Free-Variable Theories

by

Daniel Guy Schwartz

B.A., Portland State University, 1969

A Thesis Submitted in Partial Fulfillment of

The Requirements for the Degree of

Master of Science

In the Department

of

Mathematics

Simon Fraser University

April 1973

Approval

Name: Daniel Guy Schwartz

Degree: Master of Sceince

Title of Thesis: Free-Variable Theories

Examining Committee:

Chairman: Norman Reilly

____

Steven K. Thomason
Senior Supervisor

____

Harvey Gerber

____

David Ryeburn

____

Brian Alspach
External Examiner

Date Approved: April 19, 1973

Abstract

A *free-variable theory* is a first-order theory without quantifiers, plus a rule of substitution for individual variables, and possibly, with some "nonlogical" rules of proof. The idea arose from Goodstein's equation calculus $\mathcal{R}$ of Primitive Recursive Arithmetic (*Recursive Number Theory*, 1957). In Chapter 1 we survey the subject, starting with Skolem (1923). Chapter 2 defines "free-variable theory", and discusses two theories, A and A^-, of arithmetic, and a certain *formalization*, R, of $\mathcal{R}$, all of which have mathematical induction as a rule of proof. A has the axiom $1\neq 0$. *Theorem*: A^- "represents" R. A, A^- and R, hence $\mathcal{R}$, are incomplete and undecidable. For $\mathcal{R}$, undecidability is new. It is notable that, within A, Goodstein's "logical constants" are equivalent to the classical logical connectives. Chapter 3 is a semantical analysis. Validity in structures is watered down from the first-order case. *Models* are structures that validate the theorems of a theory; *strong models* further validate the rules. These provide the *usual* and *strong semantics*. A semantics is *adequate* for a theory T if, whenever P is a nontheorem, there exist models of that kind for T which invalidate P. *Theorem*: The usual semantics is adequate for all free-variable theories. This is along the lines of Henkin's well-known proof having structures built of closed terms, but

must differ in case some theory with nonlogical rules is such that either it is without constants, or the deduction theorem fails. Our proof succeeds by means of some Δ-canonical structures, which are new. Next we bear down on some admissible theories, and prove the theorem: The strong semantics is adequate for all admissible theories. This uses the former theorem, and it can be applied to show that the strong semantics is adequate for the theories A and A^-. The former theorem can be applied to show that the open theorems of an open first-order theory are exactly the theorems on a naturally corresponding free-variable theory. It is open whether a theory for which the strong semantics is adequate can have models that are not strong.

Dedication

to my father

Guy W. Schwartz

Acknowledgements

Here I would like to express my gratitude to some of those who have contributed to the production of this work. I am indebted to my supervisor, Dr. S. K. Thomason, for his inimitable patience, and for making himself available with advice and encouragement, which was always administered in the correct way and amount.

Prof. A. H. Lachlan I will thank for many helpful comments and suggestions. In particular, he mentioned the undecidability problem, and eventually stated both the lemmas that are involved in its solution.

And thanks are also due to Drs. Harvey Gerber and David Ryeburn for pointing out myriads of technical, grammatical and typographical errors in an earlier draft of the text. The author of course assumes the responsibility for whatever errors remain.

This work was begun during the summer semester of 1970 under the auspices of a Simon Fraser University President's Research Grant; and since then, it has been supported in part by the National Research Council of Canada.

Table of Contents

Errata

Page 59,line 8 : After "formula" put "such that no two members have the same (n+1)-th formula".

Page 80, line 2 from bottom: After "holds" put ", if there is one, and 0 if there is not".

It might have been well to define a rule of proof to be <u>on</u> a language L when each of its instances is in L. For this would eliminate the need for some circumlocution and, in particular, after "rule" in line 11,page 95 one could put "on L', which happens to be implied there by the definitions, but is worth emphasizing.

Introduction

This writing grew out of R. L. Goodstein's monograph, *Recursive Number Theory, A Development of Recursive Arithmetic in a Logic-Free Equation Calculus*. It was during my earliest searchings for a thesis topic that I chanced on the library copy of this book, and found it interesting. The thesis began with Steve Thomason's suggestion to "modernize" Goodstein's presentation, that is, to supply the equation calculus with a precise language consisting of specific terms and formulas, to restate its rules of proof in this context, and to report its properties.

Of course, the primary justification for such a project is that the material to be presented is worthy of review. In this regard there are three main points of interest: (i) Even though the calculus does not postulate any of classical logic, a substantial amount of elementary number theory can be derived from it. Notably one can prove the unique prime factorization theorem (sometimes called the fundamental theorem of arithmetic) and that every pair of numbers has a least common multiple. More exactly, the calculus postulates the defining equations of the primitive recursive functions, and its rules of derivation enable one to exhibit a binary primitive recursive function φ such that $\varphi(a,1),\ldots,\varphi(a,n)$ (some n) are the prime factors of a, and such that $\varphi(a,x) = 0$ if $x > n$, and a binary primitive recursive function ψ such that $\psi(a,b)$ is the least common multiple of a and b. Thus, in other words, in some significant cases, even though one cannot establish the usual first-order assertion, he can establish one of its quantifier-free equivalents, i.e. one of its Skolem forms. (Anyone who is unfamiliar with this terminology is referred to Shoenfield [39].)

(ii) Some analogues of the logical connectives are introduced, merely as a way of abbreviating certain equations, and many of the usual logical properties and interrelations are derived. For example, $E \to^* E'$ abbreviates a certain equation which is built out of the equations E and E', and it turns out that if both E and $E \to^* E'$ are derivable, then so is E', so that the rule of modus ponens is valid. Thus one has a semblance of the propositional calculus definable within the equation calculus.

(iii) The principle of generalized induction is derivable, and the calculus is incomplete in the sense that there is an equation $G(x) = 0$ which is not derivable, but is such that $G(n) = 0$ is derivable for every n. Thus it turns out that the calculus is an example of a system with weaker expressional strength and with stronger rules of proof than first-order number theory, which is nevertheless incomplete in precisely the same sense.

A modernization is warranted, mainly because of the kind of vagueness that pervades the entire monograph. Upon examination, this vagueness appears to stem from the practice of employing "signs" without distinguishing clearly between their formal and informal usage. For example, where it is said that F is some function, this sometimes means that the letter "F" is the sign of some function, and sometimes it means that the letter "F" is a metasymbol that denotes some function sign. Thus, in the early parts of the book, it is not clear whether the rules of derivation are thought to be operations on equations of functions, or on strings of signs, or both.

Later on in the book, when the calculus is "codified", it is clear that there the rules of derivation are operations on strings of signs. However, in that section one encounters another difficulty. A new phrase, "recursive term", appears without explanation; and it is not made explicit until the last chapter that "function" also includes numbers, considered as constant functions, and variables, considered as identity functions, and that "recursive function" and "recursive term" are synonymous. Moreover, in this last chapter the calculus is supplied with a precise language after all, which finally makes it clear that a sign is properly analyzed as a symbol, together with a fixed meaning.

At first sight, that the monograph even considers signs, rather than symbols, which were certainly well-known at the time of publication, is strange. But it turns out that this is done for a definite purpose. By assuming that each function symbol in the language of the system is the sign of a distinct primitive recursive function, a major step in the proof of the system's incompleteness can be eliminated. Under these conditions, there is no need to establish that every primitive recursive function is "represented" in the system. How this happens is discussed in Chapter 1 of this thesis.

Yet, in another vein, it seems strange that the concept of "a sign" as "a symbol with a fixed interpretation" is not presented earlier, so that the calculus could be introduced at the outset with a language and some clear notion of "function" and "recursive term". Apparently, the reason for this is grounded in a philosophical view of mathematics as a "developing" body of knowledge, which is being advanced. For one could reason that the naive idea of a sign is known to anyone who is familiar with the methods of mathematics, and that the formal notion becomes clear when it is needed. Since this philosophy is touched on in Chapter 1, let it only be said here that a manner of presenting these views that does not detract so severely from the intelligibility of the mathematical work, would be preferable.

But the fact remains that the information therein is worthy of attention. Hence it becomes a service to make the monograph more accessible to the students and working mathematicians of today. However, in the process of writing this thesis, that project has become submerged in a study of much wider scope, and which grew out of the author's idea of writing primitive recursive arithmetic as a system that is not logic-free, but rather postulates the propositional calculus and the axioms for equality. This idea immediately gave rise to the more general notion of a "free-variable theory", and thereafter the question of a"completeness theorem for free-variable theories" soon followed. The author's supervisor recognised that these ideas could be well worth pursuing, and encouraged him to do so.

