THE POLYNOMIAL HIERARCHY AND INTUITIONISTIC BOUNDED ARITHMETIC

Samuel R. Buss
Mathematical Sciences Research Institute
October 1985

Abstract

Intuitionistic theories IS_2^i of Bounded Arithmetic are introduced and it is shown that the definable functions of IS_2^i are precisely the $\square_i^p$ functions of the polynomial hierarchy. This is an extension of earlier work on the classical Bounded Arithmetic and was first conjectured by S. Cook. In contrast to the classical theories of Bounded Arithmetic where Σ_i^b-definable functions are of interest, our results for intuitionistic theories concern all the definable functions.

The method of proof uses $\square_i^p$-realizability which is inspired by the recursive realizability of S.C. Kleene [3] and D. Nelson [5]. It also involves polynomial hierarchy functionals of finite type which are introduced in this paper.

---

* Research supported in part by NSF Grant DMS 85-11465.

Appeared in: Structure in Complexity Theory, (1986) Spr. Ver. LNCS #223

§1. Background and Introduction

We begin by reviewing some of the main results of Buss [1,2]. In [1], very weak theories of arithmetic, called collectively Bounded Arithmetic, are formulated. These theories have the non-logical symbols 0, S, +, $\cdot$, #, $\lfloor \frac{1}{2}x \rfloor$, $|x|$ and $\leq$, where

$$|x| = \lceil \log_2(x+1) \rceil, \text{ the length of the binary representation of } x,$$

$$\lfloor \tfrac{1}{2}x \rfloor = x \text{ divided by two, rounded down,}$$

$$x\#y = 2^{|x| \cdot |y|}$$

and the rest of the symbols have their usual meanings; namely, zero, successor, plus, times and "less than or equal to". The syntax of first order logic is enlarged to include bounded quantifiers of the forms $(\forall x \leq t)$ and $(\exists x \leq t)$ where t is an arbitrary term not containing x. Bounded quantifiers of the form $(\forall x \leq |t|)$ or $(\exists x \leq |t|)$ are called sharply bounded quantifiers. The usual quantifiers are called unbounded quantifiers.

A formula is bounded if and only if all of its quantifiers are bounded. The bounded formulae are classified into a hierarchy Σ_i^b and Π_i^b by counting alternations of bounded quantifiers, ignoring sharply bounded quantifiers. This is analogous to the definition of the arithmetic hierarchy where one counts the alternation of unbounded quantifiers ignoring bounded quantifers.

The Σ_i^b-PIND axioms are the formulae

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

where A is a Σ_i^b-formula. The first order theory S_2^i is defined to have the language above and to be axiomatized by the Σ_i^b-PIND axioms and an additional, finite set of open axioms [1]. We say that S_2^i can Σ_i^b-define a function $f: \mathbb{N}^k \longrightarrow \mathbb{N}$ if and only if there exists a Σ_i^b-formula $A(\vec{x},y)$ such that

(1) $S_2^i \vdash (\forall \vec{x})(\exists! y)A(\vec{x},y)$, and

(2) For all $\vec{n}$, $\mathbb{N} \models A(\vec{n},f(\vec{n}))$.

In [1] it is shown that S_2^i can Σ_i^b-define precisely the $\square_i^p$-functions (for $i \geq 1$). The $\square_i^p$-functions are the functions at the i-th level of the polynomial hierarchy [1]. In particular, $\square_1^p$ is the set P of functions computable in polynomial time. (We differ from the usual convention that P is the set of polynomial time recognizable predicates; for us, P also denotes the set of functions which are computable by a polynomial time transducer.) In general, $\square_i^p$ is $P^{\Sigma_{i-1}^p}$.

The theories S_2^i are most advantageously viewed as Gentzen-style natural deduction systems. A formal proof in a natural deduction system contains <u>sequents</u> of the form

$$A_1,\ldots,A_\ell \longrightarrow B_1,\ldots,B_r$$

where each A_j and B_j is a formula. The meaning of such a sequent is

$$A_1 \wedge \ldots \wedge A_\ell \supset B_1 \vee \ldots \vee B_r.$$

In addition to the usual inference rules for natural deduction, the Σ_i^b-PIND inference is

$$\frac{\Gamma, A(\lfloor \tfrac{1}{2} b \rfloor) \longrightarrow A(b), \Delta}{\Gamma, A(0) \longrightarrow A(t), \Delta}$$

where A is a Σ_i^b-formula, Γ and Δ represent sequences of formulae separated by commas, t is any term and the free variable b occurs only as indicated.

The <u>intuitionistic</u> natural deduction system is defined to be the usual natural deduction system with the additional restriction that at most one formula may appear in the antecedent of a sequent (i.e., after the $\longrightarrow$). In other words, only sequents of the form

$$A_1,\ldots,A_\ell \longrightarrow B$$

or

$$A_1,\ldots,A_\ell \longrightarrow$$

may appear in an intuitionistic natural deduction proof. (See Takeuti [6] for more details.)

Definition. A formula A is <u>hereditarily</u> Σ_i^b if and only if every subformula of A is a Σ_i^b-formula. The set of all hereditarily Σ_i^b formulae is denoted $H\Sigma_i^b$.

Since any formula is a subformula of itself, every hereditarily Σ_i^b formula is a Σ_i^b-formula.

The $H\Sigma_i^b$-PIND axiom and the $H\Sigma_i^b$-PIND inference rule are defined in the obvious way. It is easy to see that the $H\Sigma_i^b$-PIND axiom is intuitionistically equivalent to the $H\Sigma_i^b$-PIND inference rule: this is proved by the method of proof of Theorem 4.2 of [1].

Definition. Suppose $i \geqslant 0$. Then IS_2^i is an intuitionistic theory of Bounded Arithmetic formalized by a Gentzen-style intuitionistic sequent calculus. The language of IS_2^i is the same as the language of S_2^i. The axioms of IS_2^i are the S_2^i-provable sequents

$$A_1,\ldots,A_\ell \longrightarrow B$$

such that $A_1,\ldots,A_\ell$ and B are hereditarily Σ_i^b formulae. In addition, IS_2^i admits the $H\Sigma_i^b$-PIND inference.

Of course, it is unimportant that IS_2^i is formalized as a Gentzen sequent calculus instead of as a Hilbert-style system. We prefer the Gentzen formulation for the proof-theoretic arguments presented below.

Note that IS_2^i satisfies a restricted version of the law of excluded middle. Namely, if $A \in \Sigma_{i-1}^b \cup \Pi_{i-1}^b$, or more generally, if both A and $\neg A$ are hereditarily Σ_i^b, then

IS_2^i proves

$$\neg\neg A \longrightarrow A$$

and

$$\longrightarrow A \vee \neg A.$$

Let i be a fixed positive integer for the remainder of this paper.

Definition. ($i \geq 1$). A formula $(\exists y)A(\vec{c},y)$ is $\square_i^p$-fulfillable if and only if there is a $\square_i^p$-function f such that for all $\vec{n} \in \mathbb{N}^k$, $A(\vec{n},f(\vec{n}))$ is valid.

The main result of this paper is

Theorem 2. ($i \geq 1$). If A is any formula and $IS_2^i \vdash (\exists y)A$ then $(\exists y)A$ is $\square_i^p$-fulfillable.

In particular, if $IS_2^1 \vdash (\forall \vec{x})(\exists y)A(\vec{x},y)$ then there is a polynomial-time computable function f: $\mathbb{N}^k \longrightarrow \mathbb{N}$ so that for all $\vec{n} \in \mathbb{N}^k$, $A(\vec{n},f(\vec{n}))$ is true.

It is an immediate corollary of Theorem 2 and of the results in [1] that the definable functions of IS_2^i are precisely the $\square_i^p$ functions. The definition of a function f being definable in IS_2^i is that there is an arbitrary formula $A(\vec{x},y)$ so that $A(\vec{n},f(\vec{n}))$ is true for all values of $\vec{n}$ and such that IS_2^i proves $(\forall \vec{x})(\exists! y)A(\vec{x},y)$.

It is instructive to compare Theorem 2 with what is known for S_2^i. By Theorem 5.1 of [1], if A is a Σ_i^b-formula and $S_2^i \vdash (\exists y)A$ then $(\exists y)A$ is $\square_i^p$-fulfillable. Theorem 2 is similar but concerns the theory IS_2^i and allows A to be an arbitrary formula.

