THE POLYNOMIAL HIERARCHY
AND
INTUITIONISTIC BOUNDED ARITHMETIC

Samuel R. Buss
Mathematical Sciences Research Institute
October 1985

Abstract

Intuitionistic theories $\mathcal{I}^4_1$ of Bounded Arithmetic are introduced and it is shown
that the definable functions of $\mathcal{I}^4_1$ are precisely the $\mathcal{I}^P_1$ 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 $\Sigma^P_1$-definable functions are of interest, our results for intuitionistic
theories concern all the definable functions.

The method of proof uses $\mathcal{I}^P_1$-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.

1

§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, +, ·, 0, 1, $L^k$, $\Sigma^k_1$, $\Pi^k_1$, and $\Sigma^k_1$ and $\Pi^k_1$, where

$$\text{1} \times l = \left(\left\lceil \log_2(l + 1) \right\rceil \right),$$

the length of the binary representation of $l$,

$$\frac{1}{2} \times j = \text{x divided by two, rounded down},$$

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 $(\forall x \in t)$ and $(\exists x \in t)$ where $t$ is an arbitrary term not containing $x$. Bounded quantifiers of the form $(\forall x \in t)$ or $(\exists x \in t)$ 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 $\Sigma^k_n$ and $\Pi^k_n$ 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 quantifiers.

The $\Sigma^b_1$-PIND axioms are the formulae

$$A(0) \land (\forall x)(A(L^2 \times j) \lor A(x)) \lor (\forall x)A(x)$$

where $A$ is a $\Sigma^b_1$-formula. The first order theory $S^b_2$ is defined to have the language above and to be axiomatized by the $\Sigma^b_1$-PIND axioms and an additional, finite set of open axioms [1]. We say that $S^b_2$ can $\Sigma^b_1$-define a function $f: \mathbb{N} \rightarrow \mathbb{N}$ and only if there exists a $\Sigma^b_1$-formula $A(x,y)$ such that

$$\text{(1) } S^b_2 \vdash (\forall x)(\exists y)A(x,y),$$

and
(2) For all \( \tilde{n} \), \( h = A(\tilde{n}, f(\tilde{n})) \).

In [11] it is shown that \( S_1^1 \) can \( \Sigma^b_1 \)-define precisely the \( \Omega^0_1 \)-functions (for \( \Omega \)). The \( \Omega^0_1 \)-functions are the functions at the \( i \)-th level of the polynomial hierarchy [11]. In particular, \( \Omega^0_1 \) 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, \( \Omega^0_1 \) is \( \Sigma^b_1 \).

The theories \( S_1^1 \) are most advantageously viewed as Gentzen-style natural deduction systems. A formal proof in a natural deduction system contains sequents of the form

\[
A_1, \ldots, A_n \rightarrow B_1, \ldots, B_n
\]

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

\[
A_1 \ldots \neg A_n \supset B_1 \cup \ldots \cup B_n
\]

In addition to the usual inference rules for natural deduction, the \( \Sigma^b_1 \)-PIND inference is

\[
\Gamma, A(\xi_{i_1}, \ldots, \xi_{i_m}) \rightarrow A(\xi), \Delta
\]

where \( A \) is a \( \Sigma^b_1 \)-formula, \( \Gamma \) and \( \Delta \) represent sequences of formulae separated by commas, \( t \) is any term and the free variable \( b \) occurs only as indicated.

The intuitionistic 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 \( \rightarrow \). In other words, only sequents of the form

\[
A_1, \ldots, A_n \rightarrow B
\]
or

\[ A_1, \ldots, A_g \rightarrow \]

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

**Definition.** A formula \( A \) is hereditarily \( \Sigma^b_1 \) if and only if every subformula of \( A \) is a \( \Sigma^b_1 \)-formula. The set of all hereditarily \( \Sigma^b_1 \) formulae is denoted \( \text{HE}_1^b \).

Since any formula is a subformula of itself, every hereditarily \( \Sigma^b_1 \) formula is a \( \Sigma^b_1 \)-formula.

The \( \text{HE}_1^b \)-PIND axiom and the \( \text{HE}_1^b \)-PIND inference rule are defined in the obvious way. It is easy to see that the \( \text{HE}_1^b \)-PIND axiom is intuitionistically equivalent to the \( \text{HE}_1^b \)-PIND inference rule; this is proved by the method of proof of Theorem 4 of [1].

**Definition.** Suppose \( \Theta \). Then \( \text{IS}^b_2 \) is an intuitionistic theory of Bounded Arithmetic formalized by a Gentzen-style intuitionistic sequent calculus. The language of \( \text{IS}^b_2 \) is the same as the language of \( S^b_2 \). The axioms of \( \text{IS}^b_2 \) are the \( S^b_2 \)-provable sequents

\[ A_1, \ldots, A_g \rightarrow B \]

such that \( A_1, \ldots, A_g \) and \( B \) are hereditarily \( \Sigma^b_1 \) formulae. In addition, \( \text{IS}^b_2 \) admits the \( \text{HE}_1^b \)-PIND inference.

Of course, it is unimportant that \( \text{IS}^b_2 \) 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 \( \text{IS}^b_2 \) satisfies a restricted version of the law of excluded middle. Namely, if \( A \in \Sigma^b_1 \cup \Pi^b_1 \), or more generally, if both \( A \) and \( \neg A \) are hereditarily \( \Sigma^b_1 \), then
$\mathsf{IS}_2^i$ proves

\[ \neg \neg A \rightarrow A \]

and

\[ \rightarrow A \neg \neg A. \]

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

**Definition.** ($\mathsf{IS}_2^i$). A formula $(\exists y)A(x, y)$ is $[\mathsf{IP}_2^i]$-fulfillable if and only if there is a $[\mathsf{IP}_2^i]$-function $f$ such that for all $\overline{n} \in \mathbb{N}^k$, $A(\overline{n}, f(\overline{n}))$ is valid.

The main result of this paper is

**Theorem 2.** ($\mathsf{IS}_2^i$). If $A$ is any formula and $\mathsf{IS}_2^i \vdash (\exists y)A$ then $(\exists y)A$ is $[\mathsf{IP}_2^i]$-fulfillable.

In particular, if $\mathsf{IS}_2^i \vdash (\forall \overline{x})(\exists y)A(\overline{x}, y)$ then there is a polynomial-time computable function $f: \mathbb{N}^k \rightarrow \mathbb{N}$ so that for all $\overline{n} \in \mathbb{N}^k$, $A(\overline{n}, f(\overline{n}))$ is true.

It is an immediate corollary of Theorem 2 and of the results in [1] that the definable functions of $\mathsf{IS}_2^i$ are precisely the $[\mathsf{IP}_2^i]$ functions. The definition of a function $f$ being definable in $\mathsf{IS}_2^i$ is that there is an arbitrary formula $A(\overline{x}, y)$ so that $A(\overline{n}, f(\overline{n}))$ is true for all values of $\overline{n}$ and such that $\mathsf{IS}_2^i$ proves $(\forall \overline{x})(\exists y)A(\overline{x}, y)$.

It is instructive to compare Theorem 2 with what is known for $\mathsf{S}_2^i$. By Theorem 5.1 of [1], if $A$ is a $\Sigma^p_2$-formula and $\mathsf{S}_2^i \vdash (\exists y)A$ then $(\exists y)A$ is $[\mathsf{IP}_2^i]$-fulfillable. Theorem 2 is similar but concerns the theory $\mathsf{IS}_2^i$ 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 $\land$, $\lor$, $\neg$, $\supset$, $\exists$, and $\forall$. 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 $\#$ which does not contain $\supset$
such that both

$$\langle \neg \psi \rangle \supset \#$$

and

$$\# \supset \langle \neg \psi \rangle$$

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) $A_R \supset A$ 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. $\langle \neg B \rangle_R = \neg (B_L)$,$\langle \neg B \rangle_L = \neg (B_R)$
2. $(B \supset C)_R = B_R \supset C_R$, $(B \supset C)_L = B_L \supset C_L$
(3) \( B \land C_R = B_R \land C_R \), \( B \land C_L = B_L \land C_L \)

(4) \( B \lor C)_R = \neg(B_L \land \neg C_R) \), \( (B \lor C)_L = \neg B_R \land C_L \)

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

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

(7) \( (\forall x \land t)B)_R = (\forall x \land t)(B_R) \), \( (\forall x \land t)B)_L = (\forall x \land t)(B_L) \)

(8) \( (\exists x \land t)B)_R = (\exists x \land t)(B_R) \), \( (\exists x \land t)B)_L = (\exists x \land t)(B_L) \).