Recently, the author discovered that, except for the semantical analysis, these ideas are not new. It turns out that, as early as 1936, Hilbert and Bernays introduced some "elementary free-variable calculi" for the purpose of formalizing the original primitive recursive arithmetic, which was introduced by Skolem; and surprisingly enough, their "calculus" is almost exactly the theory of arithmetic A, that is discussed in this thesis. Their work went only so far, however, so that most of the related results of the present work are an extension of their investigation.

Briefly, a free-variable theory is a first-order theory (as in Shoenfield [39]) without quantification, but with a rule of substitution for individual variables, and possibly, with some further "non-logical" rules of proof. Free-variable theories are so called because the variables occurring in any formula are not "bound" by any quantifiers. The reasons for adding the logical rule of substitution are (i) that it is needed, and (ii) that by eliminating quantifiers in a first-order theory, one also eliminates the "existential introduction rule", so that the substitution rules cannot be derived.

The reason for considering nonlogical rules is of a more fundamental nature. Later on it is demonstrated that, except perhaps in some very unusual cases, nothing can be gained by adding further rules of proof to a first-order theory, that can't also be had by adding some axioms instead. This is not true about free-variable theories. For suppose that P and Q are some quantifier-free formulas in which the only variable that occurs is x. It is well-known that there is no free-variable formula which is semantically equivalent to $\forall xP \rightarrow Q$, even though $\forall xP$ is semantically equivalent to P. However, the statement "if $\forall xP$ is valid, then Q is valid" means the same as the statement "if P is valid, then Q is valid", so that $\forall xP \rightarrow Q$ is semantically equivalent to the rule "from P infer Q". It follows that, in a free-variable theory, this rule cannot be replaced by a set of axioms without some loss.

In this thesis, the main example of a nonlogical rule is one of mathematical induction: from $P(0/x)$ and $P \rightarrow P(Sx/x)$ infer P (where P is any free-variable formula, 0 denotes the constant zero symbol, S denotes the successor function symbol, and $P(\ldots/\_\_)$ denotes the formula that is obtained from P by replacing each occurrence of __ with an occurrence of ..., if there are occurrences of __, and which is just P if there are not). It is clear that this rule is semantically equivalent to the collection of axioms of the form $P(0/x)\&\forall x(P\rightarrow P(Sx/x) \rightarrow P$ where P is quantifier-free, and irrespective of whatever other variables occur in P.

Of course, this is not to say that one can obtain a free-variable theory that is semantically equivalent to any given first-order theory. For there clearly is no free-variable equivalent of a formula of the form ∃xP, unless perhaps in special cases, such can be built into a free-variable theory by some other means.

Since nonlogical rules are considered, there arise two semantics for free-variable theories. In both semantics, "validity in a structure" is just the natural watering down of "validity in a structure for a first-order language". In one semantics, a structure for the language of a theory is a model of that theory if it has the usual property of validating the theorems (derivable formulae) of that theory. In the other, a structure is a model when it validates both the theorems and the rules, where a rule is valid if all inferences by it from valid hypotheses, yield valid conclusions. Respectively, these are called the "usual semantics" and the "strong semantics" for free-variable theories.

A chapter by chapter survey of this thesis now follows. Chapter 1 is an historical survey of primitive recursive arithmetics, and in which Goodstein is reviewed. Very little of this chapter is used in the thesis proper, and the reader who is interested in getting straight to the mathematics is advised to begin with Chapter 2. Then in Section 2.3 he should refer back to pages 19-22 for a few definitions, and thereafter only refer to Chapter 1 as indicated in the proof of Lemma 3 of Theorem 2.2.

The purpose of the first section of Chapter 2 is to lay down some notations and terminology. §2.2 presents a definition of "free-variable theory" and some associated notions, such as consistency and completeness, and records some elementary theorems which carry over with only slight modifications from the literature on first-order theories.

The third and last section of Chapter 2 is a study of two theories of arithmetic: the theory A of Peano arithmetic, and the theory A^- of primitive recursive arithmetic. Both theories have the defining equations of the primitive recursive functions as axioms, and mathematical induction as a nonlogical rule. They differ only in that A has the formula $1 \neq 0$ as an axiom, while A^- does not. A number theoretic function is "representable" in a free-variable theory under a definition that approximates the well-known one due to Gödel. Theorem 2.1 is that a function is representable in A and A^- if and only if it is primitive recursive. This theorem enables one to see that a certain "formal system" of primitive recursive arithmetic R uniquely formalizes Goodstein's equation calculus (denoted $\mathcal{R}$). Theorem 2.2 shows that an equation (in effect, a logic-free formula) is provable in A^- exactly if it is provable in R. An immediate consequence is that A^- thereby inherits many of the known properties of $\mathcal{R}$. In particular, A^- is incomplete.

The third theorem demonstrates that, within the theory A, every formula is equivalent to an equation; or more exactly, for each formula P of the language of A, there is a term t such that the formula $P \leftrightarrow t=0$ is provable in A. An interesting interpretation of this theorem might be that the logical connectives and their aforementioned primitive recursive analogues (herein called "logical constants") are equivalent in A; for where P and t are the above, t = 0 is an equivalent of the equation that is abbreviated by the expression that is obtained from P by replacing each logical connective by the corresponding logical constant.

A constructive consistency proof for A and A^- is presented in Theorem 2.4. The proof is recorded mainly because of its striking simplicity in comparison with similar proofs for some first-order theories.

Theorem 2.5 states that A is incomplete, and Theorem 2.6 states that A, A^- and R are undecidable. The proofs of these results begin by establishing that there is a primitive recursive enumeration of the defining equations of the primitive recursive functions, which is surprising since it is well-known that there is no primitive recursive enumeration (in the sense of Péter [33]) of these functions. The fact that certain systems of primitive recursive arithmetic are undecidable is established by Kreisel [29]; but the fact that R is undecidable is new since it deals with a system that has infinitely many axioms.

Chapter 3 is the semantical analysis. The first section deals mainly with the definition of "model" and "strong model". The two main results appear in §3.2. A semantics is "adequate for" a theory T, if for each formula P in the language of T that is not a theorem of T, there is a model of T in that semantics which invalidates P.

The first main result is Theorem 3.1: The usual semantics is adequate for all free-variable theories. The proof of this theorem is along the lines of Henkin's well-known proof of the completeness theorem for first-order theories, wherein a model for a theory T is built out of the closed terms in the language of T, but is more difficult in the case that there are no closed terms, that is, if T does not contain a constant. For if T has nonlogical rules, an extension that is obtained by adding a constant need not be "conservative". The difficulty is circumvented by means of some Δ-canonical structures, for which there need only be open terms, such as variables. These structures are new, and were defined by Steve Thomason for the purposes of this result.

It turns out that the strong semantics is not adequate for all free-variable theories. In an effort to bear down on the class of theories for which the strong semantics is adequate, some conditions on the nonlogical rules of a theory are introduced, and some collections of "admissible theories" and "weakly admissible theories" are described.

The second of the main results is that the strong semantics is adequate for all admissible theories. This is Theorem 3.5. Theorem 3.2 is a technical result about the conditions on non-logical rules. Theorems 3.3 and 3.4 lead up to Theorem 3.5. The former states some criteria under which a theory has a complete simple extension, and the second says that a consistent weakly admissible theory has a strong model. Theorem 3.6 shows that A and A^- are admissible theories.

Theorem 3.7 is an application of Theorem 3.1. The main point is the corrolary which says that the open theorems of an open first-order theory are exactly the theorems of the free-variable theory having the same nonlogical axioms. It turns out that Theorem 3.1 is a consequence of Theorem 3.7, and that the latter theorem can be proved by other means. Theorem 3.8 is an appication of Theorem 3.5 to the study of proofs in systems consisting of an open first-order theory with nonlogical rules. This theorem tells when a formula might have an "open proof".

Perhaps the most important question to be opened up but left unanswered by this thesis is whether a theory for which the strong semantics is adequate has any models that are not strong models. The question is interesting in light of the fact that A and A^- are admissible theories, and hence are theories for which the strong semantics definitely is adequate.

In the pages that follow, it is clear that the rule of mathematical induction is a primary motivating example, and that this is because its role in a proof cannot be duplicated by any set of axioms. It should be said that the only rules with this property that the author has uncovered so far, are other forms of induction, for example, the rule for induction on the elements of a tree.

It turns out, however, that other kinds of rules can be of interest, even in the first-order case, as a means of replacing infinite sets of axioms. An example that is discussed in §3.2

is the rule which expresses the duality principle in Lattice Theory. Another example is in the methods of Church [6] for eliminating all but finitely many of the axioms of primitive recursive arithmetic by incorporating the procedures of defining functions by substitution and primitive recursion as rules of proof.