Theorem 2 was first conjectured by Stephen Cook after hearing some of the results of this author's dissertation. The proof presented here is based on this author's original method of proof of Theorem 5.5 of [1], the main theorem of his dissertation. However, this original proof was never published since this author found a simpler proof and used it in [1].

§2. Eliminating Implication

The logical symbols used for the construction of formulae in a Gentzen natural deduction system are $\wedge$, $\vee$, $\neg$, $\supset$, $\forall$ and $\exists$. In order to simplify our definitions and proofs in this article, we wish to omit the implication symbol, $\supset$, from the language. In a classical theory this can be trivially done; however, in an intuitionistic theory this is more difficult. In fact, it can be shown that there is no formula ϕ which does not contain $\supset$ such that both

$$(p \supset q) \supset \phi$$

and

$$\phi \supset (p \supset q)$$

are intuitionistically provable [4]. But for our purposes, it will suffice to prove Proposition 1 and 2.

Proposition 1. Let A be any formula which may include the logical implication symbol, $\supset$. Then there are formulae A_R and A_L such that

(a) A_R and A_L do not involve $\supset$,

(b) A_R and A_L are classically equivalent to A,

(c) $A_L \supset A$ and $A \supset A_R$ are intuitionistically provable.

Proof. By induction on the complexity of A: if A is atomic then define A_R and A_L to be A itself. Otherwise define

(1) $(\neg B)_R = \neg(B_L)$, $(\neg B)_L = \neg(B_R)$

(2) $(B \wedge C)_R = B_R \wedge C_R$, $(B \wedge C)_L = B_L \wedge C_L$

(3) $(B\vee C)_R = B_R\vee C_R$, $\qquad (B\vee C)_L = B_L\vee C_L$

(4) $(B\supset C)_R = \neg(B_L\wedge\neg C_R)$, $\qquad (B\supset C)_L = \neg B_R\vee C_L$

(5) $((\forall x)B)_R = (\forall x)(B_R)$, $\qquad ((\forall x)B)_L = (\forall x)(B_L)$

(6) $((\exists x)B)_R = (\exists x)(B_R)$, $\qquad ((\exists x)B)_L = (\exists x)(B_L)$

(7) $((\forall x\leqslant t)B)_R = (\forall x\leqslant t)(B_R)$, $\qquad ((\forall x\leqslant t)B)_L = (\forall x\leqslant t)(B_L)$

(8) $((\exists x\leqslant t)B)_R = (\exists x\leqslant t)(B_R)$, $\qquad ((\exists x\leqslant t)B)_L = (\exists x\leqslant t)(B_L)$.

It is now easy to prove Proposition 1. For example, to prove that $(B\supset C)_L$ is correctly defined, suppose $B\supset B_R$ and $C_L\supset C$ are intuitionistically provable. Then consider the following intuitionistic proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{B\longrightarrow B_R}{\neg B_R, B\longrightarrow}}{\neg B_R, B\longrightarrow C} \qquad \dfrac{C_L\longrightarrow C}{C_L, B\longrightarrow C}}{\neg B_R\vee C_L, B\longrightarrow C}}{\neg B_R\vee C_L\longrightarrow B\supset C} \quad .$$

Thus $(\neg B_R\vee C_L)\supset(B\supset C)$ is intuitionistically provable. We leave the other cases to the reader. ■

Proposition 2. Let A be any hereditarily Σ_i^b formula. Then there is a hereditarily Σ_i^b formula B so that

(a) The implication symbol, $\supset$, does not appear in B.

(b) IS_2^i proves $A\supset B$ and $B\supset A$.

Proof. Just take B to be A_L as defined in the proof of Proposition 1. ■

It is now clear how we may eliminate the implication symbol, $\supset$, from the Gentzen natural deduction system. Suppose for instance that IS_2^i proves $(\forall x)A$. By Proposition 1 there is an IS_2^i proof of $(\exists x)A_R$, and by Proposition 2 it may be assumed without loss of generality that the implication symbol, $\supset$, does not appear in any principal formula of an induction inference. Furthermore, without loss of generality we can require that no axiom (initial sequent) involves $\supset$; for example, the axiom $A\supset B \longrightarrow \neg A\vee B$ can be derived by

$$\begin{array}{c} \dfrac{\dfrac{\neg A \longrightarrow \neg A}{\neg A \longrightarrow \neg A\vee B}}{\neg A\,,\, A\supset B \longrightarrow \neg A\vee B} \qquad \dfrac{\dfrac{A \longrightarrow A \qquad B \longrightarrow B}{A\,,\, A\supset B \longrightarrow B}}{A\,,\, A\supset B \longrightarrow \neg A\vee B} \\ \neg A\vee A\,,\, A\supset B \longrightarrow \neg A\vee B \\ \hline A\supset B \longrightarrow \neg A\vee B \end{array}$$

where the last inference is a cut against the sequent $\longrightarrow \neg A\vee A$ (not shown) which is an axiom since $A\supset B$ is hereditarily Σ_i^b, hence $A \in \Sigma_i^b \cap \Pi_i^b$ and $\neg A\vee A$ is hereditarily Σ_i^b.

Thus the implication symbol, $\supset$, does not appear in the axioms, the induction inferences or the conclusion of the proof; so by cut elimination (Theorem 4.3 of [1]) there is an IS_2^i proof of $(\exists x)A_R$ in which the implication symbol does not appear at all. Since A and A_R are classically equivalent, it is clear that $(\exists x)A_R$ is $\square_i^p$-fulfillable if and only if $(\exists x)A$ is. Hence it will suffice to prove Theorem 2 under the assumption that the implication symbol, $\supset$, is not in the first order language at all.

Accordingly, we shall prove Theorem 2 under the assumption that formulae do not involve the implication symbol, $\supset$.

§3. Polynomial-hierarchy Functionals

In this section a theory of polynomial-hierarchy functionals is developed. The principal difference between the theory of polynomial-hierarchy functionals and the classical (recursive) functionals is that the computational complexity of functions and functionals is restricted. For the rest of this section i will be a fixed positive integer. We define below p-types, $\square_i^p$-functionals, and extended $\square_i^p$-functionals.

Definition. A <u>suitable</u> polynomial is a polynomial in one variable with non-negative integer coefficients. If q and s are suitable polynomials, then $q \circ s$, $q \cdot s$ and $q+s$ denote their composition, product and sum, respectively.

Definition. The p-types are defined inductively by

(1) o is a p-type.

(2) If $\tau_1, \ldots, \tau_k$ are p-types, then $\langle \tau_1, \ldots, \tau_k \rangle$ a is p-type.

(3) If τ and σ are p-types and r is a suitable polynomial, then $\tau \xrightarrow{r} \sigma$ is a p-type.

Intuitively, $\tau \xrightarrow{r} \sigma$ is the class of all functions with domain τ, range σ and computational complexity bounded by r. When $k \in \mathbb{N}$ we write o^k to denote $o, \ldots, o$ with k repetitions: so $\langle o^k \rangle$ is a p-type.

We shall assume that some Gödel coding has been defined for p-types. The precise details of the Gödel coding are not important as long as it is efficient and straightforward; in particular, we assume that polynomial algorithms exist to manipulate the Gödel numbers of p-types. We shall not distinguish notationally between a p-type and its Gödel number; it should always be clear from the context which is meant.

We also need to assign Gödel numbers to Turing machines. Again, this can be done in a number of ways, and must be done so that polynomial time algorithms can be used to manipulate the Gödel numbers. Turing machines will be assumed to have one read-only input tape, an output tape, and one or more work tapes. In addition, a Turing machine has an oracle which is accessed via a query tape and a query state, an accepting state and a rejecting state; except for this oracle the Turing machine is deterministic.

Definition. Let Ω_i be a canonical Σ^p_{i-1}-complete predicate. So Ω_2 could be SAT and Ω_1 the empty set. Let m be the Gödel number of a Turing machine M_m. Then ϕ^i_m is the unary function which is computed by the Turing machine M_m with Ω_i as its oracle.

Note ϕ^i_m may be a partial function. When m is not a valid Gödel number, let ϕ^i_m be the constant zero function.

We shall frequently write just ϕ_m instead of ϕ^i_m since i is a fixed positive integer for the rest of this article.