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

\[
\frac{\neg B_R \rightarrow B}{\neg B_R \rightarrow B} \quad \frac{C_L \rightarrow C}{C_L \rightarrow B} \quad \frac{\neg B_R \land C_L, B \rightarrow C}{\neg B_R \land C_L \rightarrow B \lor C}
\]

Thus \( \neg B_R \land C \supset (B \lor C) \) is intuitionistically provable. We leave the other cases to the reader.

**Proposition 2.** Let \( A \) be any hereditarily \( \Sigma^b_1 \) formula. Then there is a hereditarily \( \Sigma^b_1 \) formula \( B \) so that

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

(b) \( IS^1_2 \) proves \( A \supset B \) and \( B \supset A \).

**Proof.** Just take \( B \) to be \( A^\prime \) 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 \( IS^1_2 \) proves \( (\forall x)A \). By Proposition 1
there is an IS\textsuperscript{1} proof of (\exists x)A\textsubscript{R}, and by Proposition 2 it may be assumed without loss of generality that the implication symbol, \textimplied, 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 \textimplied for example, the axiom \text{A\&B} \rightarrow \text{\negA\&B} can be derived by

\[
\begin{align*}
\text{\negA & \rightarrow \negA} & & \text{A & \rightarrow B} \\
\text{\negA & \rightarrow \negA & \&B} & & \text{A & \&B \rightarrow \negB} \\
\text{\negA & \&A & \&B \rightarrow \negA & \&B} & & \text{A & \&B \rightarrow \negB & \&A} \\
\text{\negA & \&A & \&B \rightarrow \negA & \&B} & & \text{A & \&B \rightarrow \negB & \&A} \\
\text{\negA & \&A & \&B \rightarrow \negA & \&B} & & \text{A & \&B \rightarrow \negB & \&A} \\
\text{\&B \rightarrow \negA & \&B} \end{align*}
\]

where the last inference is a cut against the sequent \text{\rightarrow \negA & A} (not shown) which is an axiom since A\&B is hereditarily \Sigma\textsuperscript{1} \text{b}, hence A \in \Sigma\textsuperscript{1} \text{b} & \text{A & B} and \text{\negA & A} is hereditarily \Sigma\textsuperscript{1} \text{b}.

Thus the implication symbol, \textimplied, 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\textsuperscript{1} proof of (\exists x)A\textsubscript{R} in which the implication symbol does not appear at all. Since A and A\textsubscript{R} are classically equivalent, it is clear that (\exists x)A\textsubscript{R} is \text{\Sigma} \text{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, \textimplied, 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, \textimplied.

### 8.2. 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, \text{\textbf{\textit{P}}} \text{p}-functionals, and extended \text{\textbf{\textit{P}}} \text{p}-functionals.
Definition. A suitable polynomial is a polynomial in one variable with non-negative integer coefficients. If \( q \) and \( s \) are suitable polynomials, then \( qs, q+s \) 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 \( \langle \tau_1, \ldots, \tau_k \rangle \) is a \( p \)-type.
3. If \( \tau \) and \( \sigma \) are \( p \)-types and \( r \) is a suitable polynomial, then \( \tau \cdot^r \sigma \) is a \( p \)-type.

Intuitively, \( \tau \cdot^r \sigma \) is the class of all functions with domain \( \tau \), range \( \sigma \) and computational complexity bounded by \( r \). When \( k \in \mathbb{N} \) we write \( o^k \) to denote \( o \cdot \ldots \cdot o \) 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 \( \Omega_1 \) be a canonical \( \Sigma^P_1 \)-complete predicate. So \( \Omega_2 \) could be \text{SAT} and \( \Omega_3 \) the empty set. Let \( m \) be the Gödel number of a Turing machine \( M_m \). Then \( \#^m \) is the unary function which is computed by the Turing machine \( M_m \) with \( \Omega_1 \) as its oracle.
Note $s^i_m$ may be a partial function. When $m$ is not a valid Gödel number, let $s^i_m$ be the constant zero function.

We shall frequently write just $s_m$ instead of $s^i_m$ 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 $s^i_m(n)$ is equal to the number of steps the Turing machine $M_m$ uses with oracle $O_i$ on input $z$. Let $|z|$ denote the length of the binary representation of $z$, so $|z| = \log_2(|z|+1)$. If $r$ is a suitable polynomial, then the runtime of $s^i_m(n)$ is bounded by $r$ if and only if the runtime of $s^i_m(n)$ is less than or equal to $r(|z|).

**Definition.** A (Gödel number of a) $\Omega^p_i$-functional of $p$-type $\pi$ is an ordered pair $<\pi,m>$ so that $\pi$ is the Gödel number of a $p$-type and $m \in \mathbb{N}$ and so that the following inductive definition is satisfied:

1. If $\pi \prec \sigma$ then $m$ may be any natural number.
2. If $\pi = <\pi_1,\ldots,\pi_k>$ then $m$ must be a $k$-tuple $<m_1,\ldots,m_k>$ where $<\pi_j,m_j>$ is a $\Omega^p_i$-functional for $1 \leq j \leq k$.
3. If $\pi = \pi \times \sigma$ then $m$ must be a Gödel number of a Turing machine $M_m$ so that for every (Gödel number of a) $\Omega^p_i$-functional $z$ of $p$-type $\pi$ the runtime of $s^i_m(z)$ is bounded by $r$ and the value of $s^i_m(z)$ is (the Gödel number of) a $\Omega^p_i$-functional of $p$-type $\sigma$.

**Definition.** A unary function $f$ is a $\Omega^p_i$-functional of $p$-type $\pi$ if and only if there exists $m \in \mathbb{N}$ so that $f(n) = s^i_m(n)$ for all $n \in \mathbb{N}$ and $<\pi,m>$ is a $\Omega^p_i$-functional.
As an example, consider the function \( f \) defined so that

\[
f(x) = \begin{cases} 
\#_m(n) & \text{if } x = <\langle 0^m \rangle, 0>, <m, n>> \\
\text{and the runtime of } \#_m(n) \text{ is } \in \text{r}(|in|), \\
0 & \text{otherwise}
\end{cases}
\]

Then for any suitable polynomial \( r \) and p-type \( \tau \), there is a suitable polynomial \( s \), say \( s = 10000r^2 + 1 \), so that \( f \) is a \( \text{P}_1 \)-functional of \( \text{p-type } 0^m \tau, 0^m \tau \neq s \tau \). Furthermore, for any p-type \( \kappa \) which is not of the form \( \kappa = <\langle 0 \rangle, 0> \), there is a polynomial \( s \), say \( s(n) = 10000(n+1) \), so that \( f \) is a \( \text{P}_1 \)-functional of \( p \)-type \( s \neq 0 \). Note, however, that \( f \) is not even a \( \text{P}_1 \)-function as its runtime is not bounded by a polynomial uniformly for all \( p \)-types of inputs.

**Definition.** Let \( \tau \) be a \( s \)-type. The runtime of \( \tau \), \( \text{runtime}(\tau) \), is defined inductively by:

\[
\begin{align*}
(a) & \quad \text{runtime}(0) = 0 \\
(b) & \quad \text{runtime}(\langle \tau_1, ..., \tau_k \rangle) = \sum_{j=1}^{k} \text{runtime}(\tau_j) \\
(c) & \quad \text{runtime}(\langle 0^m \rangle \tau_2) = r + \text{runtime}(\tau_2).
\end{align*}
\]

Note that the runtime of \( \tau \) is always a suitable polynomial.