Nevertheless, a question has often occurred to this writer about the worthwhileness of an extensive treatment of the general concept of free-variable theories with non-logical rules, when few interesting examples are known. It happens that the basis for continuing this work has been the likelihood that further such examples would appear, and that in truth, few have. However, it does not yet seem reasonable for this likelihood to be denied. For now, the author rests in the satisfaction that his work pre-empts some of the problems in the event that further examples be discovered. At the very least, that study sheds new light on the more general relationship of axioms and rules.

On the other hand, free-variable theories without non-logical rules are plentiful. Worth mentioning is that, due to Birkhoff's characterizations in [2] (a handier reference is Grätzer [22]), each equational class is uniquely determined by a set of equations which can serve as the axioms for a theory of that class. It turns out, in fact, that there is a one-to-one correspondence between free-variable theories and open first-order theories. In each case, the correspondent is the theory with the same non-logical axioms, and whose language differs only in that it either has or does not have quantifiers.

Proof theorists may be interested to note that the above correspondents are as described in Theorem 3.7. For by Skolem's Theorem (see [39]), this means that the consistency of any first-order theory can be reduced to that of the correspondent of some open conservative extension, thereby simplifying the consistency proof.

In this thesis, definitions, theorems and propositions are numbered-with respect to the chapters, and irrespective of the sections, with different kinds of entries being listed separately. Propositions are numbered only when it is useful for future reference. With the exception of Definitions 2.1 and 2.3, all numbered definitions and theorems are thought to be new, at least in the present context. The two exceptions are the aforementioned things whose essential parts were recently found in Hilbert and Bernays [26]. Names of theorems that are underlined are taken from some well-known theorems about first-order theories, of which all but one are in [39]. The unique readability theorem was taken from some notes for an undergraduate course in mathematical logic that was given by Steve Thomason. Names of theorems that are enclosed in parentheses are suggestions by the author.

The usual practice of underlining a word group to indicate that it is being defined for the purposes of the work is adhered to. A not so ordinary use of parentheses is to enclose a part of such a group to indicate that it is to be understood when only the other part is written. In Chapter 1, quotation marks are used to set off a word group that is being defined just for the purposes of that chapter. In these cases, the definition is usually being taken from Goodstein [16].

The double arrow "$\Leftrightarrow$" is used to abbreviate the phrase "if and only if". When an "$\Leftrightarrow$" assertion is being proved, the beginning of the "only if" part is sometimes indicated by $\Rightarrow$, in which case the beginning of the "if" part is indicated by $\Leftarrow$. More frequently, "$\Rightarrow$" is used simply to abbreviate "implies". The end of each proof is marked by an oblong: $\square$.

The thesis is thought to be self-contained. But it should be worth mentioning that the reader will find this writing much less cryptic if he first becomes acquainted with [39].

The author is indebted to many people for their suggestions, criticism and encouragement. But to more than anyone, he owes Steve Thomason, not only for the advice and encouragement, rebuffs, admonishments, interest and enthusiasm in his service as a supervisor, without which this thesis surely would not have been written, but also for many things beyond what would normally be expected from one in his official capacity, and which clearly distinguishes him as a friend. This writer is hard pressed for words to express his appreciation.

Chapter 1

A Survey of Primitive Recursive Arithmetics

> The beginning of all things lies still in the beyond in the form of ideas that have yet to become real.
>
> From the Wilhelm/Baynes translation of the *I Ching*

The first primitive recursive arithmetic was introduced by Thoralf Skolem in 1923. Today, it is folklore that this treatise [40], grandiosely entitled "The Foundations of Elementary Arithmetic Established by means of the Recursive Mode of Thought without the Use of Apparent Variables Ranging over Infinite Domains", was slow to gain more than a sideways glance from the current intelligentsia: "Is it necessary to prove that the elementary arithmetical operations exist? Moreover, even if one can seriously doubt that they exist, Skolem has not proved this. Clearly, all that has been accomplished is to define the functions in terms of some other functions whose existence might be subjected to the same scrutiny."

Now this opinion prevailed for a while, and could well have remained, had it not been for a remarkable property of those "more elementary" functions. Without a doubt, given any argument for such a function, one can compute the value in finitely many mechanical steps.

Eight years later, these "recursive" functions had a major part in Gödel's famous proof [12] (1931) of the existence of undecidable propositions in Russell and Whitehead's Principia Mathematica [38]. Now called the "primitive recursive" functions, they were eventually to admit a generalization to the (general) recursive functions (due to Gödel [13] (1934), on a suggestion of Herbrand), subsequently to become the foundation of an entirely new field of "effective computability", and thereby find their way into the heart of modern computer technology and the theory of finite automata.

As it happens, some of these functions had previously been considered by Dedekind [10] in 1888, and the first few had been defined by Peano [32] in 1889. But Skolem was first to exploit their full capacity for providing a foundation for arithmetic. Let us begin by giving a brief review of this work.

Starting with the successor function which, for each n, takes the value n+1, one can define more and more functions (and predicates) in a recursive fashion, and many of their properties can be established by means of the principle of mathematical induction. The first function so described is addition: since a+1 is defined for all a, in order to define a+b generally, one need only say, for each b, how it is defined at b+1, assuming that it is already defined at b. Simply, he sets $a+(b+1)=(a+b)+1$. In words: The sum of a and the successor of b is the successor of the sum of a and b. A typical example of a "recursive proof" is the proof by induction on c that $a+(b+c)=(a+b)+c$ for all a,b,c. By these means, Skolem was able to introduce enough functions and predicates to state and prove the fundamental theorem of arithmetic,"Up to the order of factors, every number can be uniquely written as a product of primes",and furthermore the facts that every pair of numbers has a least common multiple and a greatest common divisor.

As a system, the resulting arithmetic is a "quantifier-free" equation calculus. Proofs are conducted in the "naive arithmetic" and the "naive propositional calculus", yet stylistically approach the careful formality of the strictly syntactical arguments in [38]. Of particular importance is the introduction of the new concept of a "bounded quantifier". In contrast with the unbounded quantifiers, these are introduced simply for the purpose of abbreviating certain primitive recursive predicates. For example, $\Sigma_{1}^{a}{}_{x}(a=bx)$ is taken as an abbreviation of (a=b)or(a=2b)or···or(a=ab), and thus says that there exist x such that $1 \leq x \leq a$ and a=bx. (Note that this furthermore says that a is divisible by b.) Perhaps the single most important aspect of the"recursive mode of thought" is its ability to capture the intuitive content of the existential quantifier in a great many cases.

The concept of an apparent variable had been elucidated earlier by Russell. As an explanation, in the above example, the variable x is apparent in contradistinction with a and b, which remain fixed throughout some given context. More precisely, the assertion is made for "each" choice of a and b, for "all" x such that $1 \leq x \leq a$. The distinction is aptly viewed as one of a pseudo-temporal priority. Since all primitive recursive functions are finite valued, it is clear that the "a" in this example may be replaced by any one of these without upsetting the requirement that apparent variables range over finite domains only.

Skolem also introduced a bounded universal quantifier, $\Pi_{1^x}^{a}$ (for all x such that $1 \leq x \leq a$), and a new operator, Min(P(x),a), which yields, for each a, the least x such that $1 \leq x \leq a$ and the predicate P holds for x, if there is one, and yields 1 if there is not. This latter is now written $\mu x \leq a P(x)$ and is known as the "bounded μ-operator". Its unbounded version is shown by Kleene [27] (1936) to be a key to the general recursive functions.

Independently of Brouwer's school of intuitionism, Skolem's restriction to finite domains had denied the classical equivalence of the unbounded $\Sigma_x P(x)$ and $\overline{\Pi_x \overline{P(x)}}$ (it is not the case that for all x, not P(x)) when refering to infinite domains. Skolem's system is not intuitionistic, however. For in some places where intuitionism does admit quantification, the full expressional strength of the quantifier cannot be acheived primitive recursively. This is mainly because bounded quantifiers cannot be introduced as abbreviations unless a bound is established within the arithmetic itself. For example, one cannot introduce a statement of the negation of Fermat's Last Theorem: $\Sigma_x \Sigma_a \Sigma_b \Sigma_c (x > 2 \text{ and } a^x + b^x = c^x)$.

The first precise definition of the primitive recursive functions is due to Gödel [12]. Before going any further, let's see what these functions are, and consider a few of the more elementary ones. The following formulation is taken from Hermes [25].