__Definition.__ Let m be a Gödel number of a Turing machine. The __runtime__ of $\phi^i_m(z)$ is equal to the number of steps the Turing machine M_m uses with oracle Ω_i on input z. Let $|z|$ denote the length of the binary representation of z, so $|z| = \lceil \log_2(z+1) \rceil$. If r is a suitable polynomial, then the __runtime of__ $\phi^i_m(z)$ __is bounded by__ r if and only if the runtime of $\phi^i_m(z)$ is less than or equal to $r(|z|)$.

__Definition.__ A (Gödel number of a) $\square^p_i$-__functional__ of p-type π is an ordered pair $\langle\pi,m\rangle$ so that π is the Gödel number of a p-type and $m \in \mathbb{N}$ and so that the following inductive definition is satisfied:

(1) If $\pi = o$ then m may be any natural number.

(2) If $\pi = \langle\tau_1,\dots,\tau_k\rangle$ then m must be a k-tuple $\langle m_1,\dots,m_k\rangle$ where $\langle\tau_j,m_j\rangle$ is a $\square^p_i$-functional for $1 \leq j \leq k$.

(3) If $\pi = \tau \xrightarrow{r} \sigma$ then m must be a Gödel number of a Turing machine M_m so that for every (Gödel number of a) $\square^p_i$-functional z of p-type τ the runtime of $\phi^i_m(z)$ is bounded by r and the value of $\phi^i_m(z)$ is (the Gödel number of) a $\square^p_i$-functional of p-type σ.

__Definition.__ A unary function f is a $\square^p_i$-functional of p-type τ if and only if there exists $m \in \mathbb{N}$ so that $f(x)=\phi^i_m(x)$ for all $x \in \mathbb{N}$ and $\langle\tau,m\rangle$ is a $\square^p_i$-functional.

As an example, consider the function f defined so that

$$f(x) = \begin{cases} \phi_m(n) & \text{if } x = \langle\langle o \xrightarrow{r} \tau, o\rangle, \langle m,n\rangle\rangle \\ & \quad \text{and the runtime of } \phi_m(n) \text{ is } \leqslant r(|n|). \\ 0 & \text{otherwise} \end{cases}$$

Then for any suitable polynomial r and p-type τ, there is a suitable polynomial s, say $s=1000(r^2+1)$, so that f is a $\square_i^p$-functional of p-type $\langle o \xrightarrow{r} \tau, o\rangle \xrightarrow{s} r$. Furthermore, for any p-type π which is not of the form $\pi = \langle o \xrightarrow{r} \tau, o\rangle$, there is a polynomial s, say $s(n) = 1000(n+1)$, so that f is a $\square_i^p$-functional of p-type $\pi \xrightarrow{s} o$. Note, however, that f is not even a $\square_i^p$-function as its runtime is not bounded by a polynomial uniformly for all p-types of inputs.

Definition. Let τ be a p-type. The runtime of τ, $runtime(\tau)$, is defined inductively by:

(a) $runtime(o) = 0$

(b) $runtime(\langle\tau_1,\ldots,\tau_k\rangle) = \sum_{j=1}^{k} runtime(\tau_j)$

(c) $runtime(\tau_1 \xrightarrow{r} \tau_2) = r + runtime(\tau_2)$.

Note that the runtime of τ is always a suitable polynomial.

Definition. The function ϕ_m^i is an extended $\square_i^p$-functional if and only if there is a suitable polynomial p so that for every p-type τ there exists a p-type σ such that

(a) $runtime(\sigma) \leqslant p \circ runtime(\tau)$, and

(b) $\langle\tau \xrightarrow{s} \sigma, m\rangle$ is a $\square_i^p$-functional where $s = p \circ runtime(\tau)$.

The polynomial p bounds the runtime of the extended $\square_i^p$-functional ϕ_m^i.

Our example above of a function f which was a $\square_i^p$-functional was in fact an example of an extended $\square_i^p$-functional. That example illustrated what is perhaps the single most important property of extended $\square_i^p$-functionals, so we restate it in Proposition 3.

__Proposition__ __3.__ ($i \geq 1$).

(a) If ϕ_m^i and ϕ_n^i are extended $\square_i^p$-functionals then their composition $\phi_m^i \circ \phi_n^i$ is an extended $\square_i^p$-functional.

(b) Let f be the function defined by

$$f(x) = \begin{cases} \phi_m^i(n) & \text{if } x = \langle\langle \tau \xrightarrow{r} \sigma, \tau \rangle, \langle m,n \rangle\rangle \\ & \quad \text{and } \phi_m^i(n) \text{ has runtime} \leq r(|n|) \\ 0 & \text{otherwise.} \end{cases}$$

Then f is an extended $\square_i^p$-functional.

Proof.

(a) Let p_m and p_n bound the runtimes of ϕ_m and ϕ_n. Let τ be any p-type. Then there exists a p-type σ_1 so that $\langle \tau \xrightarrow{r} \sigma_1, n \rangle$ is a $\square_i^p$-functional where $r = p_n \circ \text{runtime}(\tau)$. There also exists a p-type σ_2 so that $\langle \sigma_1 \xrightarrow{s} \sigma_2, m \rangle$ is a $\square_i^p$-functional where $s = p_m \circ \text{runtime}(\sigma_1)$. Furthermore, the runtime of σ_1 is $\leq p_n \circ \text{runtime}(\tau)$ and the runtime of σ_2 is $\leq p_m \circ \text{runtime}(\sigma_1)$; hence the runtime of σ_2 is $\leq p_m \circ p_n \circ \text{runtime}(\tau)$.

Consider a Turing machine M which computes $\phi_m \circ \phi_n$ in the straightforward manner and let k be the Gödel number of M, so $\phi_k = \phi_m \circ \phi_n$. The runtime of ϕ_k is bounded by q(r,s) for some fixed polynomial q. Now let p be $q(p_n, p_m \circ p_n)$.

We claim that ϕ_k is an extended $\square_i^p$-functional with runtime bounded by p. This is immediate from the definition of p and the fact that $p(z) \geq p_m \circ p_n(z)$ for all $z \in \mathbb{N}$.

Part (b) is also easy to prove and we omit the details here (see the example above). ■

We need one further definition which allows a notational convenience for handling vectors of functionals and numbers.

__Definition.__ If $\vec{x}$ is a vector of $\square_i^p$-functionals and $n_1,\ldots,n_k$ are non-negative integers, then $\langle\vec{x};\vec{n}\rangle$ denotes the $\square_i^p$-functional

$$\langle\vec{x},\langle o,n_1\rangle,\ldots,\langle o,n_k\rangle\rangle.$$

__§4. Realization of a Formula__

In this section, we define what it means to $\square_i^p$-realize a formula and prove some basic properties. We begin by reviewing a definition in §5.1 of Buss [1].

Suppose $A(\vec{c})$ is a Σ_i^b-formula where $\vec{c}$ is a k-tuple containing all of the free variables in A. A formula $Witness_A^{i,\vec{c}}$ is defined in [1] with k+1 free variables; the intended meaning of $Witness_A^{i,\vec{c}}(w,\vec{c})$ is that w codes a "witness" to, or a "proof" of, the truth of $A(\vec{c})$. Indeed, the following conditions hold:

(1) $Witness_A^{i,\vec{c}}(w,\vec{c})$ is a Δ_i^p-predicate.

(2) $Witness_A^{i,\vec{c}}(w,\vec{c})$ is defined by a Δ_i^b-formula in the theory of S_2^i.

(3) There is a term t_A so that S_2^i proves

$$A(\vec{c}) \longleftrightarrow (\exists w \leq t_A(\vec{c}))Witness_A^{i,\vec{c}}(w,\vec{c}).$$

Intuitively, $\mathit{Witness}_A^{i,\vec{c}}(w,\vec{c})$ holds if and only if w codes values for the existentially quantified variables of A which make $A(\vec{c})$ true. The reader should refer to [1] for the definition of $\mathit{Witness}_A^{i,\vec{c}}$ if he wishes to fully understand the proofs of Propositions 4, 5 and 6 below.