**Definition.** The function \( \#_m \) is an extended \( \text{P}_1 \)-functional if and only if there is a suitable polynomial \( p \) so that for every p-type \( \tau \) there exists a \( p \)-type \( \sigma \) such that

\[
\begin{align*}
(a) & \quad \text{runtime}(\sigma) \leq p \text{runtime}(\tau), \text{ and} \\
(b) & \quad \langle \tau, \sigma, m \rangle \text{ is a } \text{P}_1 \text{-functional where } s = p \text{runtime}(\tau).
\end{align*}
\]

The polynomial \( p \) bounds the runtime of the extended \( \text{P}_1 \)-functional \( \#_m \).

11
Our example above of a function $f$ which was a $\mathcal{F}_P^1$-functional was in fact an example of an extended $\mathcal{F}_P^1$-functional. That example illustrated what is perhaps the single most important property of extended $\mathcal{F}_P^1$-functionals, so we restate it in Proposition 3.

**Proposition 3.** (Def. 1).

(a) If $\sigma_m^1$ and $\sigma_n^1$ are extended $\mathcal{F}_P^1$-functionals then their composition $\sigma_m^1 \circ \sigma_n^1$ is an extended $\mathcal{F}_P^1$-functional.

(b) Let $f$ be the function defined by

$$ f(x) = \begin{cases} 
\sigma_m^1(n) & \text{if } x = \langle\tau, \sigma_m^1 \circ \sigma, \langle m, n \rangle \rangle \\
0 & \text{otherwise.}
\end{cases} $$

Then $f$ is an extended $\mathcal{F}_P^1$-functional.

**Proof.**

(a) Let $p_m$ and $p_n$ bound the runtimes of $\sigma_m^1$ and $\sigma_n^1$. Let $\tau$ be any $p$-type. Then there exists a $p$-type $\sigma_1^1$ so that $\langle\tau, \sigma_1^1 \circ \sigma, \langle m, n \rangle \rangle$ is a $\mathcal{F}_P^1$-functional where $r = p_n \cdot \text{runtime}(\tau)$.

There also exists a $p$-type $\sigma_2^1$ so that $\langle\sigma, \sigma_2^1 \circ \sigma, \langle m, n \rangle \rangle$ is a $\mathcal{F}_P^1$-functional where $s = p_m \cdot \text{runtime}(\sigma_1^1)$. Furthermore, the runtime of $\sigma_1^1$ is $\leq p_n \cdot \text{runtime}(\tau)$ and the runtime of $\sigma_2^1$ is $\leq p_m \cdot \text{runtime}(\sigma_1^1)$; hence the runtime of $\sigma_2^1$ is $\leq p_m \cdot p_n \cdot \text{runtime}(\tau)$.

Consider a Turing machine $M$ which computes $\sigma_m^1 \circ \sigma_n^1$ in the straightforward manner and let $k$ be the Gödel number of $M$, so $\sigma_k^1 = \sigma_m^1 \circ \sigma_n^1$. The runtime of $\sigma_k^1$ is bounded by $q(r, s)$ for some fixed polynomial $q$. Now let $p = q(p_n, p_m, p_n)$. We claim that $\sigma_k^1$ is an extended $\mathcal{F}_P^1$-functional with runtime bounded by $p$. This is
immediate from the definition of p and the fact that p(c) > p_m = p_m(c) for all n \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 \( \mathbf{z} \) is a vector of \( \mathcal{L}^n \)-functionals and \( n_1, \ldots, n_k \) are non-negative integers, then \( \langle z, n_1, \ldots, n_k \rangle \) denotes the \( \mathcal{L}^n \)-functional

\[
\langle z, n_1, \ldots, n_k \rangle
\]

**§4. Realization of a Formula**

In this section, we define what it means to \( \mathcal{L}^n \)-realize a formula and prove some basic properties. We begin by reviewing a definition in §5.1 of Buss [1].

Suppose \( A(\mathbf{z}) \) is a \( \Sigma^b_k \)-formula where \( \mathbf{z} \) is a k-tuple containing all of the free variables in \( A \). A formula \( \text{Witness}_{\mathcal{L}^n}^k(z, \mathbf{z}) \) is defined in [1] with \( k+1 \) free variables; the intended meaning of \( \text{Witness}_{\mathcal{L}^n}^k(w, \mathbf{z}) \) is that \( w \) codes a "witness" to, or a "proof" of, the truth of \( A(\mathbf{z}) \). Indeed, the following conditions hold:

1. \( \text{Witness}_{\mathcal{L}^n}^k(z, \mathbf{z}) \) is a \( \Delta^b_k \)-predicate.
2. \( \text{Witness}_{\mathcal{L}^n}^k(z, \mathbf{z}) \) is defined by a \( \Delta^b_k \)-formula in the theory of \( S^1_2 \).
3. There is a term \( t_A \) so that \( S^1_2 \) proves

\[
A(\mathbf{z}) \iff (\exists w) t_A(z) \text{Witness}_{\mathcal{L}^n}^k(w, \mathbf{z}).
\]
Intuitively, \( \text{Witness}_{A}^{B}(w, z) \) holds if and only if \( w \) codes values for the existentially quantified variables of \( A \) which make \( A(z) \) true. The reader should refer to [1] for the definition of \( \text{Witness}_{A}^{B}(z) \) 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 \( x \in \mathbb{D}_{i}^{P} \)-realizes \( A \) is defined by the following inductive definition:

**Case (1):** If \( A \equiv A(z) \) has free variables \( c_{1}, \ldots, c_{k} \) where \( k \neq 0 \), then \( x \) must equal \( \langle r, m \rangle \), the Gödel number of a \( \mathbb{D}_{i}^{P} \)-functional of \( \pi \)-type \( \pi = \zeta \langle \mathcal{Z} \rangle \), and for all \( \tilde{z} \in \mathbb{N}^{k}, \#_{m}(\tilde{z}; \tilde{n}) \) must \( \mathbb{D}_{i}^{P} \)-realize \( A(\tilde{n}) \).

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

**Case (2a):** If \( A \) is hereditarily \( \Sigma_{i}^{b} \), \( \text{Witness}_{A}^{b}(m) \) and \( x \) is \( \langle \cdot, m \rangle \) then \( x \in \mathbb{D}_{i}^{P} \)-realizes \( A \).

**Case (2b):** If \( A = (\forall x)B(x) \) and if \( x \in \mathbb{D}_{i}^{P} \)-realizes \( B(c) \) where \( c \) is a new free variable, then \( x \in \mathbb{D}_{i}^{P} \)-realizes \( A \).

**Case (2c):** If \( A = B \cdot C \) and \( \langle \tau_{1}, m_{1} \rangle \) and \( \langle \tau_{2}, m_{2} \rangle \) \( \mathbb{D}_{i}^{P} \)-realize \( B \) and \( C \), respectively, and if \( x = \langle \langle \tau_{1}, \tau_{2}, \langle m_{1}, m_{2} \rangle \rangle \rangle \), then \( x \in \mathbb{D}_{i}^{P} \)-realizes \( A \).

**Case (2d):** If \( A = B \cdot C \), \( x \) is \( \langle \cdot, \tau_{1}, \tau_{2}, \langle m_{0}, m_{1}, m_{2} \rangle \rangle \) and either

(i) \( m_{0} = 0 \) and \( \langle \tau_{1}, m_{1} \rangle \) \( \mathbb{D}_{i}^{P} \)-realizes \( B \), or

(ii) \( m_{0} \neq 0 \) and \( \langle \tau_{2}, m_{2} \rangle \) \( \mathbb{D}_{i}^{P} \)-realizes \( C \),

then \( x \in \mathbb{D}_{i}^{P} \)-realizes \( A \).
Case (2c): If \( A = (\exists x)B(x) \) and \( x \in \mathcal{P} \)-realizes \( B(m_1) \) then \( x \in \mathcal{P} \)-realizes \( A \).