Throughout this thesis, the natural numbers include 0 (zero). For each natural number x, x' denotes the next greater, and is called the <u>successor of</u> x. The <u>primitive recursive</u> functions are as follows:

(i) the <u>successor function</u> S defined by $S(x)=x'$, the constant <u>zero function</u> Z defined by $Z(x)=0$ and, for each i and n, the n-ary <u>identity function</u> I_i^n defined by $I_i^n(x_1,\ldots,x_n)=x_i$ are primitive recursive,

(ii) if G is an m-ary primitive recursive function, and $H_1,\ldots,H_m$ are n-ary primitive recursive functions, then $S_m^n(G,H_1,\ldots,H_m)$ (which is abbreviated $S_m^n(G,H_i)$) defined by

$$S_m^n(G,H_i)(x_1,\ldots,x_n)=G(H_1(x_1,\ldots,x_n),\ldots,H_m(x_1,\ldots,x_n))$$

is primitive recursive,

(iii) for $n\geq 1$, if G is n-ary, H is (n+2)-ary, and both are primitive recursive, then $R^n(G,H)$ defined by

$$R^n(G,H)(0,x_1,\ldots,x_n)=G(x_1,\ldots,x_n)$$

$$R^n(G,H)(x',x_1,\ldots,x_n)=H(x,R^n(G,H)(x,x_1,\ldots,x_n),x_1,\ldots,x_n)$$

is primitive recursive.

The functions listed in (i) are <u>initial functions</u>. The S_m^n and R^n are respectively the <u>schemata of definition by substitution</u> and the <u>schemata of definition by primitive recur-</u>

sion. This way of denoting them is found in Kleene [28]. In this thesis, an explicit definition of a function is a definition of it by means of one of these schemata in terms of some other primitive recursive functions which have already been so defined.

In this terminology, x+y has the explicit definition $R^1(I^1_1,H)(x,y)$ where H is $S^3_1(S,I^3_2)$. For upon simplification we have that $0+y=R^1(I^1_2,H)(0,y)=I^1_2(0,y)=y$ and that $x'+y=R^1(I^1_2,H)(x',y)=S^3_1(S,I^3_2)(x,R^1(I^1_2,H)(x,y),y)=S^3_1(S,I^3_2)(x,x+y,y)=S(x+y)=(x+y)'$. In like manner one can devise explicit definitions for $\cdot$ (multiplication) such that $0\cdot x=0$ and $x'\cdot y=x\cdot y+x$, $\dot{-}1$ (predecessor) such that $0\dot{-}1=0$ and $x'\dot{-}1=x$, $\dot{-}$ ((modified) subtraction) such that $y\dot{-}0=y$ and $y\dot{-}x'=(y\dot{-}x)\dot{-}1$, $|,|$ (positive difference) such that $|x,y|=(x\dot{-}y)+(y\dot{-}x)$, and Rt such that $Rt(0)=0$ and $Rt(x')=Rt(x)+(1\dot{-}H(x,Rt(x)))$ where $H(x,y)=(y'\cdot y')\dot{-}x'$. Rt(x) is the greatest y such that $y^2\leq x$.

The characteristic function of a predicate P of n variables is the function K_P defined by $K_P(x_1,\ldots,x_n)=0$ if $P(x_1,\ldots,x_n)$ holds, and $K_P(x_1,\ldots,x_n)=1$ if not. Gödel was also first to point out that a primitive recursive predicate is just one whose characteristic function is primitive recursive. Thus, equality is primitive recursive, since $K_=(x,y)=1\dot{-}(1\dot{-}|x,y|)$. Since = is primitive recursive, it turns out that every equation of primitive recursive functions describes a primitive recursive predicate. It follows that any P may be viewed simply as an abbreviation of certain equations, e.g. $K_P(x)=0$.

Some equations for ≤, <, ≥ and > will appear later on.

Today, there are several formulations of primitive recursion. It appears that the most elegant one is due to Péter [33] where it is proved that one needs only S, Z and the unary identity function as initial functions, the schemata S^n_m and the schema R^1 of definition by primitive recursion with one parameter. Gödel's formulation differs from Péter's by admitting recursions in any finite number of parameters. Hermes' differs from Gödel's by including the I^n_i among the initial functions. Both of Shoenfield [39] and Kleene [28] also include, for each n and q, the n-ary constant function C^n_q defined by $C^n_q(x_1,\ldots,x_n)=q$. Any of [39], [28], and especially [33] are good sources regarding primitive recursion in general.

Hilbert and Bernays treated Skolem's arithmetic in [26] (pg. 307). Their main interest in it was that its proofs are 'finitary" and hence easily formalized, and that its "constructive" consistency proof is simple. Excepting some points of detail in the following Definition 3.3 (§2.3), their formalization of this arithmetic is the free-variable theory A. In particular it postulates the sentential calculus (a close relative of the propositional calculus in §2.2), the axioms for equality (§2.2), the defining equations of the primitive recursive functions, the formula 0≠0', and both substitution for individual variables (§2.2) and mathematical induction as rules of proof. Its quantifier-free language contains the classical logical connectives: ~ (not, <u>negation</u>), v (or, <u>disjunction</u>),

& (and, conjunction), → (implies, implication) and ↔ (if and only if, (logical) equivalence).

In [12], Gödel states that there is a primitive recursive function γ such that, for all numbers a and b, $\gamma(a,b)=0$ if and only if $a=b$. (γ is the positive difference function.) It follows that in Skolem's system, every equation is equivalent to an equation of the form $t=0$, where t is some recursive term (see the following). Hilbert and Bernays showed that in their formalization, every equation is logically equivalent to an equation of this form. By introducing some primitive recursive analogues of the above logical connectives, this enabled them to further prove that every formula of their formalization is logically equivalent to such an equation, and subsequently to arrive at the first explicit definition of the bounded quantifiers and the bounded μ-operator. A slightly different version of these analogues, the same explicit definitions of the bounded quantifiers, and essentially the same explicit definition of the bounded μ-operator will be discussed.

In this chapter we shall examine a constructive consistency proof which is along the lines of Hilbert, but for a different system. Let us note here that "verifiability" and its related notions, though implicit in [40], are in fact due to Hilbert and Bernays. In Theorem 2.4 we shall see what amounts to Hilbert's proof for the above system. There this is compared with a similar, more well-known proof, which is due to Gödel. For what is meant by a "constructive" proof, the reader is referred there and to the remarks at the end of §2.1.

[26] summarizes all the major developments out of Skolem's treatise prior to 1934. In particular there is Ackerman's [1] (1928) enumeration of the hierarchy of arithmetical operations as an example of a "doubly recursive" function (see the following) that is not primitive recursive, and Péter's work on reductions to primitive recursion and the elimination of parameters (most recently published in [33].)

In 1941 the first "logic-free" arithmetics were introduced simultaneously and independently by Goodstein [15] (printed in 1945) and Curry [9]. These are significant, not just because they demonstrate how the arithmetic can be developed without logical considerations, naive or otherwise, but also because they show that, to a certain degree, elementary logic can be founded in elementary arithmetic. Both [15] and [9] present analogues of the logical connectives which differ from one another and from Hilbert's only with respect to negations. It turns out that this difference is crucial. Hilbert needs the axiom $\sim(0=0')$ for making his definition. In Curry's system the primitive recursive negation of $0=0'$ is derivable. In Goodstein's system it is not.

Goodstein's version leaves open another case, and it is the only one with which we shall be concerned. For want of a better name, we shall follow him in [16] by calling the analogues the "logical constants". They are presented in a review of [16] to which we now turn.

The introduction is a short essay on the nature and definition of numbers, the definition and formalization of counting, and the concept of a formal system. Chapter I introduces the aforementioned elementary primitive recursive functions, and the aforementioned doubly recursive function, provides Gödel's formulation of primitive recursion, and indicates the natural generalization to multiple recursion. To avoid having to reformulate the primitive recursive functions in §2.3, let us here assume the foregoing due to Hermes. From what follows, it becomes clear that, for the purposes of Goodstein's monograph, this can be done without loss.

Primitive recursive functions are also called "singly recursive". In [16], a definition of the doubly recursive functions is obtained from the definition of the primitive recursive by replacing "primitive" by "doubly" throughout, and adding another case (where to conserve space let us assume that there are no parameters)

(iv) if G is unary, H_1 is binary, H_2 is unary, H_3 is quaternary, H_4 is ternary, and all are doubly recursive, then $R_2^0(G, H_1,\ldots,H_4)$ (which is abbreviated $R_2^0(G,H_i)$) defined by

$$R_2^0(G,H_i)(0,y)=G(y)$$

$$R_2^0(G,H_i)(x',0)=H_1(x,R_2^0(G,H_i)(x,H_2(x)))$$

$$R_2^0(G,H_i)(x',y')=H_3(x,y,R_2^0(G,H_i)(x,H_4(x,y,R_2^0(G,H_i)(x',y))),$$
$$R_2^0(G,H_i)(x',y))$$

is doubly recursive.