Definition. Let $x \in \mathbb{N}$ and A be an arbitrary formula. Then x $\square_i^p$-realizes A is defined by the following inductive definition:

Case (1): If $A = A(\vec{c})$ has free variables $c_1,\ldots,c_k$ where $k \neq 0$, then x must equal $\langle\tau,m\rangle$, the Gödel number of a $\square_i^p$-functional of p-type $\tau = \langle o^k \rangle \xrightarrow{r} \sigma$, and for all $\vec{n} \in \mathbb{N}^k$, $\phi_m(\langle;\vec{n}\rangle)$ must $\square_i^p$-realize $A(\vec{n})$.

Case (2): If A has no free variables, then:

Case (2a): If A is hereditarily Σ_i^b, $\mathbb{N} \models \mathit{Witness}_A^i(m)$ and x is $\langle o,m\rangle$ then x $\square_i^p$-realizes A.

Case (2b): If $A = (\forall x)B(x)$ and if x $\square_i^p$-realizes B(c) where c is a new free variable, then x $\square_i^p$-realizes A.

Case (2c): If $A = B \wedge C$ and $\langle\tau_1,m_1\rangle$ and $\langle\tau_2,m_2\rangle$ $\square_i^p$-realize B and C, respectively, and if $x = \langle\langle\tau_1,\tau_2\rangle,\langle m_1,m_2\rangle\rangle$, then x $\square_i^p$-realizes A.

Case (2d): If $A = B \vee C$, x is $\langle\langle o,\tau_1,\tau_2\rangle,\langle m_0,m_1,m_2\rangle\rangle$ and either

(i) $m_0 = 0$ and $\langle\tau_1,m_1\rangle$ $\square_i^p$-realizes B, or

(ii) $m_0 \neq 0$ and $\langle\tau_2,m_2\rangle$ $\square_i^p$-realizes C

then x $\square_i^p$-realizes A.

Case (2e): If $A = (\exists x)B(x)$, x is $\langle\langle o,\tau\rangle,\langle m_1,m_2\rangle\rangle$ and $\langle\tau,m_2\rangle$ $\square_i^p$-realizes $B(m_1)$ then x $\square_i^p$-realizes A.

Case (2f): If $A = (\forall x\leq t)B(x)$ and x $\square_i^p$-realizes $(\forall x)(\neg x\leq t\vee B(x))$ then x $\square_i^p$-realizes A.

Case (2g): If $A = (\exists x\leq t)B(x)$ and x $\square_i^p$-realizes $(\exists x)(x\leq t\wedge B(x))$ then x $\square_i^p$-realizes A.

Case (2h): If $A = \neg B$ and B is not $\square_i^p$-realizable then any $x = \langle o,m\rangle$ $\square_i^p$-realizes A.

Note that whenever x $\square_i^p$-realizes a formula A, x is a $\square_i^p$-functional. However, the p-type of x is not uniquely determined by A. For example, if B is hereditarily Σ_i^b and $A = (\exists x\leq t)B(x)$ is a closed, true formula then there are $\square_i^p$-functionals of p-types o and $\langle o,o\rangle$ which $\square_i^p$-realize A. Namely, if $\mathit{Witness}_A^i(m)$ then $\langle o,m\rangle$ $\square_i^p$-realizes A, and if $\mathit{Witness}_{B(c)}^{i,c}(m_2,m_1)$ and $m_1\leq t$ then $\langle\langle o,o\rangle,\langle m_1,\langle 0,m_2\rangle\rangle\rangle$ $\square_i^p$-realizes A.

Definition. A formula A is $\square_i^p$-realizable if and only if there exists an $x\in\mathbb{N}$ which $\square_i^p$-realizes A.

Following the reasoning of Kleene [3], it is easy to see that it is possible for a formula to be (classically) true and yet not $\square_i^p$-realizable; conversely, a formula may be $\square_i^p$-realizable but (classically) false.

The next proposition is a simple consequence of the definition of $\mathit{Witness}_A^{i,\vec{c}}$ and is readily proved by the methods of §5.1 of [1].

Proposition 4. Let $A(\vec{c})$ be a formula in $\Sigma_i^b\cap\Pi_i^b$. Then there is a $\square_i^p$-function g such that

$$\mathbb{N} \models (\forall \vec{c})[A(\vec{c}) \supset \mathit{Witness}_A^{i,\vec{c}}(g(\vec{c}),\vec{c})].$$

In spite of our remarks above about the independence of truth and $\square_i^p$-realizability, the next proposition shows that these notions are equivalent for hereditarily Σ_i^b sentences.

Proposition 5. Let A be a closed, hereditarily Σ_i^b formula. Then A is $\square_i^p$-realizable if and only if A is true.

Proof.

$\Leftarrow$ Suppose A is true. Since A is closed and Σ_1^b, there is a number w such that $\mathit{Witness}_A^i(w)$. Hence $\langle o,w\rangle$ $\square_i^p$-realizes A.

$\Rightarrow$ For the converse direction we argue by induction on the complexity of A. The argument splits into cases depending on the outermost logical connective of A and the p-type of the $\square_i^p$-functional which $\square_i^p$-realizes A.

Case (1): A is $\square_i^p$-realized by $\langle o,m\rangle$. There are two possibilities. The first is that $\mathit{Witness}_A^i(m)$ and hence A is true. The second is that A = $\neg$B and B is not $\square_i^p$-realizable. But then B must be false by the first half of this proposition. So, again, A is true.

Case (2): Suppose A is $(\exists x\leqslant t)B(x)$ and $\langle\langle o,\tau\rangle,\langle m_1,m_2\rangle\rangle$ $\square_i^p$-realizes A. Then $\langle\tau,m_2\rangle$ $\square_i^p$-realizes $m_1\leqslant t\wedge B(m_1)$. So by the induction hypothesis $m_1\leqslant t\wedge B(m_1)$ is true. Hence A is true.

<u>Case (3):</u> Suppose A is $(\forall x \leq t)B(x)$ and $\langle o \xrightarrow{r} \tau, m\rangle$ $\square_i^p$-realizes A. For all $n \in \mathbb{N}$, $\phi_m(n)$ $\square_i^p$-realizes $\neg n \leq t \vee B(n)$ and by the induction hypothesis, $\neg n \leq t \vee B(n)$ is true for all $n \in \mathbb{N}$. Hence A is true.

The rest of the cases are also easy and are left to the reader. ∎

It is an immediate consequence of Proposition 5 that whenever a hereditarily Σ_i^b formula $A(\vec{c})$ is $\square_i^p$-realizable then it is true for all values of $\vec{c}$. Thus it is not unreasonable to expect that there is an effective procedure which given an $x \in \mathbb{N}$ which $\square_i^p$-realizes $A(\vec{n})$ produces a $w \in \mathbb{N}$ so that $\mathit{Witness}_A^{i,\vec{c}}(w,\vec{n})$. This is stated more fully as Proposition 6.

<u>Proposition 6.</u> Let $A(\vec{c})$ be a hereditarily Σ_i^b formula where $c_1,\ldots,c_k$ are the only free variables in A. Then there is an extended $\square_i^p$-functional f_A so that whenever $\vec{n} \in \mathbb{N}^k$ and x $\square_i^p$-realizes $A(\vec{n})$ then $f_A(\langle x;\vec{n}\rangle)$ is (the Gödel number of) a $\square_i^p$-functional of p-type o which $\square_i^p$-realizes $A(\vec{n})$, and moreover, $f_A(\langle x;\vec{n}\rangle)$ is of the form $\langle o,m\rangle$ where $\mathbb{N} \models \mathit{Witness}_A^{i,\vec{c}}(m,\vec{n})$.

Note that it follows from Proposition 5.3 of §5.1 of [1] that there is a term t_A in the language of S_2 such that we can assume without loss of generality that $f_A(\langle x;\vec{n}\rangle) \leq t_A(\vec{n})$ for all x and $\vec{n}$.

Proof. The proof is by induction on the complexity of A, so assume that if B and C are formulae less complex than A then f_B and f_C are extended $\square_i^p$-functionals satisfying the conditions of Proposition 6.

The input to f_A is the Gödel number of a $\square_i^p$-functional. We define f_A so that

$$f_A(y) = \begin{cases} x & \text{if } y = \langle\langle o,x\rangle;\vec{n}\rangle \text{ where } \mathbb{N}\models Witness_A^{i,\vec{c}}(x,\vec{n}) \\ g_A(\tau,j,\vec{n}) & \text{if } y = \langle\langle \tau,j\rangle;\vec{n}\rangle \text{ and the above condition fails} \\ 0 & \text{otherwise} \end{cases}$$

where g_A is defined below. The definition of g_A is by cases depending on the outermost logical connective of A.