Case (2d): If \( A = (\forall x)(\exists t)B(x) \) and \( z \in \mathcal{P} \)-realizes \( (\forall x)(\exists t)B(x) \) then \( x \in \mathcal{P} \)-realizes \( A \).

Case (2e): If \( A = (\exists x)(\exists t)B(x) \) and \( z \in \mathcal{P} \)-realizes \( (\exists x)(\exists t)B(x) \) then \( x \in \mathcal{P} \)-realizes \( A \).

Case (2f): If \( A = \lnot B \) and \( B \) is not \( \mathcal{P} \)-realizable then any \( x = \langle o, m \rangle \) \( \mathcal{P} \)-realizes \( A \).

Note that whenever \( x \in \mathcal{P} \)-realizes a formula \( A \), \( x \) is a \( \mathcal{P} \)-functional. However, the \( p \)-type of \( x \) is not uniquely determined by \( A \). For example, if \( B \) is hereditarily \( \Sigma^b_1 \) and \( A = (\exists x)(\exists t)B(x) \) is a closed, true formula then there are \( \mathcal{P} \)-functionals of \( p \)-types \( o \) and \( <o, o> \) which \( \mathcal{P} \)-realize \( A \). Namely, if \( Witness(m) \) then \( \langle o, m \rangle \in \mathcal{P} \)-realizes \( A \), and if \( Witness_{B(c)}(m_1, m_1) \) and \( m_1 \in t \) then \( \langle o, o \rangle, \langle m_1, <0, m_2> \rangle \in \mathcal{P} \)-realizes \( A \).

Definition. A formula \( A \) is \( \mathcal{P} \)-realizable if and only if there exists an \( x \in \mathbb{N} \) which \( \mathcal{P} \)-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 \( \mathcal{P} \)-realizable; conversely, a formula may be \( \mathcal{P} \)-realizable but (classically) false.

The next proposition is a simple consequence of the definition of \( Witness^1_{A, \mathcal{E}} \) and is readily proved by the methods of §5.1 of [1].

Proposition 4. Let \( A(c) \) be a formula in \( \Sigma_1^b \cap \Pi_1^b \). Then there is a \( \mathcal{P} \)-function
g such that

\[ \mathcal{N} = (\forall \mathcal{G}) (A(\mathcal{G}) \supset Witness^A_{\Sigma^1_{\mathcal{G}}} (\mathcal{G}(\mathcal{C}), \mathcal{C})) \].

In spite of our remarks above about the independence of truth and \( \Pi^2 \)-realizability, the next proposition shows that these notions are equivalent for hereditarily \( \Sigma^b_1 \) sentences.

**Proposition 5.** Let \( A \) be a closed, hereditarily \( \Sigma^b_1 \) formula. Then \( A \) is \( \Pi^2 \)-realizable if and only if \( A \) is true.

**Proof.**

\( \subseteq \) Suppose \( A \) is true. Since \( A \) is closed and \( \Sigma^b_1 \), there is a number \( w \) such that \( Witness^A_{\Sigma^1}(w) \). Hence \( <o,w> \) \( \Pi^2 \)-realizes \( A \).

\( \supseteq \) 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 \( \Pi^2 \)-functional which \( \Pi^2 \)-realizes \( A \).

**Case (1):** \( A \) is \( \Pi^2 \)-realized by \( <o,m> \). There are two possibilities. The first is that \( Witness^A_{\Sigma^1}(m) \) and hence \( A \) is true. The second is that \( A = \neg B \) and \( B \) is not \( \Pi^2 \)-realizable. But then \( B \) must be false by the first half of this proposition. So, again, \( A \) is true.

**Case (2):** Suppose \( A \) is \( (\exists x \in \exists B(x)) \) and \( \langle <0,7>,<m_1,m_2> \rangle \) \( \Pi^2 \)-realizes \( A \). Then \( \langle <o,m> \rangle \) \( \Pi^2 \)-realizes \( m_1 \in \exists B(m_1) \). So by the induction hypothesis \( m_1 \in \exists B(m_1) \) is true. Hence \( A \) is true.
Case (3): Suppose \( A \) is \( \forall x(\exists t)B(x) \) and \( \varphi^{A^P, \tau, m} \) \( \forall \varphi \) realizes \( A \). For all \( n \in \mathbb{N} \), \( \varphi^{A^P, \tau, m} \) realizes \( \forall n(\exists t)B(n) \) and by the induction hypothesis, \( \forall n(\exists t)B(n) \) 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. \( \square \)

It is an immediate consequence of Proposition 5 that whenever a hereditarily \( \Sigma_1^b \) formula \( A(\bar{c}) \) is \( \forall \varphi \)-realizable then it is true for all values of \( \bar{c} \). Thus it is not unreasonable to expect that there is an effective procedure which given an \( x \in \mathbb{N} \) which \( \forall \varphi \)-realizes \( A(\bar{n}) \) produces a \( \forall \varphi \) so that \( \text{Witness}^{A^P, \tau, A^P}_A(w, \bar{n}) \). This is stated more fully as Proposition 6.

Proposition 6. Let \( A(\bar{c}) \) be a hereditarily \( \Sigma_1^b \) formula where \( c_1, \ldots, c_k \) are the only free variables in \( A \). Then there is an extended \( \forall \varphi \)-functional \( f_A \) so that whenever \( \forall \varphi \in \mathbb{N}^k \) and \( x \in \mathbb{N}^k \) \( \forall \varphi \)-realizes \( A(\bar{c}) \) then \( f_A(x, \bar{n}) \) is (the Goedel number of) a \( \forall \varphi \)-functional of \( p \)-type \( \rho \) which \( \forall \varphi \)-realizes \( A(\bar{c}) \), and moreover, \( f_A(x, \bar{n}) \) is of the form \( \varphi(\bar{a}, \bar{n}) \) where \( \bar{a} \in \text{Witness}^{A^P, \tau, A^P}_A(w, \bar{n}) \).

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 \( f_A(x, \bar{n}) = (t_A, \bar{n}) \) for all \( x \) and \( \bar{n} \).

Proof. The proof is by induction on the complexity of \( A \), so assume that if \( B \) and \( C \) are formulas less complex than \( A \) then \( f_B \) and \( f_C \) are extended \( \forall \varphi \)-functionals satisfying the conditions of Proposition 6.

The input to \( f_A \) is the Goedel number of a \( \forall \varphi \)-functional. We define \( f_A \) so that
\[
f_A(y) = \begin{cases} 
    x & \text{if } y = \langle \sigma, x \rangle; \bar{\pi} \text{ where } \text{Witness}_A^{1, \zeta}(x, \pi) \\
    g_A(\tau, j; \bar{\pi}) & \text{if } y = \langle \tau, j \rangle; \bar{\pi} \text{ and the above condition fails} \\
    0 & \text{otherwise}
\end{cases}
\]

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

**Case (1):** Suppose \(A \in \Sigma^b_1 \cap \Pi^b_1\). By Proposition 4 there is a \(\Pi^0_1\)-function \(g\) so that

\[
\text{Witness}_A^{1, \zeta}(\sigma; \bar{\pi}) = \langle \sigma, g(\bar{\pi}) \rangle.
\]

So define \(g_A(\tau, j; \bar{\pi}) = \langle \sigma, g(\bar{\pi}) \rangle\). Now by Proposition 5, if \(\langle \tau, j \rangle\) \(\Pi^0_1\)-realizes \(\bar{\pi}\), then \(A(\bar{\pi})\) is true and thus \(\text{Witness}_A^{1, \zeta}(\sigma; \bar{\pi})\).

**Case (2):** Suppose \(A\) is \(\neg B\). Since \(A\) is hereditarily \(\Sigma^b_1\), \(A \in \Sigma^b_1 \cap \Pi^b_1\). Hence Case (1) applies.

