princeton.

Berarducci, A., *The interpretability Logic of Peano Arithmetic*, Manuscript, 1988.

Boolos, G., 1976, *On deciding the truth of certain statements involving the notion of consistency*, JSL 41, 33-35.

Boolos, G., 1979, *The unprovability of consistency*, CUP, London.

Buss, S., 1985, *Bounded Arithmetic*, Thesis, Princeton University, Princeton. Reprinted: 1986, Bibliopolis, Napoli.

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

Gaifman, H. & Dimitracopoulos, C., 1982, *Fragments of Peano's Arithmetic and the MRDP theorem*, in: *Logic and Algorithmic*, Monography 30 de l'Enseignement Mathematique, Genève, 187-206.

Hájek, P., & Montagna, M., 1989, *ILM is the logic of Π_1-conservativity*, manuscript.

Hájek, P., & Svejdar, V., 1989, *A note on the normal form of closed formulas of Interpretability Logic*, manuscript.

Jongh, D.H.J. de & Veltman F., 1990, *Provability logics for relative interpretability*, in Petkov, P.P. (ed.), 1990, *Mathematical Logic*, Plenum Press, New York, 31-42..

Jongh, D.H.J. de & Visser, A., 1989, *Explicit Fixed Points in Interpretability Logic*, Logic Group Preprint Series 44, Department of Philosophy, University of Utrecht.

Kalsbeek, M.B., 1988, *An Orey Sentence for Predicative Arithmetic*, ITLI Prepublication Series X-8-01.

Magari, R., 1975, *The diagonalizable Algebras*, Bull. Unione Mat. Ital. 66-B, 117-125.

Parikh, R., 1971, *Existence and feasibility in arithmetic*, JSL 36, 494-508.

Paris, J.B., Dimitracopoulos, C., 1983, *A note on the undefinability of cuts*, JSL 48, 564-569.

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

Pudlák, P., 1983a, *Some prime elements in the lattice of interpretability types*, Transactions of the AMS 280, 255-275.

Pudlák, P., 1985, *Cuts, consistency statements and interpretability*, JSL 50, 423-441.

Pudlák, P., 1986, *On the length of proofs of finitistic consistency statements in finitistic theories,* in: Paris, J.B. &al, eds., *Logic Colloquium '84,* North Holland, 165-196.

Schwichtenberg, H., 1977, *Proof Theory: Some Applications of Cut-Elimination,* in: J. Barwise (ed.), 1977, *Handbook of Mathematical Logic,* North Holland, 867-895.

Shavrukov, V. Yu., 1988, *The Logic of Relative Interpretability over Peano Arithmetic,* Preprint 5 of the Steklov Mathematical Institute.

Smorynski, C., 1985a, *Self-Reference and Modal Logic,* Springer Verlag.

Svejdar, V., 1983, *Modal analysis of generalized Rosser sentences,* JSL 48, 986-999.

Svejdar, V., 1989, *Some independence results in Interpretability Logic,* manuscript.

Takeuti, G., 1988, *Bounded arithmetic and truth definition,* Annals of Pure & Applied Logic 36, 75-104.

Verbrugge, L.C., 1988, *Does Solovay's Completeness Theorem extend to Bounded Arithmetic?,* Master's Thesis, Department of Mathematics and Computer Science, University of Amsterdam, Plantage Muidergracht 24, 1018TV, Amsterdam.

Verbrugge, L.C., 1988, 1989, *Σ-completeness and Bounded Arithmetic,* ITLI Prepublication Series ML-89-05. Department of Mathematics and Computer Science, University of Amsterdam, Plantage Muidergracht 24, 1018TV, Amsterdam.

Visser, A., 1985, *Evaluation, provably deductive equivalence in Heyting's Arithmetic of substitution instances of propositional formulas,* Logic Group Preprint Series nr 4, Dept. of Philosophy, University of Utrecht, Heidelberglaan 2, 3584CS Utrecht.

Visser, A., 1988, *Preliminary Notes on Interpretability Logic,* Logic Group Preprint Series nr 29, Dept. of Philosophy, University of Utrecht, Heidelberglaan 2, 3584CS Utrecht.

Visser, A, 1990, *Interpretability Logic,* in Petkov, P.P. (ed.), 1990, *Mathematical Logic,* Plenum Press, New York, 175-208.

Visser, A, 1989, *The Formalization of Interpretability,* Logic Group Preprint Series nr 47, Dept. of Philosophy, University of Utrecht, Heidelberglaan 2, 3584CS Utrecht.

Logic Group Preprint Series

Department of Philosophy
University of Utrecht
Heidelberglaan 2
3584 CS Utrecht
The Netherlands