<u>Case (1):</u> Suppose $A \in \Sigma_i^b \cap \Pi_i^b$. By Proposition 4 there is a $\square_i^p$-function g so that

$$\mathbb{N} \models (\forall\vec{c})[A(\vec{c}) \supset Witness_A^{i,\vec{c}}(g(\vec{c}),\vec{c})].$$

So define $g_A(\tau,j,\vec{n}) = \langle o,g(\vec{n})\rangle$. Now by Proposition 5, if $\langle\tau,j\rangle$ $\square_i^p$-realizes $A(\vec{n})$, then $A(\vec{n})$ is true and thus $Witness_A^{i,\vec{c}}(g(\vec{n}),\vec{n})$.

<u>Case (2):</u> Suppose A is $\neg$B. Since A is hereditarily Σ_i^b, $A \in \Sigma_i^b \cap \Pi_i^b$. Hence Case (1) applies.

<u>Case (3):</u> Suppose $A(\vec{c}) = (\exists x{\le}t(\vec{c}))B(x,\vec{c})$. Then the p-type τ must be of the form $\langle o,\sigma\rangle$; otherwise $\langle\tau,j\rangle$ can not possibly $\square_i^p$-realize $A(\vec{n})$. Furthermore, we must have $j = \langle j_1,j_2\rangle$ so that $\langle\sigma,j_2\rangle$ $\square_i^p$-realizes $j_1{\le}t(\vec{n})\wedge B(j_1,\vec{n})$. Let $C(c_0,\vec{c})$ be the formula $c_0{\le}t(\vec{c})\wedge B(c_0,\vec{c})$ and define g_A by

$$g_A(\tau,j,\vec{n}) = \begin{cases} \langle o,\langle j_1,\beta(2,z)\rangle\rangle & \text{if } \tau = \langle o,\sigma\rangle,\ j = \langle j_1,j_2\rangle \\ & \qquad \text{and } f_C(\langle\langle\sigma,j_2\rangle;j_1,\vec{n}\rangle) = \langle o,z\rangle \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\beta(2,z)$ is the Gödel beta function and whenever $Witness_{D\wedge E}^{i}(z)$ then

$Witness^i_E(\beta(2,z))$. It is apparent from the definition of $Witness^i_A$ and the induction hypothesis that the definition of g_A makes f_A satisfy Proposition 6.

Case (4): Suppose $A(\vec{c}) = B(\vec{c}) \vee C(\vec{c})$. In order for $\langle\tau,j\rangle$ to $\square^p_i$-realize $A(\vec{n})$ we must have $\tau = \langle o,\tau_1,\tau_2\rangle$ and either $\langle\tau_1,\beta(2,j)\rangle$ $\square^p_i$-realizes $B(\vec{n})$ or $\langle\tau_2,\beta(3,j)\rangle$ $\square^p_i$-realizes $C(\vec{n})$. Accordingly, we define g_A so that

$$g_A(\tau,j,\vec{n}) = \begin{cases} \langle o,\langle z_B,0\rangle\rangle & \text{if } \tau = \langle o,\tau_1,\tau_2\rangle,\ \beta(1,j) = 0, \\ & \quad \text{and } f_B(\langle\langle\tau_1,\beta(2,j)\rangle;\vec{n}\rangle) = \langle o,z_B\rangle \\ \langle o,\langle 0,z_C\rangle\rangle & \text{if } \tau = \langle o,\tau_1,\tau_2\rangle,\ \beta(1,j) \neq 0, \\ & \quad \text{and } f_C(\langle\langle\tau_2,\beta(3,j)\rangle;\vec{n}\rangle) = \langle o,z_C\rangle \\ 0 & \text{otherwise.} \end{cases}$$

Case (5): The case where $A = B \wedge C$ is similar to Case (4) and is left to the reader.

Case (6): Suppose $A(\vec{c}) = (\forall x \leq |t(\vec{c})|)B(x,\vec{c})$. Let $C(c_0,\vec{c})$ be the formula $c_0 \leq |t(\vec{c})| \wedge B(c_0,\vec{c})$. In order for $\langle\tau,j\rangle$ to $\square^p_i$-realize $A(\vec{n})$ τ must be of the form $o \xrightarrow{r} \sigma$ and for all $n_0 \in \mathbb{N}$ $f_j(\langle o;n_0\rangle)$ $\square^p_i$-realizes $C(n_0,\vec{n})$.

Define g_A so that if τ is $o \xrightarrow{r} \sigma$ then

$$g_A(\tau,j,\vec{n}) = \langle o,\langle d_0,\ldots,d_{|t(\vec{n})|}\rangle\rangle$$

where

$$d_m = \beta(2,f_C(\langle f_j(\langle o,m\rangle);m,\vec{n}\rangle)).$$

Otherwise set $g_A(\tau,j,\vec{n}) = 0$. From the induction hypothesis and the definition of $Witness^i_A$ it is straightforward to see that when x $\square^p_i$-realizes $A(\vec{n})$ then $f_A(\langle x;\vec{n}\rangle)$ $\square^p_i$-realizes $A(\vec{n})$ and is of p-type o. Furthermore, the kind of reasoning used to prove

Proposition 3 shows that f_A is an extended $\square_i^p$-functional. Q.E.D. ■

§5. K_i-Realization of a Formula

Although we have spent a lot of time on the concept of $\square_i^p$-realization we shall actually need the closely related concept of K_i-realization. We shall modify slightly the definition of $\square_i^p$-realize to define K_i-realize; this is based on an idea of Kleene's [3]. The reason we need to use the notion of K_i-realization is that under certain circumstances, K_i-realizability implies validity; see Proposition 8 below.

Definition. The definition of "x K_i-realizes A" is formed by altering the definition of "x $\square_i^p$-realizes A" by replacing "$\square_i^p$-realize" everywhere by "K_i-realize" and by replacing Cases (2d) and (2e) by:

Case (2d): If $A = B \vee C$ and x is $\langle\langle o,\tau_1,\tau_2\rangle,\langle m_0,m_1,m_2\rangle\rangle$ and either

(i) $m_0 = 0$ and $\langle\tau_1,m_1\rangle$ K_i-realizes B and IS_2^i proves B, or

(ii) $m_0 \neq 0$ and $\langle\tau_2,m_2\rangle$ K_i-realizes C and IS_2^i proves C,

then x K_i-realizes A.

Case (2e): If $A = (\exists x)B(x)$, x is $\langle\langle o,\tau\rangle,\langle m_1,m_2\rangle\rangle$, and $\langle\tau,m_2\rangle$ K_i-realizes $B(m_1)$ and IS_2^i proves $B(m_1)$ then x K_i-realizes A.

Definition. A formula A is K_i-realizable if and only if there exists an $x \in \mathbb{N}$ which K_i-realizes A.

Proposition 7. Propositions 5 and 6 hold when "$\square_i^p$-realize" and "$\square_i^p$-realizable" are replaced everywhere by "K_i-realize" and "K_i-realizable".

Proof. One can readily verify that the proofs of Propositions 5 and 6 can easily be modified to prove Proposition 7. ■

The next proposition is the reason we need the concept of K_i-realizability.

Proposition 8. If $(\exists x)A(x,\vec{c})$ is K_i-realizable then it is $\square_i^p$-fulfillable (and hence valid).

Proof. Suppose $\langle\langle o^k\rangle \xrightarrow{r} \langle o,\tau\rangle, m\rangle$ K_i-realizes $(\exists x)A(x,c_1,\ldots,c_k)$. Then for all $\vec{n}\in\mathbb{N}^k$, $\phi_m(\langle;\vec{n}\rangle)$ is a $\square_i^p$-functional of p-type $\langle o,\tau\rangle$ which K_i-realizes $(\exists x)A(x,\vec{n})$. So there are $\square_i^p$-functions f and g so that

$$\phi_m(\langle;\vec{n}\rangle) = \langle\langle o,\tau\rangle,\langle f(\vec{n}),g(\vec{n})\rangle\rangle$$

and IS_2^i proves $A(f(\vec{n}),\vec{n})$. Since every theorem of IS_2^i is true, f is a $\square_i^p$-function which fulfills $(\exists x)A(x,\vec{c})$. Q.E.D. ■

§6. The Main Theorems and Proof

We are now ready to state and prove Theorem 1. The main result, Theorem 2, is an immediate corollary of Theorem 1 and Proposition 8.