Further such generalizations yield the rest of the multiply recursive functions. In [16] these latter are called simply "recursive functions". To avoid confusion, let us note with Kleene [28] that these are not likely to include all those that are known by that name today.

Chapter II introduces a nonformal equation calculus of these recursive functions. It is described completely by a definition of "proved equation" which shall be quoted. Before doing so, however, let us digress to explain the notion of a "sign". This explanation is not in [16], but is hoped to clarify what is vague there. It will be of value to us for describing the formal system R in §2.3.

The following proceeds by comparing signs with "symbols". For what is meant by the latter, the reader can go to the remark at the end of §2.1 and the first few paragraphs of §2.2.

Suppose that we are given some mathematical object, say a function. Then, for the purpose of talking about it, we may allot to it a sign, say F, and agree that F will "denote" that function throughout the context of the discussion. This is the informal use of signs that is common thoughout mathematics. Usually it would not cause alarm to just say that F "is" the function. Yet signs can be found to have a formal aspect. To do this, one simply distinguishes them from the objects they denote, and considers them as things in themselves, i.e., as independently existing. Doing this enables one to speak of "concatenating" signs or "strings" of signs, "replacing" signs by other signs, and so on.

On the other hand, symbols are just objects, mere things, and hence are apriori formal. In fact, for these, the name "symbol" is slightly misleading; for such an object doesn't symbolize anything unless, by fiat, one supplies it with something. When this is done, the latter object is a "meaning" or "interpretation", and the symbol is said to be "interpreted".

Moreover, all this applies to any array of signs (or symbols) considered as a unit, that is, considered as having an interpretation (or various interpretations) of its own, which may or may not be dependent on the interpretations of its components. It is a practice also to call an array of signs a sign, but not to call an array of symbols a symbol. Goodstein adheres to this practice, and so shall we.

Thus, evidently, a sign is a symbol or an array of symbols considered as having an interpretation which remains fixed throughout some discussion. Another way of saying this is that a sign is an ordered pair whose first member is a symbol or an array of symbols, and whose second member is an interpretaition. For example, in [16] the "numerals" denoted 0, S0, SS0,... are in fact the ordered pairs (0,zero),(S0,one),(SS0,two),... with S and 0 taken as symbols.

Notice that the sign S is of the successor function, and that the sign 0 is of the number zero, while the sign S0 is of the value of the successor function for the argument zero.

In [16] it further happens that the signs F and F(x), say, denote the same function, while F(0) denotes that function evaluated at zero, but not the value. This latter distinction is the well-known one of "intention" versus "extension".

In the following definition of proof the letters F, G and H are metavariables that denote function signs. (For what is meant by a "metavariable" the reader can go to the aforementioned discussion of symbols and note that the letters x,y,P,Q, etc. are such kinds of variables.) "F is a function" means that F denotes either a numeral (viewed as denoting a constant function whose value is the interpretation of that numeral), a variable sign (viewed as denoting the unary identity function of the interpretation of that sign), or an expression built up of numerals, variable signs, and function signs that "makes sense", i.e., that denotes a specific function of a certain number of variables, or such a function evaluated at some arguments. It is understood that the same function may be denoted by different signs.

A 'proof' is a table of equations each of which is either (part of) the definition of a function, or an equation of the form F=F, or is a 'proved' equation. If F=G is one of the equations of a proof, then a proved equation is obtained by replacing the function F by the function G at one or more places at which F occurs in some equation of a proof.

Furthermore, the equation formed by replacing a variable at all the points at which it occurs in some equation of a proof, by another variable, or by a definite numeral or function, is a proved equation.

Finally, F=G is a proved equation if equations of a proof are obtained by substituting the function F for a function H, and by substituting the function G for H, in the equations which define the function H. [16, p. 27]

This last rule of proof can also be expressed by saying that F=G if F and G "satisfy the same introductory equations". In effect, this asserts that any function defined by means of one of the schemata S_m^n and R_m^n is unique. For example, the equations 0+y=y and Sx+y=S(x+y) define addition "so that any F(x,y) which satisfies the same equations", namely F(0,y)=y and F(Sx,y)=SF(x,y), "is just another notation for the same function"[16, p. 28].

The first project is to establish within this calculus, some elementary properties of +, $\cdot$ and $\dot{-}$, and prove "the key equation" $x+(y\dot{-}x)=y+(x\dot{-}y)$. The proof of this latter equation uses the above "equalizing rule" in an application to the defining equations of a doubly recursive function. It should be pointed out that this is the only place in the subsequent proofs (Chapter IV) of the fundamental theorem of arithmetic and the theorem on least common multiples that anything other than a single recursion is involved. Precisely, the equation's single use is to establish that, for any functions F and G, the equations F=G and $|F,G|=0$ are derivable from one another.

Once this is done, three functions Σ_F, Π_F and μ_F are explicitly defined and discussed. $\Sigma_F(n)$ and $\Pi_F(n)$ are the familiar finite sum and finite product, sometimes written $\sum_{x=0}^{n}(F(x))$ and $\prod_{x=0}^{n}(F(x))$. $\mu_F(n)$ is the least $m \le n$ such that F(m)=0 if there is such m, and is 0 if there is not. Then the inequalities $\ge$ and $\le$ are introduced by taking $x \ge y$ as an abbreviation of the equation $x=y+(x\dot{-}y)$, and taking $x \le y$ as an abbreviation of $x=y\dot{-}(y\dot{-}x)$. The strict inequalities > and < are obtained respectively by putting Sy in for y in the former, and Sx in for x in the latter. A discussion of their properties is followed by a proof of the calculus' "freedom from contradiction".

Briefly, the latter is as follows. The sign of a function $F(x_1,\ldots,x_n)$ is "totally eliminable" if, for each sequence $N_1,\ldots,N_n$ of numerals, there is exactly one numeral N such that the equation $F(N_1,\ldots,N_n)=N$ is provable. Another way of expressing this is to say that, for each sequence N_1, $\ldots,N_n$, $F(N_1,\ldots,N_n)$ is "reducible" to a unique numeral. It is easy to see that Z and the I_i^n are eliminable. It is proved that the property of eliminability is inherited through the processes of definition by substitution and definition by primitive recursion. Thus the sign of every primitive recursive function is eliminable. An equation F=G is "verifiable" only if F and G are the same numeral,or if each substitution of numerals for the variables in the equation yields an equation F'=G' such that F' and G' are reducible to the same numeral. By showing that the axioms are verifiable, and that an application of a rule of proof to verifiable hypotheses yields a verifiable conclusion, one has that every provable equation is verifiable. Hence the equation S0=0 is not provable.

Without explaining how any contradiction is involved, Goodstein stops here, apparently taking this to mean "freedom from contradiction". More correctly, this implies "freedom from contradiction" in the sense that no equation is such that both it and its primitive recursive negation (see the following) are provable. What remains to be pointed out is that, if the calculus were not free from this kind of contradiction, then every equation would be provable.

Chapter III begins by introducing the "logical constants": for all equations F=F' and G=G',

$\sim^*(F=F')$ abbreviates $1 \dot{-} |F,F'|=0$

$(F=F')\&^*(G=G')$ abbreviates $|F,F'|+|G,G'|=0$

$(F=F')\vee^*(G=G')$ abbreviates $|F,F'|\cdot|G,G'|=0$

$(F=F')\rightarrow^*(G=G')$ abbreviates $\sim^*(F=F')\vee^*(G=G')$

$(F=F')\leftrightarrow^*(G=G')$ abbreviates $((F=F')\rightarrow^*(G=G'))\&^*((G=G')\rightarrow^*(F=F'))$.

All equations are "formulas". If F and G do not contain variables, the formula is a "proposition". Otherwise it is a "propositional function". Formulas will be denoted by P or Q, or by p, p(x), p(x,y), and so on, according to the number of variables.

Let F=G be a proposition. Then F=G is a "true proposition" if $|F,G|=0$ is provable, and a "false proposition" if $|F,G|>0$ is provable. Every proposition is either a true or a false one. Since every provable equation is verifiable, no proposition is both true and false. A formula $p(x_1,\ldots,x_n)$ is "true for the values" $N_1,\ldots,N_n$ if $p(N_1,\ldots,N_n)$ is a true proposition, and "false for the values" if not.