**Case (3):** Suppose \(A(\bar{\pi}) = (3x)(\exists y)(B(y, \bar{\pi}))\). Then the \(p\)-type \(\tau\) must be of the form \(\langle \sigma, \sigma \rangle\); otherwise \(\langle \tau, \rho \rangle\) can not possibly \(\Pi^0_1\)-realize \(A(\bar{\pi})\). Furthermore, we must have \(j = \langle j_1, j_2 \rangle\) so that \(\langle \sigma, j_1 \rangle\) \(\Pi^0_1\)-realizes \(j_1(\bar{\pi}); B(y, \bar{\pi})\). Let \(C(\bar{\pi})\) be the formula \(\langle x, (\exists y)(B(x, \bar{\pi}))\rangle\) and define \(g_A\) by

\[
g_A(\tau, j; \bar{\pi}) = \begin{cases} 
    \langle \sigma, j_1, \#(z, \bar{\pi}) \rangle & \text{if } \tau = \langle \sigma, \sigma \rangle, \ z = \langle j_1, j_2 \rangle \\
    & \text{and } f_C(\langle \sigma, j_2 \rangle; j_1, \bar{\pi}) = \langle \sigma, z \rangle \\
    0 & \text{otherwise} \end{cases}
\]

Note that \(\#(z, \bar{\pi})\) is the Gödel beta function and whenever \(\text{Witness}_A^{1, \zeta}(z)\) then
It is apparent from the definition of \( \text{Witness}_A^1 \) and the induction hypothesis that the definition of \( g_A \) makes \( f_A \) satisfy Proposition 6.

**Case (4):** Suppose \( A(\tilde{c}) = B(\tilde{c}) \cdot C(\tilde{c}) \). In order for \( \langle \tau, \tilde{n} \rangle \) to \( \Omega^4 \)-realize \( A(\tilde{n}) \) we must have \( \tau = \langle o, \tau_1, \tau_2 \rangle \) and either \( \langle \tau_1, \tilde{n} \rangle \) \( \Omega^4 \)-realizes \( B(\tilde{n}) \) or \( \langle \tau_2, \tilde{n} \rangle \) \( \Omega^4 \)-realizes \( C(\tilde{n}) \). Accordingly, we define \( g_A \) so that

\[
\begin{cases}
\langle o, \langle x_B, 0 \rangle \rangle \quad & \text{if } \tau = \langle o, \tau_1, \tau_2 \rangle, \quad A(1, 1) = 0, \\
\quad \quad \quad \text{and } f_B(\langle \tau_1, \langle x_B, 0 \rangle \rangle) = o, x_B > \\
\langle o, \langle x_C, 0 \rangle \rangle \quad & \text{if } \tau = \langle o, \tau_1, \tau_2 \rangle, \quad A(1, 1) \neq 0, \\
\quad \quad \quad \text{and } f_C(\langle \tau_2, \langle x_C, 0 \rangle \rangle) = o, x_C > \\
0 & \text{otherwise.}
\end{cases}
\]

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

**Case (6):** Suppose \( A(\tilde{c}) = (\forall x \exists y \exists z(t(\tilde{c}) \cdot B(x, \tilde{c})) \cdot C(\tilde{c}) \). Let \( C(\tilde{c}, \tilde{c}) \) be the formula \( \forall x \exists y \exists z \langle x, y, z, t(\tilde{c}) \rangle \cdot B(x, \tilde{c}) \cdot C(\tilde{c}, \tilde{c}) \). In order for \( \langle \tau, \tilde{n} \rangle \) to \( \Omega^4 \)-realize \( A(\tilde{n}) \) \( \tau \) must be of the form \( o \cdot \mathcal{L}_m x \) and for all \( n \in \mathbb{N} \), \( f(\langle o, n \rangle) \) \( \Omega^4 \)-realizes \( C(\tilde{n}, \tilde{n}) \).

Define \( g_A \) so that if \( \tau \) is \( o \cdot \mathcal{L}_m x \) then

\[
g_A(\tau, \tilde{n}) = \langle o, \langle d_m, \ldots, d_1 t(\tilde{n}) \rangle \rangle
\]

where

\[
d_m = \langle 2, f_C(\langle f(\langle o, m \rangle), m, \tilde{n} \rangle) \rangle
\]

Otherwise set \( g_A(\tau, \tilde{n}) = 0 \). From the induction hypothesis and the definition of \( \text{Witness}_A^1 \) it is straightforward to see that when \( x \) \( \Omega^4 \)-realizes \( A(\tilde{n}) \) then \( f_A(\langle x, \tilde{n} \rangle) \) \( \Omega^4 \)-realizes \( A(\tilde{n}) \) and is of \( p \)-type \( o \). Furthermore, the kind of reasoning used to prove
Proposition 3 shows that $f_A$ is an extended $\Omega_1^P$-functional.

\section*{5. $K_1$-Realization of a Formula}

Although we have spent a lot of time on the concept of $\Omega_1^P$-realization we shall actually need the closely related concept of $K_1$-realization. We shall modify slightly the definition of $\Omega_1^P$-realize to define $K_1$-realize; this is based on an idea of Kleene's [3]. The reason we need to use the notion of $K_1$-realization is that under certain circumstances, $K_1$-realizability implies validity; see Proposition 8 below.

\textbf{Definition.} The definition of "$x$ $K_1$-realizes $A$" is formed by altering the definition of "$x$ $\Omega_1^P$-realizes $A$" by replacing "$\Omega_1^P$-realize" everywhere by "$K_1$-realize" and by replacing Cases (2d) and (2e) by:

\textbf{Case (2d):} If $A = B \cdot C$ and $x$ is $\langle o, r, r, m_1, m_2 \rangle$ and either

(i) $m_0 = 0$ and $\langle r, m_1 \rangle$ $K_1$-realizes $B$ and $IS_2^1$ proves $B$, or

(ii) $m_0 \neq 0$ and $\langle r, m_2 \rangle$ $K_1$-realizes $C$ and $IS_2^1$ proves $C$,

then $x$ $K_1$-realizes $A$.

\textbf{Case (2e):} If $A = (\exists x)B(x)$, $x$ is $\langle o, r, r, m_1, m_2 \rangle$, and $\langle r, m_2 \rangle$ $K_1$-realizes $Bm_1$ and $IS_2^1$ proves $Bm_1$ then $x$ $K_1$-realizes $A$.

\textbf{Definition.} A formula $A$ is $K_1$-\textbf{realizable} if and only if there exists an $x \in \mathbb{N}$ which $K_1$-realizes $A$.

\textbf{Proposition 7.} Propositions 5 and 6 hold when "$\Omega_1^P$-realize" and "$\Omega_1^P$-realizable" are replaced everywhere by "$K_1$-realize" and "$K_1$-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 $K_1$-realizability.

**Proposition 8.** If $(3x)A(x,\bar{z})$ is $K_1$-realizable then it is $[\Pi^P_1]$-fulfillable (and hence valid).

Proof. Suppose $\langle o^{K_1}, \phi_{o}, \phi_{\tau}, m \rangle$ $K_1$-realizes $(3x)A(x,c_1,\ldots,c_k)$. Then for all $\bar{z} \in \mathcal{M}^k$, $\sigma_m(\bar{z}; \bar{z})$ is a $[\Pi^P_1]$-functional of $\tau$-type $\langle o, \tau \rangle$ which $K_1$-realizes $(3x)A(x,\bar{z})$.

So there are $[\Pi^P_1]$-functions $f$ and $g$ so that

$$\sigma_m(\bar{c}; \bar{z}) = \langle o^{K_1}, \phi_{o^{K_1}}, \phi_{\tau}, m \rangle$$

and $IS_2^k$ proves $A(f(\bar{z}), \bar{z})$. Since every theorem of $IS_2^k$ is true, $f$ is a $[\Pi^P_1]$-function which fulfills $(3x)A(x,\bar{z})$.

Q.E.D.