1 C.P.J. Koymans, J.L.M. Vrancken, *Extending Process Algebra with the empty process,* September 1985
2 J.A. Bergstra, *A process creation mechanism in Process Algebra,* September 1985
3 J.A. Bergstra, *Put and get, primitives for synchronous unreliable message passing,* October 1985
4 A. Visser, *Evaluation, provably deductive equivalence in Heyting's arithmetic of substitution instances of propositional formulas,* November 1985
5 G.R. Renardel de Lavalette, *Interpolation in a fragment of intuitionistic propositional logic,* January 1986
6 C.P.J. Koymans, J.C. Mulder, *A modular approach to protocol verification using Process Algebra,* April 1986
7 D. van Dalen, F.J. de Vries, *Intuitionistic free abelian groups,* April 1986
8 F. Voorbraak, *A simplification of the completeness proofs for Guaspari and Solovay's R,* May 1986
9 H.B.M. Jonkers, C.P.J. Koymans & G.R. Renardel de Lavalette, *A semantic framework for the COLD-family of languages,* May 1986
10 G.R. Renardel de Lavalette, *Strictheidsanalyse,* May 1986
11 A. Visser, *Kunnen wij elke machine verslaan? Beschouwingen rondom Lucas' argument,* July 1986
12 E.C.W. Krabbe, *Naess's dichotomy of tenability and relevance,* June 1986
13 H. van Ditmarsch, *Abstractie in wiskunde, expertsystemen en argumentatie,* Augustus 1986
14 A. Visser, *Peano's Smart Children, a provability logical study of systems with built-in consistency* , October 1986
15 G.R. Renardel de Lavalette, *Interpolation in natural fragments of intuitionistic propositional logic,* October 1986
16 J.A. Bergstra, *Module Algebra for relational specifications,* November 1986
17 F.P.J.M. Voorbraak, *Tensed Intuitionistic Logic,* January 1987
18 J.A. Bergstra, J. Tiuryn, *Process Algebra semantics for queues,* January 1987
19 F.J. de Vries, *A functional program for the fast Fourier transform,* March 1987
20 A. Visser, *A course in bimodal provability logic,* May 1987
21 F.P.J.M. Voorbraak, *The logic of actual obligation, an alternative approach to deontic logic,* May 1987
22 E.C.W. Krabbe, *Creative reasoning in formal discussion,* June 1987
23 F.J. de Vries, *A functional program for Gaussian elimination,* September 1987
24 G.R. Renardel de Lavalette, *Interpolation in fragments of intuitionistic propositional logic,* October 1987 (revised version of no. 15)
25 F.J. de Vries, *Applications of constructive logic to sheaf constructions in toposes,* October 1987
26 F.P.J.M. Voorbraak, *Redeneren met onzekerheid in expertsystemen,* November 1987
27 P.H. Rodenburg, D.J. Hoekzema, *Specification of the fast Fourier transform algorithm as a term rewriting system,* December 1987

28 D. van Dalen, *The war of the frogs and the mice, or the crisis of the Mathematische Annalen,* December 1987

29 A. Visser, *Preliminary Notes on Interpretability Logic,* January 1988

30 D.J. Hoekzema, P.H. Rodenburg, *Gauß elimination as a term rewriting system*, January 1988

31 C. Smoryński, *Hilbert's Programme,* January 1988

32 G.R. Renardel de Lavalette, *Modularisation, Parameterisation, Interpolation,* January 1988

33 G.R. Renardel de Lavalette, *Strictness analysis for POLYREC, a language with polymorphic and recursive types*, March 1988

34 A. Visser, *A Descending Hierarchy of Reflection Principles,* April 1988

35 F.P.J.M. Voorbraak, *A computationally efficient approximation of Dempster-Shafer theory*, April 1988

36 C. Smoryński, *Arithmetic Analogues of McAloon's Unique Rosser Sentences,* April 1988

37 P.H. Rodenburg, F.J. van der Linden, *Manufacturing a cartesian closed category with exactly two objects*, May 1988

38 P.H. Rodenburg, J.L.M.Vrancken, *Parallel object-oriented term rewriting : The Booleans*, July 1988

39 D. de Jongh, L. Hendriks, G.R. Renardel de Lavalette, *Computations in fragments of intuitionistic propositional logic*, July 1988

40 A. Visser, *Interpretability Logic*, September 1988

41 M. Doorman, *The existence property in the presence of function symbols,* October 1988

42 F. Voorbraak, *On the justification of Dempster's rule of combination*, December 1988

43 A. Visser, *An inside view of EXP, or: The closed fragment of the provability logic of* $I\Delta_0+\Omega_1$, February 1989

44 D.H.J. de Jongh & A. Visser, *Explicit Fixed Points in Interpretability Logic,* March 1989

45 S. van Denneheuvel & G.R. Renardel de Lavalette, *Normalisation of database expressions involving calculations*, March 1989

46 M.F.J. Drossaers, *A Perceptron Network Theorem Prover for the Propositional Calculus*, July 1989

47 A. Visser, *The Formalization of Interpretability,* August 1989

48 J.L.M. Vrancken, *Parallel Object Oriented Term Rewriting : a first implementation in Pool2*, September 1989

49 G.R. Renardel de Lavalette, *Choice in applicative theories*, September 1989

50 C.P.J. Koymans & G.R. Renardel de Lavalette, *Inductive definitions in COLD-K*, September 1989

51 F. Voorbraak, *Conditionals, probability, and belief revision (preliminary version),* October 1989

52 A. Visser, *On the* Σ_1^0*-Conservativity of* Σ_1^0*-Completeness,* October 1989

53 G.R. Renardel de Lavalette, *Counterexamples in applicative theories with choice*, January 1990

54 D. van Dalen, *L.E.J. Brouwer. Wiskundige en Mysticus*, June 1990

55 F. Voorbraak, *The logic of objective knowledge and rational belief,* September 1990

56 J.L.M. Vrancken, *Reflections on Parallel and Functional Languages*, September 1990

57 A. Visser, *An inside view of EXP, or: The closed fragment of the provability logic of* $I\Delta_0+\Omega_1$, revised version with new appendices, October 1990