Since, for all F and G, F=G and $|F,G|=0$ are derivable from one another, a proposition is true if and only if it is provable. Hence, it follows that under this notion of truth, the logical constants generate the same truth tables as the logical connectives.

The following things are known: (i) For all F and G, $F=G\leftrightarrow*|F,G|=0$ is a proved equation. [16] points this out only for F and G variable-free, a case which follows by the above definition of truth. The fact for all F and G is more complicated. Let H denote the function $||1\dot{-}|F,G|,0|\cdot||F,G|,0|,0|$ and let H' denote $||1\dot{-}||F,G|,0|,0|\cdot|F,G|,0|$. Then the foregoing equivalence is $H+H'=0$. It is certainly the case that $0+0=0$ and $||x,y|,0|=|x,y|$ are proved equations. So the desired result follows easily with the aid of $(1\dot{-}x)\cdot x=0$, which may be found in the problem section for Chapter III.

(ii) If $P\leftrightarrow*P'$ and $Q\leftrightarrow*Q'$ are provable, then all of $\sim*P\leftrightarrow*\sim*P'$, $P\&*Q\leftrightarrow*P'\&*Q'$, $P\vee*Q\leftrightarrow*P'\vee*Q'$, $(P\rightarrow*Q)\leftrightarrow*(P'\rightarrow*Q')$ and $(P\leftrightarrow*Q)\leftrightarrow*(P'\leftrightarrow*Q')$ are provable.

(iii) The principle of "tertium non datur", or "the excluded middle", $P\vee*\sim*P$, is provable. The principle of "non-contradiction", $\sim*(P\&*\sim*P)$, is provable. (This latter does not in itself mean that the calculus is free from contradiction in the sense we mentioned earlier, but can be used to prove it.)

(iv) All formulas of the form $(x_1=y_1\rightarrow*\cdots\rightarrow*(x_n=y_n\rightarrow*(p(x_1,\ldots,x_n)\rightarrow*p(y_1,\ldots,y_n)))\cdots)$ are provable. ([16] states this for only n=1, but the rest follows by repeated applications.)

(v) The schema

$$\frac{P,\ P\rightarrow*Q}{Q}$$

of "modus ponens" is valid. That is, if P and $P \to^* Q$ are provable, then so is Q.

(vi) The schema

$$\frac{p(0), p(x) \to^* p(Sx)}{p(x)}$$

of "mathematical induction" is valid.

(vii) The schema (where F is any binary function)

$$\frac{p(x,0), p(F(x,y),y) \to^* p(x,Sy)}{p(x,y)}$$

of "generalized induction" is valid.

(viii) The following "Deduction Theorem": "If the equation A=B is derivable...from an hypothesis F=G (i.e. an unproved equation) and if the derivation does not involve substitution for the variables in the hypothesis, then $(F=G) \to^* (A=B)$ is derivable".

The bounded quantifiers ("limited universal and existential operators") are defined by letting $A_x^n(F(x)=0)$ stand for the propositional function $\Sigma_F(n)=0$, and letting $E_x^n(F(x)=0)$ stand for $\Pi_F(n)=0$. The "minimal operator" is defined by letting $L_x^n(F(x)=0)$ stand for $\mu_F(n)$. These operators are now defined generally simply because every equation is equivalent to an equation of the form $F(x_1,\ldots,x_n)=0$. (It is clear that the foregoing F may well have additional variables.)

It turns out that, for each n, the equation abbreviated by $A_x^n(F(x)=0)$ is equivalent to the equation abbreviated by $F(0)=0 \&^* \cdots \&^* F(n)=0$ and that the equation abbreviated by $E_x^n(F(x)=0)$ is equivalent to the one abbreviated by $F(0) \vee^* \cdots$

$\vee$*F(n)=0. This fact is interesting, and perhaps useful. However, this author finds it strange that Goodstein offers these equivalences to "justify" the reading of A_x^n as "for all x from 0 to n", and the reading of E_x^n as "for some x from 0 to n". For surely, if the sum of n numbers is 0, then all are 0, and if the product of n numbers is 0, then at least one is 0.

The logical constants, bounded quantifiers, and the bounded μ-operator, together facilitate defining the notion of a prime number, and subsequently proving the two theorems of number theory that were mentioned earlier. Chapter IV is devoted mainly to this. Even with these abbreviations to aid the intuition, the proofs are complicated and long.

The chapter concludes by introducing a new operator, N_x^n, called the "counting operator". N_x^n(F(x)=0) is the number of solutions of the equation F(x)=0 as x varies from 0 to n. The given proof that N_x^n does indeed have this property contains a proof of the formula $(x>n)\vee^*(x\leq n)$, which requires an application of the equalizing rule to a double recursion. It becomes clear that this is the reason that Goodstein merely presents this operator, and does not refer to it in the following pages of his book.

Chapter V presents $\mathcal{R}$, discusses it, and then reduces it to an equivalent system $\mathcal{R}^*$. Alternatively, $\mathcal{R}$ is called a "formalization" and a "codification of primitive recursive arithmetic". In the context of this thesis, the latter is more suitable, since $\mathcal{R}$ falls short of being a formal system in the sense of §2.3, in that it lacks a precisely described language.

The definition of $\Re$ makes use of the notion of a "recursive term", a notion which, as was said in the introduction, is used synonomously in [16] with "recursive function". For this reason, the intended meaning has been incorporated into the foregoing description of "a function", which should suffice for the present discussion. Precisely, a recursive term is a term of the language of the formal system R that is defined in §2.3 of this thesis.

Besides F, G and H, we shall also have A, B and C denote recursive terms. F(x) denotes a recursive term in which the variable sign x occurs. F(A) denotes the term obtained from F(x) by replacing the variable sign x by the term A.

The axioms of $\Re$ are the defining equations of the primitive recursive functions only. ([16] does not say this exactly. It is clear that $\Re$ does not include the equations F=F. But the use of terminology there does not explicitly rule out the inclusion of the multiply recursive functions. However, the fact that it's called a system of "primitive" recursive arithmetic, together with further comments and the work in Chapter VIII, imply that indeed it is intended to formalize only the primitive recursive part of the foregoing equation calculus.)

The rules of inference are given by the substitution schemata

$$Sb_1 \qquad \frac{F(x)=G(x)}{F(A)=G(A)}$$

$$Sb_2 \qquad \frac{A=B}{F(A)=F(B)}$$

$$T \qquad \frac{A=B, A=C}{B=C};$$

and the schema of the "primitive recursive uniqueness rule"

$$U \qquad \frac{F(Sx)=H(x,F(x))}{F(x)=H^x(F(0))}$$

where H^x is defined by the primitive recursion $H^0(y)=y$ and $H^{Sx}(y)=H(x,H^x(y))$. The function H is to be a function of not more than two variables, and in Sb_1, a term H in which x does not occur may be taken in place of G(x) provided it is also taken in place of G(A).

About this Goodstein says: "The novelty of this codification lies in the derivation of the key equation $a+(b\dot{-}a)=b+(a\dot{-}b)$ by means of the primitive recursive uniqueness rule, instead of requiring a doubly recursive equalizing rule as before." This means that except for the properties of the counting operator, all the foregoing proved equations and valid rule schemata are derivable in $\mathcal{R}$. This requires a verification of course, to which the following several pages of [16] are devoted.

For future reference, let us record here that U is equivalent to the schema

$$U_1 \qquad \frac{\begin{matrix} F(0)=G(0) \\ F(Sx)=H(x,F(x)) \\ G(Sx)=H(x,G(x)) \end{matrix}}{F(x)=G(x)}$$

where the same agreement is made regarding H. One can show that U_1 is equivalent to the schema of mathematical induction.

The system $\mathcal{R}^*$ is obtained by some reductions of the schema

U. Precisely, $\mathcal{R}^*$ has, instead of U, the schema

$$E \qquad \frac{F(0)=0,\ F(x)=F(Sx)}{F(x)=0}$$

and the key equation $x+(y \dot{-} x)=y+(x \dot{-} y)$ as an axiom, and instead of the defining equations of the predecessor function, the axiom $Sx \dot{-} Sy = x \dot{-} y$. The reason for wanting to consider $\mathcal{R}^*$ becomes clear in Chapter VIII.

Chapter VI is concerned with reductions to primitive recursion. Here it is shown that certain kinds of multiply recursive functions have explicit (primitive recursive) definitions.