65. 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.** (S2). Let $A_1(\bar{c}), \ldots, A_k(\bar{c}) \rightarrow B(\bar{c})$ be a sequent provable by $IS_2^k$ where $c_1, \ldots, c_k$ are all the free variables in $A_1, \ldots, A_k$ and $B$. Then there is an extended $[\Pi^P_1]$-functional $\sigma_m$ so that whenever $\bar{z} \in \mathcal{M}^k$ and $x_1, \ldots, x_k$ $K_1$-realize $A_1(\bar{c}), \ldots, A_k(\bar{c})$, respectively, and each of $A_1(\bar{c}), \ldots, A_k(\bar{c})$ is provable by $IS_2^k$ then $\sigma_m(\bar{c}; \bar{z})$ $K_1$-realizes
Note that in Theorem 1, \( \mathcal{A} \) 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 \( \bar{n} \in \mathbb{N}^k \), at least one of \( A_1(\bar{n}), \ldots, A_\mathcal{A}(\bar{n}) \) is either not \( K_1 \)-realizable or not \( IS^1_2 \)-provable. Of course this is trivial since \( IS^1_2 \) is consistent.

Theorem 1 also holds if we replace "\( K_1 \)-realizes" by "\( IS^1_2 \)-realizes" and drop the condition that each \( A_\mathcal{A}(\bar{n}) \) be \( IS^1_2 \)-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 \( IS^1_2 \)-proof \( \mathcal{P} \) of \( A_1 \ldots A_\mathcal{A} \rightarrow B \). The argument splits into a large number of cases depending on the last inference of \( \mathcal{P} \).

Case 1. Suppose \( \mathcal{P} \) has no inferences. Then \( A_1 \ldots A_\mathcal{A} \rightarrow B \) is a theorem of \( S^1_2 \) and each of \( A_1 \ldots A_\mathcal{A} \) and \( B \) is hereditarily \( \Sigma^b \). By Theorem 5.5 of [1], there is a \( \Sigma^b \)-function \( h \) so that whenever \( \mathcal{N} \models Witness^1_{\mathcal{A}, \mathcal{B}}(w, \bar{n}) \) for \( \mathcal{N} \models \mathcal{P} \), then

\[
\mathcal{N} \models Witness^1_{\mathcal{A}, \mathcal{B}}(w, h(\mathcal{G}, \bar{n}), \bar{n}).
\]

For \( \mathcal{N} \models \mathcal{P} \), let \( g_1 \) be the function guaranteed to exist by Propositions 6 and 7 such that whenever \( x_1 \) \( K_1 \)-realizes \( A_\mathcal{A}(\bar{n}) \) then \( Witness^1_{\mathcal{A}, \mathcal{B}}(g_1(x_1), \bar{n}) \) and so that the mapping

\[
<\bar{x}, \bar{n}> \mapsto <\bar{0}, g_1(\bar{x}), \bar{n}>
\]
is an extended \( \Pi_1 \)-functional. Define \( m \) so that
\[
\phi_{m}(\bar{x}, \bar{y}) = \phi_{o, h}(x_1, \ldots, x_g, y_1, \ldots, y_n).
\]

**Case (2).** (\( \land \)-left). Suppose the last inference of \( P \) is
\[
\frac{A_1, A_2, \ldots, A_g \rightarrow B}{A_1 \land A_2, \ldots, A_g \rightarrow B}.
\]

By the induction hypothesis there is an \( m_0 \in \mathcal{K} \) so that if \( x_j \) \( K \)-realizes \( A_j(\bar{a}) \) and \( IS_1^2 \vdash A_j(\bar{a}) \) for \( 1 \leq j \leq g \) then \( \phi_{m_0}(\bar{x}, \bar{y}) \) \( K \)-realizes \( B \). Define \( g \) to be the \( \Pi_1 \)-function so that
\[
g(x) = \begin{cases} 
\phi_{o, h}(x, z) & \text{if } x = \phi_{o, z} \\
\phi_{\sigma_1, x_1} & \text{if } x = \phi_{\sigma_1, \sigma_2, z_1, z_2} \\
0 & \text{otherwise}
\end{cases}
\]

Define \( m \) to be the Gödel number of the function defined by
\[
\phi_{m}(\bar{x}, \bar{y}) = \phi_{m_0}(g(x_1, x_2, \ldots, x_g, y_1))
\]

Then \( \phi_{m} \) is an extended \( \Pi_1 \)-functional and satisfies the desired conditions.

**Case (3).** (\( \lor \)-left). Suppose the last inference of \( P \) is
\[
\frac{A_0, A_2, \ldots, A_g \rightarrow B}{A_0 \lor A_1, A_2, \ldots, A_g \rightarrow B}.
\]

Let \( m_0 \) and \( m_1 \) be the numbers given by the induction hypothesis so that if \( p = 0 \) or \( 1 \) and if \( x_j \) \( K \)-realizes \( A_j(\bar{a}) \) and \( IS_2^1 \) proves \( A_j(\bar{a}) \) for all appropriate \( j \), then
\( \sigma_\mu(\langle x_1, x_2, \ldots, x_k, \bar{n} \rangle) \) \( K_1 \)-realizes \( B(\bar{n}) \). Recall that if \( x \ \mu \)-realizes \( A_0(\bar{n}) \cup A_1(\bar{n}) \) then either \( x = \langle 0, x' \rangle \) where \( \text{Witness}_1^1 \langle x, \bar{n} \rangle \) or \( x = \langle \langle 0, \tau_1, \tau_2 \rangle, \langle 0, x'_1, x'_2 \rangle \rangle \) where \( \tau_1 \neq \tau_2 \) \( K_1 \)-realizes \( A_{p-1}(\bar{n}) \) where \( p \) is 1 or 2 depending on whether \( \tau_0 \) is zero or non-zero. Define \( m \in \mathbb{N} \) so that

\[
\sigma_m(\langle x_1, \bar{n} \rangle) = \begin{cases} 
\sigma_0 \left( \langle s_0(x_1, \bar{n}), x_2, \ldots, x_k, \bar{n} \rangle \right) & \text{if } h(x_1, \bar{n}) = 0 \\
\sigma_1 \left( \langle s_1(x_1, \bar{n}), x_2, \ldots, x_k, \bar{n} \rangle \right) & \text{otherwise}
\end{cases}
\]

where

\[
h(\sigma, \bar{n}) = \begin{cases} 
\delta(1, x) & \text{if } \sigma = \langle 0, \tau_1, \tau_2 \rangle \\
1 & \text{if } \sigma = 0 \text{ and } \text{Witness}_1^1 \langle \delta(2, x), \bar{n} \rangle \\
0 & \text{otherwise}
\end{cases}
\]

and, for \( i = 1, 2, \)

\[
\sigma_i(\langle 0, \bar{n} \rangle) = \begin{cases} 
\langle 0, \delta(i+1, x) \rangle & \text{if } \sigma = \langle 0, \tau_1, \tau_2 \rangle \\
\langle 0, \delta(1, x) \rangle & \text{if } \sigma = 0
\end{cases}
\]

It is not hard to see that \( \sigma_m \) satisfies the conditions of Theorem 1; indeed, whenever \( x_1 \)
\( K_1 \)-realizes \( A_0(\bar{n}) \cup A_1(\bar{n}) \) then either \( h(x_1, \bar{n}) = 0 \) and \( \sigma_0(x_1, \bar{n}) \) \( K_1 \)-realizes \( A_0(\bar{n}) \) or \( h(x_1, \bar{n}) \neq 0 \) and \( \sigma_1(x_1, \bar{n}) \) \( K_1 \)-realizes \( A_1(\bar{n}) \).

**Case (4), (3) left.** Suppose the last inference of \( P \) is

\[
\frac{A(x_0), A_2, \ldots, A_k}{(\exists x) A(x), A_2, \ldots, A_k}
\]

where the free variable \( x_0 \) appears only as indicated. By the induction hypothesis, there is an \( m \in \mathbb{N} \) so that whenever \( A(x_0, \bar{n}) \) and \( A_j(\bar{n}) \) are provable by \( IS_2^i \), \( x \) \( K_1 \)-realizes
$A(n, \mathcal{A})$ and $x_k$ $K_1$-realizes $A_k(\mathcal{A})$ for $2 \leq k \leq d$, then $\phi_{m_0}(\langle \xi, n_0, \mathcal{A} \rangle)$ $K_1$-realizes $B(\mathcal{A})$.