Theorem 1. $(i\geq 1)$. Let $A_1(\vec{c}),\ldots,A_\ell(\vec{c})\longrightarrow B(\vec{c})$ be a sequent provable by IS_2^i where $c_1,\ldots,c_k$ are all the free variables in $A_1,\ldots,A_\ell$ and B. Then there is an extended $\square_i^p$-functional ϕ_m so that whenever $\vec{n}\in\mathbb{N}^k$ and $x_1,\ldots,x_\ell$ K_i-realize $A_1(\vec{n}),\ldots,A_\ell(\vec{n})$, respectively, and each of $A_1(\vec{n}),\ldots,A_\ell(\vec{n})$ is provable by IS_2^i then $\phi_m(\langle\vec{x};\vec{n}\rangle)$ K_i-realizes

$B(\vec{n})$.

Note that in Theorem 1, ℓ may be 0 or B may be missing. In the latter case, the conclusion of Theorem 1 should be interpreted as saying that for all $\vec{n}\in\mathbb{N}^k$, at least one of $A_1(\vec{n}),\ldots,A_\ell(\vec{n})$ is either not K_i-realizable or not IS_2^i-provable. Of course this is trivial since IS_2^i is consistent.

Theorem 1 also holds if we replace "K_i-realizes" by "$\square_i^P$-realizes" and drop the condition that each $A_j(\vec{n})$ be IS_2^i-provable. This is proved by almost exactly the same argument as is used below to prove Theorem 1.

As we remarked above, Theorem 1 is proved in a way very similar to this author's first proof (which was never published) of Theorem 5.5 of [1]. However, it differs in some important respects; in particular, the cut elimination theorem is not used!

Proof of Theorem 1. The proof is by induction on the number of inferences in an IS_2^i-proof P of $A_1,\ldots,A_\ell \longrightarrow B$. The argument splits into a large number of cases depending on the last inference of P.

<u>Case (1).</u> Suppose P has no inferences. Then $A_1,\ldots,A_\ell \longrightarrow B$ is a theorem of S_2^i and each of $A_1,\ldots,A_\ell$ and B is hereditarily Σ_i^b. By Theorem 5.5 of [1], there is a $\square_i^P$-function h so that whenever $\mathbb{N} \models \mathit{Witness}_{A_j}^{i,\vec{c}}(w_j,\vec{n})$ for $1\leq j\leq \ell$ then

$$\mathbb{N} \models \mathit{Witness}_B^{i,\vec{c}}(h(\vec{w},\vec{n}),\vec{n}).$$

For $1\leq j\leq \ell$, let g_j be the function guaranteed to exist by Propositions 6 and 7 such that whenever x_j K_i-realizes $A_j(\vec{n})$ then $\mathit{Witness}_{A_j}^{i,\vec{c}}(g_j(x_j,\vec{n}),\vec{n})$ and so that the mapping

$$\langle x_j;\vec{n}\rangle \longmapsto \langle o,g_j(x_j,\vec{n})\rangle$$

is an extended $\square_i^p$-functional. Define m so that

$$\phi_m(<\vec{x};\vec{n}>) = <o,h(g_1(x,\vec{n}),\ldots,g_\ell(x_\ell,\vec{n}),\vec{n})>.$$

<u>Case (2).</u> ($\wedge$:left). Suppose the last inference of P is

$$\frac{A_1, A_2, \ldots, A_\ell \longrightarrow B}{A_1 \wedge C, A_2, \ldots, A_\ell \longrightarrow B}.$$

By the induction hypothesis there is an $m_0 \in \mathbb{N}$ so that if x_j K_i-realizes $A_j(\vec{n})$ and $IS_2^i \vdash A_j(\vec{n})$ for $1 \leq j \leq \ell$ then $\phi_{m_0}(<\vec{x};\vec{n}>)$ K_i-realizes B. Define g to be the $\square_i^p$-function so that

$$g(x) = \begin{cases} <o,\beta(1,z)> & \text{if } x = <o,z> \\ <\sigma_1,z_1> & \text{if } x = <<\sigma_1,\sigma_2>,<z_1,z_2>> \\ 0 & \text{otherwise} \end{cases}.$$

Define m to be the Gödel number of the function defined by

$$\phi_m(<\vec{x};\vec{n}>) = \phi_{m_0}(<g(x_1),x_2,\ldots,x_\ell;\vec{n}>).$$

Then ϕ_m is an extended $\square_i^p$-functional and satisfies the desired conditions.

<u>Case (3).</u> ($\vee$:left). Suppose the last inference of P is

$$\frac{A_0, A_2, \ldots, A_\ell \longrightarrow B \qquad A_1, A_2, \ldots, A_\ell \longrightarrow B}{A_0 \vee A_1, A_2, \ldots, A_\ell \longrightarrow B}.$$

Let m_0 and m_1 be the numbers given by the induction hypothesis so that if p is 0 or 1 and if x_j K_i-realizes $A_j(\vec{n})$ and IS_2^i proves $A_j(\vec{n})$ for all appropriate j, then

$\phi_{m_p}(\langle x_p, x_2, \ldots, x_\ell; \vec{n}\rangle)$ K_i-realizes $B(\vec{n})$. Recall that if x K_i-realizes $A_0(\vec{n}) \vee A_1(\vec{n})$ then either $x = \langle o, z\rangle$ where $Witness^{i,\vec{c}}_{A_0 \vee A_1}(z, \vec{n})$ or $x = \langle\langle o, \tau_1, \tau_2\rangle, \langle z_0, z_1, z_2\rangle\rangle$ where $\langle \tau_p, z_p\rangle$ K_i-realizes $A_{p-1}(\vec{n})$ where p is 1 or 2 depending on whether z_0 is zero or non-zero. Define $m \in \mathbb{N}$ so that

$$\phi_m(\langle \vec{x}; \vec{n}\rangle) = \begin{cases} \phi_{m_0}(\langle g_0(x_1, \vec{n}), x_2, \ldots, x_\ell; \vec{n}\rangle) & \text{if } h(x_1, \vec{n}) = 0 \\ \phi_{m_1}(\langle g_1(x_1, \vec{n}), x_2, \ldots, x_\ell; \vec{n}\rangle) & \text{otherwise} \end{cases}$$

where

$$h(\langle \sigma, z\rangle, \vec{n}) = \begin{cases} \beta(1, z) & \text{if } \sigma = \langle o, \tau_1, \tau_2\rangle \\ 1 & \text{if } \sigma = o \text{ and } Witness^{i,\vec{c}}_{A_1}(\beta(2, z), \vec{n}) \\ 0 & \text{otherwise} \end{cases}$$

and, for i = 1, 2,

$$g_i(\langle \sigma, z\rangle, \vec{n}) = \begin{cases} \langle \tau_{i+1}, \beta(i+2, z)\rangle & \text{if } \sigma = \langle o, \tau_1, \tau_2\rangle \\ \langle o, \beta(i+1, z)\rangle & \text{if } \sigma = o \end{cases}$$

It is not hard to see that ϕ_m satisfies the conditions of Theorem 1; indeed, whenever x_1 K_i-realizes $A_0(\vec{n}) \vee A_1(\vec{n})$ then either $h(x_1, \vec{n}) = 0$ and $g_0(x_1, \vec{n})$ K_i-realizes $A_0(\vec{n})$ or $h(x_1, \vec{n}) \neq 0$ and $g_1(x_1, \vec{n})$ K_i-realizes $A_1(\vec{n})$.

<u>Case (4).</u> ($\exists$:left). Suppose the last inference of P is

$$\frac{A(c_0), A_2, \ldots, A_\ell \longrightarrow B}{(\exists x)A(x), A_2, \ldots, A_\ell \longrightarrow B}$$

where the free variable c_0 appears only as indicated. By the induction hypothesis, there is an $m_0 \in \mathbb{N}$ so that whenever $A(n_0, \vec{n})$ and $A_j(\vec{n})$ are provable by IS^i_2, x_1 K_i-realizes

$A(n_0,\vec{n})$ and x_j K_i-realizes $A_j(\vec{n})$ for $2 \leq j \leq \ell$, then $\phi_{m_0}(<\vec{x};n_0,\vec{n}>)$ K_i-realizes $B(\vec{n})$.