Chapter VII deals with elimination of the parameters $x_1, \ldots, x_n$ in the schema of definition by recursion. This is done by first setting $J(u,v)=(u+v)^2+u$ and demonstrating (i) that J assigns a unique number to each pair (u,v), and (ii) that there are primitive recursive U and V such that, if $z=J(u,v)$ for some u and v, then $U(z)=u$ and $V(z)=v$. Repeated applications of this enables the elimination of all parameters but one. Elimination of the last requires further tricks which we shall not go into.

These reductions and eliminations are due to Péter (see [33]). After Péter, Goodstein uses this material to establish the following fact: Given the defining equations of the functions +, $\dot{-}$, $\cdot$ and Rt, all the primitive recursive functions can be obtained by means of the schemata S_1^1 and S_2^1 of definition by substitution, and the <u>iteration schema</u> It for defining functions of one variable: $It(F)(0)=F(0)$, $It(F)(Sx)=F(It(F)(x))$

(in [16] the reading is closer to $It(F)(x)=F^x(0)$. [16] mentions, but does not use what is also due to Péter, that one needs just the functions + and E where $E(x)=x\dot{-}(Rt(x))\cdot(Rt(x))$.)

This result enables one to define a doubly recursive function $\varphi_m(n)$ that enumerates all the one variable primitive recursive functions. Exactly, for each primitive recursive function F of one variable, there is an m such that $\varphi_m(n)=F(n)$ for all n. The complicated definition of $\varphi_m(n)$ will be omitted. This function is not primitive recursive; for if it were, then the function ψ defined by $\psi(n)=\varphi_n(n)+1$ would be included among the φ_m, which is not the case.

The main purpose of Chapter VIII is to show that $\mathcal{R}^*$, and hence the equivalent system $\mathcal{R}$, is incomplete in the sense that there is a primitive recursive function G such that the equation $G(x)=0$ is verifiable, but not provable in $\mathcal{R}^*$. This is to be proved along the lines of Gödel [12], which requires first of all, that the system have a precisely described language, and secondly, that there be an assignment of "Gödel numbers" to the elements of this system (signs, sequences of signs, terms, formulas, sequences of formulas, proofs) such that the predicate Pr(m,n), which holds exactly if m is the Gödel number of a sequence of formulas, n is the number of the last member of this sequence, and the sequence is a proof, is a primitive recursive predicate.

It turns out that the proof in [16] contains an error, but that the error is reparable. A minor point is that the system $\mathcal{R}^*$ to be proved incomplete is similar to, but not the same as, the earlier $\mathcal{R}^*$. Nor is it an equivalent system, since one of the axioms is the defining axiom of a doubly recursive function. For clearness' sake let us call this system $\mathcal{R}^+$.

Without making the error of [16], $\mathcal{R}^+$ is as follows: Its language consists of the variable signs $m, n, x_1, x_2, \ldots$, and the function signs $\varphi, \varphi_0, \varphi_1, \ldots$ together with the signs $+$, $\dot{-}$ and $\cdot$ (φ_3 is the sign of Rt). (The interpretation of the sign φ is the function $\varphi_m(n)$.) Its axioms are the equation $m+(n\dot{-}m)= n+(m\dot{-}n)$, the equation $Sm\dot{-}Sn=m\dot{-}n$, the defining equations of $+$, $\dot{-}$ and $\cdot$, and the defining equation of the function $\varphi_m(n)$ (henceforth written $\varphi(m,n)$) only. Its proof schemata are just those of $\mathcal{R}^*$. Since $+$, $\dot{-}$, $\cdot$ and the φ_m are signs for all of the primitive recursive functions, everything derivable in $\mathcal{R}^*$ is derivable in $\mathcal{R}^+$.

The error in [16] is simply that the sign of the function $\varphi_m(n)$ was omitted. This has the consequence that in the subsequent Gödel numbering, this function, and hence its defining axiom, is not assigned a number. Thus, adding φ and writing $\varphi_m(n)$ as $\varphi(m,n)$ so that it can be assigned a number, is the first step towards a remedy. The remedy is completed by makimg the following alterations in the Gödel numbering that is already established in [16]: Assign φ any unused number, say 0. Renumber the signs $\varphi_0, \varphi_1, \ldots$ by assigning to each φ_i the number of the expression $\varphi(N_i, n)$ where N_i is the Gödel number of the i-th numeral. Build into the predicates $S_1(x,y)$ (which says that y is the number of an equation that is derivable by Sb_1 from the equation with number x) and $S_2(x,y)$ (which says similarly for Sb_2) the provision that, if x is the number of the defining axiom of $\varphi(m,n)$, then the object put in for the variable sign m must be a numeral. This will ensure that, with respect to the Gödel numbering, the defining axiom for this function can enter into a proof only for the purpose of yielding the definition of some φ_i. The reader may check for himself that the "proof predicate" Pr of [16] now becomes what is needed for the ensuing proof.

It is part of the Gödel numbering to define a function St such that $St_e(v/n)$ is the number of the expression that is obtained by substituting the n-th numeral for the variable with number v in the expression with number e (assuming n, v and e are such that this is possible). The following is a slightly different rendering of the concluding paragraphs of the incompleteness result (now for $\mathbb{R}^+$).

$\sim$*$Pr(m,St_n(19/n))$ is a primitive recursive predicate of the two variables m and n. Hence it may be viewed as an abbreviation of some equation of primitive recursive terms, which contain the variable signs m and n only. Let p be the Gödel number of this equation. Then $St_p(19/p)$ is the Gödel number of the equation that is obtained from it by substituting the p-th numeral for the variable sign with number 19, which is the sign n. It follows that this latter equation is abbreviated by $\sim$*$Pr(m,St_p(19/p))$.

Let G be the sign of the characteristic function of $\sim$*Pr(m,St_p(19/p)). We have pointed out that any primitive recursive predicate is introducible as an abbreviation of an equation of primitive recursive terms. At one point the incompleteness proof in [16] uses something which amounts to: if P is a primitive recursive predicate of the variable m (only), then one may assume that the equation abbreviated by P is F(m)=0 where the sign F is ———————— the pair (F,K_P). Note that this is true simply because, for all F and G, the equations F=G and |F,G|=0 are derivable from one another; for if P abbreviates F=G, then |F,G| is K_P. Let's assume this for G. Note that we thereby assume that St_p(19/p) is the Gödel number of the equation G(m)=0.

Suppose that G(m)=0 has a proof in $\mathcal{R}^+$. Then on the one hand, this proof has a Gödel number, say k, and Pr(k,St_p(19/p)) holds by the definition of Pr; while on the other hand, the equation G(k)=0 (with k here the k-th numeral) is derivable from G(m)=0 by Sb_2, which means that $\sim$*Pr(k,St_p(19/p)) holds by the definition of "characteristic function". Hence G(m)=0 is not provable in $\mathcal{R}^+$.

Since St_p(19/p) is the Gödel number of G(m)=0, this latter fact is expressible by saying that $\sim$*Pr(k,St_p(19/p)) holds for all k. So G(k)=0 for all k, by the definition of "characteristic function". This implies that the equations G(0)=0, G(S0)=0,... are derivable in $\mathcal{R}^*$; for $\mathcal{R}^*$ is equivalent to $\mathcal{R}$, and it is known that in $\mathcal{R}$ every variable-free term is reducible to a unique numeral, and that only verifiable equations are provable. Moreover, since every equation that is derivable in $\mathcal{R}^*$ is also derivable in $\mathcal{R}^\dagger$, the equation G(m)=0 is not provable in $\mathcal{R}^*$. Hence $\mathcal{R}^*$ (and so also $\mathcal{R}$) are incomplete in the sense we have described.

Chapter VIII, and the monograph, concludes by establishing Skolem's nonstandard model of arithmetic as a model of $\mathcal{R}$. Here it should be pointed out that (i) $\mathcal{R}$ is assumed to have a precise language, (ii) the signs of this language are extricated from their affixed meanings, and regarded just as symbols. We shall have occasion to go into the construction of this model in §3.3, where it is construed as a model of the free-variable theory A.

Regarding the model, we must take issue with [16] on one point. There it is asserted that by exhibiting this model, Skolem showed "that not only systems like $\mathcal{R}$ or $\mathcal{R}^*$, but every formalization of arithmetic fails to characterize the number concept completely and admits as values of the number variables a class of entities of which the natural numbers form only the initial segment". If by "only the initial segment" is meant "a proper initial segment", this assertion is not true. For the second-order theory of Peano arithmetic (see [32]) is categorical, which means that, up to some isomorphic copies (see §3.3), it is modeled by the natural numbers only.

In the introduction we mentioned that there are some apparent reasons for Goodstein's use of signs instead of symbols.