If $x$ $K_1$-realizes $(\exists x)(A(x, \mathcal{A}))$, it must be the case that $x = \langle <o, \sigma>, <\xi, x_2> \rangle$ where $<\sigma, x_2>$ $K_1$-realizes $A(\xi, \mathcal{A})$ and $IS^1_2 \vdash A(\xi, \mathcal{A})$. Define $g$ and $h$ to be $\Pi^0_2$-functions so that

$$g(\langle <o, \sigma>, <\xi, x_2> \rangle) = <\sigma, x_2>$$

and

$$h(\langle <o, \sigma>, <\xi, x_2> \rangle) = x_1.$$  

Let $m$ be the Gödel number of the function defined by

$$\phi_m(\langle \xi, n_0 \rangle) = \phi_{m_0}(\langle g(x_1), x_2, \ldots, x_d; h(x_1), n_0 \rangle).$$

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

**Case (5).** When the last inference of $P$ is an $(\exists x)$-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 $\Sigma^b_1$. We leave the details to the reader.

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

$$\frac{\lambda(x), \lambda_2, \ldots, \lambda_d \rightarrow \alpha}{(\forall x) \lambda(x), \lambda_2, \ldots, \lambda_d \rightarrow \alpha}.$$  

The induction hypothesis is that there is an $m_0 \in \mathbb{N}$ so that if $A(t(\mathcal{A}), \mathcal{A})$ and all of $A_k(\mathcal{A})$ are $IS^1_2$-provable and if $x_k$ $K_1$-realizes $A(t(\mathcal{A}), \mathcal{A})$ and $x_k$ $K_1$-realizes $A_j(\mathcal{A})$ for $2 \leq k \leq n$, then $\phi_{m_0}(\langle \xi, n_0 \rangle)$ $K_1$-realizes $B(\mathcal{A})$. Recall that if $x$ $K_1$-realizes $(\forall x)(A(x, \mathcal{A}))$ then $x$ is $\langle <o, \sigma>, x \rangle$ where for all $n_0$, $\phi_{n_0}(\langle 0 \rangle) K_1$-realizes $A(n_0, \mathcal{A})$. Define $m \in \mathbb{N}$ so that
\[ \varphi_m(<z, \pi>) = \begin{cases} \varphi_0(\varphi_z(t(\pi)), x_2, \ldots, x_d; \pi) & \text{if } x_1 = \varphi, z \\ 0 & \text{otherwise} \end{cases} \]

**Case (7).** (\(\forall z\) 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 inductively \(\Sigma^b_i\). We leave the details for the reader.

**Case (8).** (\(\forall z\) left). Suppose the last inference of \(P\) is

\[
\begin{array}{c}
A_1, \ldots, A_d \rightarrow B \\
\neg B, A_1, \ldots, A_d \rightarrow \neg B
\end{array}
\]

As we remarked above, this case is trivial since \(\text{IS}^4_{\pi}\) is consistent.

**Case (9).** (\(\forall\) right). Suppose the last inference of \(P\) is

\[
\begin{array}{c}
A_1, \ldots, A_d \rightarrow B \\
A_1, \ldots, A_d \rightarrow B \lor C
\end{array}
\]

Let \(\varphi_0\) be an extended \([P]_n\)-functional satisfying the induction hypothesis. Let \(g\) be a \([P]_m\)-function so that

\[ g(<\tau, y>) = <<0, \tau, 0, 0, 0, 0>>. \]

So if \(x K_\pi\)-realizes \(B(\pi)\), then \(g(x) K_\pi\)-realizes \(B(\pi) \lor C(\pi)\). Finally let \(m\in W\) be the Gödel number of the function

\[ \varphi_m(<z, \pi>) = g(\varphi_0(<z, \pi>)). \]

**Case (10).** (\(\forall\) right). Suppose the last inference of \(P\) is
\[ A_1, \ldots, A_n \rightarrow B_1 \quad A_1, \ldots, A_n \rightarrow B_2 \]
\[ \quad A_1, \ldots, A_n \rightarrow B_1 \land B_2 \]  

Let \( \phi_{m_1} \) and \( \phi_{m_2} \) be extended \( \Box^i \)-functionals satisfying the induction hypothesis for the left and right upper sequents, respectively. Define \( g \) to be a \( \Box^i \)-function so that
\[ g(\langle \tau_1, \tau_2 \rangle, \langle \tau_2, \tau_1 \rangle) = \langle \langle \tau_1, \tau_2 \rangle, \langle \tau_2, \tau_1 \rangle \rangle. \]

So if \( x_1 \) and \( x_2 \) \( K_i \)-realize \( B_1(\bar{n}) \) and \( B_2(\bar{n}) \), respectively, then \( g(x_1, x_2) \) \( K_i \)-realizes \( B_1(\bar{n}) \land B_2(\bar{n}) \). So let \( m \) be the Gödel number of the function defined by
\[ \phi_m(\langle \tau_3, \bar{n} \rangle) = g(\phi_{m_1}(\langle \tau_2, \bar{n} \rangle), \phi_{m_2}(\langle \tau_1, \bar{n} \rangle)). \]

**Case (1).** (3:right). Suppose the last inference of \( P \) is
\[ A_1, \ldots, A_n \rightarrow B(x) \]
\[ A_1, \ldots, A_n \rightarrow (\exists x) B(x) \]

The induction hypothesis is that there is an extended \( \Box^i \)-functional \( \phi_{m_0} \) so that if \( x_j \) \( K_i \)-realizes \( A_j(\bar{n}) \) and \( IS^1_2 \vDash A_j(\bar{n}) \) for \( 1 \leq j \leq n \) then \( \phi_{m_0}(\langle \tau_2, \bar{n} \rangle) \) \( K_i \)-realizes \( B(t(\bar{n}), \bar{n}) \). Of course, these conditions imply \( B(t(\bar{n}), \bar{n}) \) is \( IS^1_2 \)-provable. Let \( m \) be the Gödel number of the function defined by
\[ \phi_m(\langle \tau_3, \bar{n} \rangle) = g(\phi_{m_0}(\langle \tau_2, \bar{n} \rangle), t(\bar{n})). \]

where \( g \) is a \( \Box^i \)-function such that

27
\[ g(\langle \tau, \gamma \rangle, z) = \langle \langle 0, \tau \rangle, \langle z, \gamma \rangle \rangle. \]

It is easy to verify that \( \#_m \) satisfies the desired conditions.

**Case (13).** The case where the final inference of \( P \) is an \((\exists \xi\text{:left})\) inference is very much like Case (11).

**Case (13).** (V:right). Suppose the last inference of \( P \) is

\[
\frac{\Lambda_1, \ldots, \Lambda_k \rightarrow \exists \xi \phi(x)}{\Lambda_1, \ldots, \Lambda_k \rightarrow (\forall x) \exists \xi \beta(x)}
\]

where the free variable \( c_0 \) appears only as indicated. By the induction hypothesis, there is an extended \([1]_P\)-function \( \#_{m_0} \) such that whenever \( x_i = \langle \xi, \gamma \rangle \) \( K_i \)-realizes \( A_0(\xi) \) and \( \text{IS}^1_2 \) proves \( A_0(\xi) \) for \( \xi \in \mathcal{F} \), then \( \#_{m_0}(\langle \xi, n_0, \vec{n} \rangle) \) \( K_i \)-realizes \( B(n_0, \vec{n}) \). Let \( p_0 \) be a suitable polynomial which bounds the runtime of \( \#_{m_0} \).

Define \( m \) to be the Gödel number of the function defined by

\[
\#_m(\langle \xi, \vec{n} \rangle) = \langle 0, r \cdot \pi, \lambda n_0 \#_{m_0}(\langle \xi, n_0, \vec{n} \rangle) \rangle
\]

where

\[
r = p_0 \cdot \text{runtime}(\langle \xi, \vec{n} \rangle)
\]

\[
\pi = \text{p-type of } \#_{m_0}(\langle \xi, 0, \vec{n} \rangle)
\]

and \( \lambda n_0 \#_{m_0}(\langle \xi, n_0, \vec{n} \rangle) \) is the Gödel number of the Turing machine which computes the function

\[
r_0 \mapsto \#_{m_0}(\langle \xi, n_0, \vec{n} \rangle).
\]

28
It is clear that $\sigma_m$ is an extended $L_1^0$-functional by Proposition 3. Also it is readily seen that $\sigma_m$ satisfies the desired conditions of Theorem 1.