If x K_i-realizes $(\exists x)A(x,\vec{n})$, it must be the case that $x = <<o,\sigma>,<z_1,z_2>>$ where $<\sigma,z_2>$ K_i-realizes $A(z_1,\vec{n})$ and $IS_2^i \vdash A(z_1,\vec{n})$. Define g and h to be $\square_1^P$-functions so that

$$g(<<o,\sigma>,<z_1,z_2>>) = <\sigma,z_2>$$

and

$$h(<<o,\sigma>,<z_1,z_2>>) = z_1.$$

Let m be the Gödel number of the function defined by

$$\phi_m(<\vec{x};\vec{n}>) = \phi_{m_0}(<g(x_1),x_2,\ldots,x_\ell;h(x_1),\vec{n}>).$$

It is easy to see that the desired conditions are satisfied.

Case (5). When the last inference of P is an $(\exists\leq$:left) inference the argument is much like the proof of Case (4); albeit complicated by the fact that the principal formula of the inference may be hereditarily Σ_i^b. We leave the details to the reader.

Case (6). $(\forall$:left). Suppose the last inference of P is

$$\frac{A(t), A_2, \ldots, A_\ell \longrightarrow B}{(\forall x)A(x), A_2, \ldots, A_\ell \longrightarrow B} .$$

The induction hypothesis is that there is an $m_0 \in \mathbb{N}$ so that if $A(t(\vec{n}),\vec{n})$ and all of $A_j(\vec{n})$ are IS_2^i-provable and if x_1 K_i-realizes $A(t(\vec{n}),\vec{n})$ and x_j K_i-realizes $A_j(\vec{n})$ for $2 \leq j \leq n$, then $\phi_{m_0}(<\vec{x};\vec{n}>)$ K_i-realizes $B(\vec{n})$. Recall that if x K_i-realizes $(\forall x)A(x,\vec{n})$ then x is $<o \xrightarrow{r} \tau,z>$ where for all n_0, $\phi_z(n_0)$ K_i-realizes $A(n_0,\vec{n})$. Define $m \in \mathbb{N}$ so that

$$\phi_m(<\vec{x};\vec{n}>) = \begin{cases} \phi_{m_0}(<\phi_z(t(\vec{n})),x_2,\ldots,x_\ell;\vec{n}>) & \text{if } x_1 = <\sigma,z> \\ 0 & \text{otherwise} . \end{cases}$$

<u>Case</u> <u>(7).</u> ($\forall\leq$:left). The proof for this case is much like that of Case (6), but slightly complicated by the fact that the principal formula may be hereditarily Σ_i^b. We leave the details for the reader.

<u>Case</u> <u>(8).</u> ($\neg$:left). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell \longrightarrow B}{\neg B, A_1,\ldots,A_\ell \longrightarrow} .$$

As we remarked above, this case is trivial since IS_2^i is consistent.

<u>Case</u> <u>(9).</u> ($\vee$:right). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell \longrightarrow B}{A_1,\ldots,A_\ell \longrightarrow B\vee C} .$$

Let ϕ_{m_0} be an extended $\square_i^p$-functional satisfying the induction hypothesis. Let g be a $\square_1^p$-function so that

$$g(<\tau,y>) = <<o,\tau,o>,<0,y,0>>.$$

So if x K_i-realizes $B(\vec{n})$, then g(x) K_i-realizes $B(\vec{n})\vee C(\vec{n})$. Finally let $m\in\mathbb{N}$ be the Gödel number of the function

$$\phi_m(<\vec{x};\vec{n}>) = g(\phi_{m_0}(<\vec{x};\vec{n}>)).$$

<u>Case</u> <u>(10).</u> ($\wedge$:right). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell \longrightarrow B_1 \qquad A_1,\ldots,A_\ell \longrightarrow B_2}{A_1,\ldots,A_\ell \longrightarrow B_1 \wedge B_2}.$$

Let ϕ_{m_1} and ϕ_{m_2} be extended $\Box_i^P$-functionals satisfying the induction hypothesis for the left and right upper sequents, respectively. Define g to be a $\Box_1^P$-function so that

$$g(\langle\tau_1,y_1\rangle,\langle\tau_2,y_2\rangle) = \langle\langle\tau_1,\tau_2\rangle,\langle y_1,y_2\rangle\rangle.$$

So if x_1 and x_2 K_i-realize $B_1(\vec{n})$ and $B_2(\vec{n})$, respectively, then $g(x_1,x_2)$ K_i-realizes $B_1(\vec{n})\wedge B_2(\vec{n})$. So let m be the Gödel number of the function defined by

$$\phi_m(\langle\vec{x};\vec{n}\rangle) = g(\phi_{m_1}(\langle\vec{x};\vec{n}\rangle),\phi_{m_2}(\langle\vec{x};\vec{n}\rangle)).$$

Case (11). ($\exists$:right). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell \longrightarrow B(t)}{A_1,\ldots,A_\ell \longrightarrow (\exists x)B(x)}.$$

The induction hypothesis is that there is an extended $\Box_i^P$-functional ϕ_{m_0} so that if x_j K_i-realizes $A_j(\vec{n})$ and $IS_2^i \vdash A_j(\vec{n})$ for $1\leq j\leq \ell$ then $\phi_{m_0}(\langle\vec{x};\vec{n}\rangle)$ K_i-realizes $B(t(\vec{n}),\vec{n})$. Of course, these conditions imply $B(t(\vec{n}),\vec{n})$ is IS_2^i-provable. Let m be the Gödel number of the function defined by

$$\phi_m(\langle\vec{x};\vec{n}\rangle) = g(\phi_{m_0}(\langle\vec{x};\vec{n}\rangle),t(\vec{n}))$$

where g is a $\Box_1^P$-function such that

$$g(<\tau,y>,z) = <<o,\tau>,<z,y>>.$$

It is easy to verify that ϕ_m satisfies the desired conditions.

Case (12). The case where the final inference of P is an ($\exists\leqslant$:left) inference is very much like Case (11).

Case (13). ($\forall$:right). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell \longrightarrow B(c_0)}{A_1,\ldots,A_\ell \longrightarrow (\forall x)B(x)}$$

where the free variable c_0 appears only as indicated. By the induction hypothesis, there is an extended $\square_i^p$-functional ϕ_{m_0} such that whenever $x_j = <\tau_j,y_j>$ K_i-realizes $A_j(\vec{n})$ and IS_2^i proves $A_j(\vec{n})$ for $1\leqslant j\leqslant \ell$, then $\phi_{m_0}(<\vec{x};n_0,\vec{n}>)$ K_i-realizes $B(n_0,\vec{n})$. Let p_0 be a suitable polynomial which bounds the runtime of ϕ_{m_0}.

Define m to be the Gödel number of the function defined by

$$\phi_m(<\vec{x};\vec{n}>) = <o\xrightarrow{r}\pi,\ \lambda n_0 \phi_{m_0}(<\vec{x};n_0,\vec{n}>)>$$

where

$$r = p_0 \circ \text{runtime}(<\vec{\tau}>)$$

$$\pi = \text{p-type of } \phi_{m_0}(<\vec{x};0,\vec{n}>)$$

and $\lambda n_0 \phi_{m_0}(<\vec{x};n_0,\vec{n}>)$ is the Gödel number of the Turing machine which computes the function

$$n_0 \longmapsto \phi_{m_0}(<\vec{x};n_0,\vec{n}>).$$

It is clear that ϕ_m is an extended $\square_i^p$-functional by Proposition 3. Also it is readily seen that ϕ_m satisfies the desired conditions of Theorem 1.

Case (14). The case where the last inference is a ($\forall\leq$:right) inference is handled similarly to Case (13) and we omit the details.

Case (15). (Cut). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell \longrightarrow C \qquad C, A_1,\ldots,A_\ell \longrightarrow B}{A_1,\ldots,A_\ell \longrightarrow B}.$$

By the induction hypothesis there are extended $\square_i^p$-functionals ϕ_{m_0} and ϕ_{m_1} so that if x_j K_i-realizes $A_j(\vec{n})$ and $IS_2^i \vdash A_j(\vec{n})$ for $1 \leq j \leq \ell$, then $\phi_{m_0}(\langle\vec{x};\vec{n}\rangle)$ K_i-realizes $C(\vec{n})$, and so that when in addition x_0 K_i-realizes $C(\vec{n})$ then $\phi_{m_1}(\langle x_0,\vec{x};\vec{n}\rangle)$ K_i-realizes $B(\vec{n})$. (Note that if IS_2^i proves $A_j(\vec{n})$ for all j, then $C(\vec{n})$ is IS_2^i-provable.)

So we define m so that

$$\phi_m(\langle\vec{x};\vec{n}\rangle) = \phi_{m_1}(\langle\phi_{m_0}(\langle\vec{x};\vec{n}\rangle),\vec{x};\vec{n}\rangle).$$

Case (16). ($H\Sigma_i^b$-PIND). Suppose the last inference of P is

$$\frac{A_1,\ldots,A_\ell, B(\lfloor\tfrac{1}{2}c_0\rfloor) \longrightarrow B(c_0)}{A_1,\ldots,A_\ell, B(0) \longrightarrow B(t)}$$

where the free variable c_0 appears only as indicated and B is a hereditarily Σ_i^b formula. The induction hypothesis is that there is an extended $\square_i^p$-functional so that whenever x_j K_i-realizes $A_j(\vec{n})$, x_0 K_i-realizes $B(\lfloor\tfrac{1}{2}n_0\rfloor,\vec{n})$, $IS_2^i \vdash A_j(\vec{n})$ and $IS_2^i \vdash B(\lfloor\tfrac{1}{2}n_0\rfloor,\vec{n})$, for

$1 \leq j \leq \ell$, then $\phi_{m_0}(<\vec{x},x_0;n_0,\vec{n}>)$ K_i-realizes $B(n_0,\vec{n})$.

First note that if $A_1(\vec{n}),\ldots,A_\ell(\vec{n})$ and $B(0,\vec{n})$ are IS_2^i-provable, then $B(n_0,\vec{n})$ is a theorem of IS_2^i for any $n_0 \in \mathbb{N}$. Second, since B is hereditarily Σ_i^b, Propositions 6 and 7 assert that there is an extended $\square_i^p$-functional ϕ_{m_1} such that whenever x K_i-realizes $B(n_0,\vec{n})$ then $\phi_{m_1}(<x;n_0,\vec{n}>)$ is a $\square_i^p$-functional of p-type o which also K_i-realizes $B(n_0,\vec{n})$. Furthermore, by Proposition 5.3 of [1], we may assume that there is a term t_B in the language of IS_2^i such that $\phi_{m_1}(<x;n_0,\vec{n}>) \leq t_B(n_0,\vec{n})$ for all x, n_0 and $\vec{n}$. Next define h to be the extended $\square_i^p$-functional so that

$$h(<\vec{x},x_0;n_0,\vec{n}>) = \phi_{m_1}(<\phi_{m_0}(<\vec{x},x_0;n_0,\vec{n}>);n_0,\vec{n}>).$$

So h has all the properties of ϕ_{m_0} mentioned above and in addition $h(<\vec{x},x_0;n_0,\vec{n}>)$ is of p-type o and is less than or equal to $t_B(n_0,\vec{n})$.

Define the function g inductively by

$$g(\vec{x},x_0,0,\vec{n}) = h(<\vec{x},x_0;0,\vec{n}>)$$
$$g(\vec{x},x_0,n_0,\vec{n}) = h(<\vec{x},g(\vec{x},x_0,\lfloor \tfrac{1}{2}n_0 \rfloor,\vec{n});n_0,\vec{n}>).$$

It is clear that when x_j K_i-realizes $A_j(\vec{n})$, IS_2^i proves $A_j(\vec{n})$, x_0 K_i-realizes $B(0,\vec{n})$ and IS_2^i proves $B(0,\vec{n})$ for all $1 \leq j \leq \ell$, then $g(\vec{x},x_0,n_0,\vec{n})$ K_i-realizes $B(n_0,\vec{n})$. Also, $g(\vec{x},x_0,n_0,\vec{n})$ is always less than or equal to $t_B(n_0,\vec{n})$. Now define m to be the Gödel number of the function defined so that

$$\phi_m(<\vec{x},x_0;\vec{n}>) = g(x,x_0,t(\vec{n}),\vec{n}).$$

It remains to check that ϕ_m is an extended $\square_i^p$-functional. But this follows from the fact that g was defined by limited iteration (see [1]) from the extended $\square_i^p$-functional h.

Case (17). The remaining cases, (exchange:left), (weak:left), (weak:right) and (contraction:left), are all very simple and we leave them to the reader.

Q.E.D. ■

§7. Some Open Questions

When we compare Theorem 2 above to Theorem 5.1 of [1], it is evident that Theorem 2 is closely analogous to a weakening of the latter theorem. But can the rest of the analogy be proved; that is to say, is the following conjecture true?

Conjecture 1. Suppose $IS_2^i \vdash (\exists y)A(y,\vec{c})$. Then there is a formula $B(a,\vec{c})$ such that IS_2^i proves the following three formulae:

(1) $(\forall y)(\forall \vec{x})[B(y,\vec{x}) \supset A(y,\vec{x})]$

(2) $(\forall y)(\forall z)(\forall \vec{x})[B(y,\vec{x}) \wedge B(z,\vec{x}) \supset y=z]$

(3) $(\forall \vec{x})(\exists y)B(y,\vec{x})$.

As in [1], when $n \in \mathbb{N}$ let I_n be a closed term in the language of IS_2^i so that the value of I_n is n and so that S_2^1 can Σ_1^b-define the (polynomial time) function mapping n to the Gödel number of I_n. When $\vec{x}$ is a vector then $I_{\vec{x}}$ is the vector of terms $I_{x_1},\ldots,I_{x_k}$.

A different way to strengthen Theorem 2 in the case i=1 would be to prove the next conjecture.

Conjecture 2. (i=1). Suppose IS_2^1 proves $(\exists y)A(y,\vec{c})$. Then there exist polynomial time functions f and g so that for all $\vec{n} \in \mathbb{N}^k$, $f(\vec{n})$ is the Gödel number of an IS_2^1-proof of $A(I_{g(n)},I_{\vec{n}})$.

Let $Prf_{IS_2^i}(w,v)$ be the Δ_1^b-defined predicate of S_2^1 which asserts that w is the Gödel number of an IS_2^i-proof of the formula with Gödel number v [1]. We strengthen Conjecture 2 as:

<u>Conjecture</u> <u>3.</u> (i=1). Suppose IS_2^1 proves $(\exists y)A(y,\vec{c})$. Then

$$S_2^1 \vdash (\forall\vec{x})(\exists y)(\exists w)Prf_{IS_2^1}(w,\ulcorner A(I_y,I_{\vec{x}})\urcorner).$$

It is not likely that Conjectures 2 and 3 can be directly generalized for arbitrary i>1. Indeed, the generalizations obtained by substituting IS_2^i for IS_2^1, S_2^i for S_2^1, and $\square_i^p$ for "polynomial time" imply that NP = co-NP when i>1.

On the other hand, the author conjectures that some generalizations of Conjecture 2 and 3 do hold for i>1; however, the generalizations are too complicated to be worth explaining here. (Hint: axiomatize IS_2^i in a different way.)

ACKNOWLEDGEMENTS

I have benefited from discussions with Simon Kochen, Robert Solovay and especially Stephen Cook.

REFERENCES

[1] S.R. Buss, *Bounded Arithmetic*, Ph.D. dissertation, Princeton University, 1985.

[2] S.R. Buss, "The polynomial hierarchy and fragments of Bounded Arithmetic", 17th Annual ACM Symp. on Theory of Computing, Providence, R.I., pp. 285-290.

[3] S.C. Kleene, "On the interpretation of intuitionistic number theory", Journal of Symbolic Logic, 10(1945), 109-124.

[4] J.C.C. McKinsey, "Proof of the independence of the primitive symbols of Heyting's calculus of propositions", Journal of Symbolic Logic 4(1939), 155-158.

[5] D. Nelson, "Recursive functions and intuitionistic number theory", Transactions of the American Mathematical Society, 61(1947), 307-368.

[6] G. Takeuti, *Proof Theory*, North-Holland, 1975.