**Case (14).** The case where the last inference is a $(\forall x_0)$-right inference is handled similarly to Case (13) and we omit the details.

**Case (15).** (Cont.). Suppose the last inference of $P$ is

$$\frac{A_1, \ldots, A_n \rightarrow C, C, A_1, \ldots, A_n \rightarrow B}{A_1, \ldots, A_n \rightarrow B}.$$  

By the induction hypothesis there are extended $L_1^0$-functionals $\sigma_{m_0}$ and $\sigma_{m_1}$ so that if $x_j K_j$-realizes $A_j(\overline{n})$ and $IS_{L_1^0}^1 A_j(\overline{n})$ for $1 \leq j \leq \delta$, then $\sigma_{m_0}(\overline{x_0, \overline{n}})$ $K_j$-realizes $C(\overline{n})$, and so that when in addition $x_0$ $K_j$-realizes $C(\overline{n})$ then $\sigma_{m_1}(\overline{x_0, \overline{n}})$ $K_j$-realizes $B(\overline{n})$. (Note that if $IS_{L_1^0}^1$ proves $A_j(\overline{n})$ for all $j$, then $C(\overline{n})$ is $IS_{L_1^0}^1$-provable.)

So we define $m$ so that

$$\sigma_m(\overline{x, \overline{n}}) = \sigma_{m_1}(\overline{x_0, \overline{n}}, \overline{x_1, \overline{n}}).$$

**Case (16).** (H2c,b-PIND). Suppose the last inference of $P$ is

$$\frac{A_1, \ldots, A_n \rightarrow B(1/2 c_0, \overline{n}) \rightarrow B(c_0)}{A_1, \ldots, A_n \rightarrow B(0) \rightarrow B(c)}.$$

where the free variable $c_0$ appears only as indicated and $B$ is a hereditarily $L_1^0$-formula.

The induction hypothesis is that there is an extended $L_1^0$-functional so that whenever $x_j K_j$-realizes $A_j(\overline{n})$, $x_0 K_j$-realizes $B(1/2 n_0, \overline{n})$, $IS_{L_1^0}^1 A_j(\overline{n})$ and $IS_{L_1^0}^1 B(1/2 n_0, \overline{n})$, for
First note that if $A_1(\bar{n}), \ldots, A_k(\bar{n})$ and $B(0, \bar{n})$ are $\text{IS}_{2}^{2}$-provable, then $B(0, \bar{n})$ is a theorem of $\text{IS}_{2}^{2}$ for any $n_0 \in \mathbb{N}$. Second, since $B$ is hereditarily $\Sigma_{1}^{b}$, Propositions 6 and 7 assert that there is an extended $[\text{I}_{3}]^p$-functional $\varphi_{m_1}$ such that whenever $x K_{1}$-realizes $B(n_0, \bar{n})$ then $\varphi_{m_1}(\langle x, n_0, \bar{n} \rangle)$ is a $[\text{I}_{3}]^p$-functional of $p$-type $\omega$ which also $K_{1}$-realizes $B(n_0, \bar{n})$. Furthermore, by Proposition 5.3 of [1], we may assume that there is a term $t_B$ in the language of $\text{IS}_{2}^{2}$ such that $\varphi_{m_1}(\langle x, n_0, \bar{n} \rangle) \leq t_B(n_0, \bar{n})$ for all $x$, $n_0$ and $\bar{n}$. Next define $h$ to be the extended $[\text{I}_{3}]^p$-functional so that

$$h(\langle x, n_0, \bar{n} \rangle) = \varphi_{m_1}(\varphi_{m_0}(\langle x, n_0, \bar{n} \rangle)).$$

So $h$ has all the properties of $\varphi_{m_0}$ mentioned above and in addition $h(\langle x, n_0, \bar{n} \rangle)$ is of $p$-type $\omega$ and is less than or equal to $t_B(n_0, \bar{n})$.

Define the function $g$ inductively by

$$g(\langle x, x_0, 0, \bar{n} \rangle) = h(\langle x, x_0, 0, \bar{n} \rangle)$$

$$g(\langle x, x_0, n_0, \bar{n} \rangle) = h(\langle x, x_0, t_{B}(n_0, \bar{n}), \bar{n} \rangle).$$

It is clear that when $x_0 K_{1}$-realizes $A_{0}(\bar{n})$, $\text{IS}_{2}^{1}$ proves $A_{0}(\bar{n})$, $x_0 K_{1}$-realizes $B(0, \bar{n})$ and $\text{IS}_{2}^{1}$ proves $B(0, \bar{n})$ for all $1 \leq x \leq z$, then $g(\langle x, n_0, \bar{n} \rangle)$ $K_{1}$-realizes $B(n_0, \bar{n})$. Also, $g(\langle x, x_0, n_0, \bar{n} \rangle)$ is always less than or equal to $t_B(n_0, \bar{n})$. Now define $m$ to be the Gödel number of the function defined so that

$$\varphi_{m}(\langle z, x_0, \bar{n} \rangle) = g(x, x_0, 1(\bar{n}), \bar{n}).$$

30
It remains to check that $\theta^*_m$ is an extended $[P^1_1]$-functional. But this follows from the fact that $g$ was defined by limited iteration (see [1]) from the extended $[P^1_1]$-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. ■

87. 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 $IS^{1}_2 \vdash (\exists y)A(y, \bar{z})$. Then there is a formula $B(a, \bar{z})$ such that $IS^{1}_2$ proves the following three formulae:

1. $(\forall y)(\forall \bar{x}([B(y, \bar{z})\supset A(y, \bar{z})])$  
2. $(\forall y)(\forall \bar{x}((\forall \bar{x}([B(y, \bar{z})\supset B(a, \bar{z})]) \supset y = z))$  
3. $(\forall \bar{x}((\exists y)B(y, \bar{z})))$.

As in [1], when $n \in \mathbb{N}$ let $I_n$ be a closed term in the language of $IS^{1}_2$ so that the value of $I_n$ is $n$ and so that $S^1_n$ can $\Sigma^0_1$-define the (polynomial time) function mapping $n$ to the Gödel number of $I_n$. When $\bar{x}$ is a vector then $I_{\bar{x}}$ 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.** Suppose $IS^{1}_2$ proves $(\exists y)A(y, \bar{z})$. Then there exist polynomial time functions $f$ and $g$ so that for all $\bar{a} \in \mathbb{N}^k$, $f(\bar{a})$ is the Gödel number of an $IS^{1}_2$-proof.
of $\text{A}_{\text{SIS}_2^1}$. 

Let $\text{Prf}_{\text{SIS}_2^1}(w,v)$ be the $\Delta^1_1$-defined predicate of $S_2^1$ which asserts that $w$ is the Gödel number of an $\text{SIS}_2^1$-proof of the formula with Gödel number $v$ [1]. We strengthen Conjecture 2 as:

**Conjecture 2 (i≥1).** Suppose $\text{SIS}_2^1$ proves $(\exists y)\forall (y,z)$. Then

$$S_2^1 \vdash (\forall z)(\exists y)(\exists w)\text{Prf}_{\text{SIS}_2^1}(w,\text{A}_{\text{SIS}_2^1},L,z).$$

It is not likely that Conjectures 2 and 3 can be directly generalized for arbitrary $i>1$. Indeed, the generalizations obtained by substituting $\text{IS}_2^1$ for $\text{SIS}_2^1$, $S_2^1$ for $S_2^1$, and $P_i$ for "polynomial time" imply that $\text{NP} = \text{co-NP}$ 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 $\text{SIS}_2^1$ in a different way.)

**ACKNOWLEDGEMENTS**

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