A mathematical reason is that, for the purposes of establishing the foregoing incompleteness result along the lines of Gödel, since $\mathcal{R}$ is a system of primitive recursion, one is thereby enabled to dispense with the "representation theorem" (similar to Theorem 2.1, §2.3) that accompanies such proofs for other systems. For, as was just pointed out, if $P(x_1,\ldots, x_n)$ is primitive recursive, then we may assume that it abbreviates an equation of the form $F(x_1,\ldots,x_n)=0$ where the interpretation of the sign F is the function K_P. Hence every primitive recursive P is automatically "represented" in $\mathcal{R}$.

A philosophical theme is caught up in the words "a development" in the subtitle of the monograph. A quick glance through reveals that, as a system, Recursive Number Theory is taken through four distinct steps. The calculus of Chapter II is nonformal; that is, the formal aspect of the equations as composed of signs, is barely mentioned, so that the proofs in the calculus have a particularly intuitive character. In Chapter V the calculus is cut down to one of primitive recursion, modified with respect to its rules of proof, and formalized as the system $\mathcal{R}$. The desire is to retain (or recover) proofs of the fundamental theorem of arithmetic and the theorem on least common multiples in a system of primitive recursion, to bring out that all the earlier proofs can be formalized, and to demonstrate that most of the proofs carry over directly. One notices that at this step, he begins to consider signs formally.

The next step is taken in Chapter VIII, where a modification (extension) of $\mathcal{R}$ receives a precisely determined language. Here one explicitly distinguishes the sign from its interpretation. The fourth step is where Skolem's nonstandard model is considered, where, as was pointed out, signs are considered as symbols independent of interpretation. At this last step, $\mathcal{R}$ becomes a formal system, precisely in the sense of §2.3.

Thus encapsulated, and depicted here in the examples of symbols and formal systems, is the manner in which a mathematical concept is arrived at through naive implementation giving over to explicit description. In this, there is implicit a philosophical assertion which this author would make as follows: Beginning with root simple concepts, mathematics evolves; and this evolution entails the repeated act of the mathematician of formalizing his role in relation to his subject into the body of his work.

This concludes a review of [16]. Works by Goodstein that are of related interest are [18] and [19] which consider some decidable fragments of $\mathcal{R}$, and [17] which shows that, under a different version of the logical constants, Post's (n+1)-valued logics can be modeled in $\mathcal{R}$. This modeling has not been considered entirely satisfactory, since the deduction theorem does not hold in it.

In [9] Curry showed that with the obvious interpretation, via his version of the logical constants, a formula is provable in Hilbert and Bernays' formalization of primitive recursive arithmetic if and only if its interpretation is provable in his logic-free equation calculus. In Goodstein [21] there appears a system $\mathcal{R}$ which is equivalent to the $\mathcal{R}$ of [16], wherein, via the foregoing logical constants, there is an interpretation of the sentential calculus such that a formula is provable in the sentential calculus if and only if its interpretation is provable in $\mathcal{R}$. ([21] does not say that the $\mathcal{R}$ there is equivalent to the $\mathcal{R}$ of [16], but this can be proved.) A brief summary in [21] of some recent work on recursive arithmetics accounts for the citations in the following paragraph.

For a system T of "ternary arithmetic", which is equivalent to $\mathcal{R}$, Rose [37] proves both of Gödel's incompleteness theorems, and shows that its consistency can be established in an extension T^+ that is obtained by adding the schema of double recursion, or more exactly, the defining equation of the function $\varphi_m(n)$. The method of the first incompleteness result is the one just described for $\mathcal{R}$. In terms of $\mathcal{R}$, the second of these is that, if p is the Gödel number of the equation 1=0, and F is the characteristic function of Pr(m,p), then the equation F(m)=1 which says that $\mathcal{R}$ is consistent, is verifiable but not provable in $\mathcal{R}$. Pozsgay [34] has proved that a weaker system EA of "elementary arithmetic" also satisfies the second incompleteness theorem. Cleave [8] and Rose [37] show that the consistency of EA can be proved in $\mathcal{R}$, and in some weaker systems. The possibility of replacing Sb_2 by finitely many of its instances has been studied by Heath [23]. The subject of "multiple successor arithmetics", which has given rise to the subject of "word arithmetics", was introduced by Vuckovič [45]. This work is furthered by Goodstein [19]. In $\mathcal{R}$, $x+(y\dot{-}x)$ and $x\dot{-}(x\dot{-}y)$ are respectively the greater and lessor of x and y. Partis, a student of Goodstein, has shown that the elements in Vuckovič's system have a vector representation, and that there, the two terms are respectively the least upper bound and the greatest lower bound of x and y, so that the system forms a lattice.

[22] also notes that Church studied a formalization of Skolem's arithmetic as early as 1936 ([4]). We add that he took up the subject again in [5] (1955) and [6] and [7] (1957). The system presented in [6] is an "equation logic" of arithmetic. That is, it also postulates the propositional calculus and some axioms for equality. This system is interesting because, instead of having the defining equations of the primitive recursive functions as axioms, it has only those for the initial functions, and incorporates the schemata for definition by substitution and primitive recursion into its rules of proof. Hence it has only finitely many axioms. [7] examines applications of recursive arithmetic to some problems of circuit synthesis.

Of course, Skolem has returned to the subject repeatedly. The aforementioned nonstandard model appeared in [41] (1933). A record of much of his work has been recorded by himself in [42] (1946). This shall not be gone into, since most of it does not pertain directly to the equation calculus as such.

For much of the historical information, we are in debt to van Heijenoort for his work in [44]. Those references that are reprinted there have been indicated in the bibliography of this thesis. It is worth mentioning that all readings in [44] are in English, even though the original publication may not have been. References that came out of [21] have been so indicated in the foregoing. Some were also found in the bibliography of [16].

Chapter 2

Free-Variable Theories of Arithmetic

The first two sections will set basic terminology and notations, define "free-variable theory" and some related notions, and state some well-known theorems. The third section uses this to define two theories of arithmetic that are then studied at length.

§ 2.1 Preliminaries

The set theory employed in this thesis is standard. A well-known reference is Fraenkel and Bar-Hillel's book [11]. But Monk [31], for example, has the needed information and is more readable. Beyond the usual "naive" set theory, one will require the notion of a proper class. Concerning classes, it is useful to know that every set is a class and that, if some subclass X of a proper class Y happens to be a set, then the complement of X with respect to Y is also a proper class. Most of the relevant notation and terminology has been fixed as follows here.

The empty set is denoted by ϕ. The Greek letter ε and the word "in" are used to indicate (class) membership, $\subset$ is used for inclusion, $\cup$ for union, $\cap$ for intersection, - for complementation (with Y-X for the complement of X with respect to Y), $\{\ldots | \_\_\_\}$ for the set of all ... such that ___, $\{\ldots\}$ for the set of all ..., and sometimes $\{\ldots\}_{i=1}^{n}$ for the set of all ... such that $1 \leq i \leq n$. <u>Sequences</u> are thought of informally as just listings. In almost all cases, they are indexed by the natural numbers. (Ordered) n-tuples are finite sequences of length n, and are distinguished visually by enclosing parentheses. Those n-tuples consisting exclusively of the members of a class X are said to be from X, and the class of all n-tuples from X is denoted by X^n. An n-ary predicate or relation on a set X is a subset of X^n. An n-ary function or mapping from a set X to a set Y is an assignment of an unique member of Y to each member of X^n. Where F is a function, $F(x_1,\ldots,x_n)=y$ will indicate that F assigns the value y to the argument $(x_1,\ldots,x_n)$. In most places, this will serve to define F completely. This can be exemplified here with an application. If F is an n-ary function from X to Y and if $Z\subset X^n$, then F/Z denotes the restriction of F to Z, which is defined by $(F/Z)(x_1,\ldots,x_n)=F(x_1,\ldots,x_n)$ for all $(x_1,\ldots,x_n)\varepsilon Z$. It is worth noting that functions are defined on sets only. It will occasionally be convenient to think of an n-ary function as a set of ordered (n+1)-tuples. The words "unary" and "binary" will replace "1-ary" and "2-ary" and, unless indicated otherwise, "function" and "predicate" standing alone mean that they are n-ary for an arbitrary n. The first infinite cardinal is written $\aleph_0$.

Let X be any class. An n-ary rule on X is an assignment of an unique member of X to each member of some subclass X' of X^n, in effect, a subclass of X^{n+1}. Notice that if X were a set then the rule would just be an n-ary partial function from X to itself. Most of the above notation and terminology for functions extends naturally to rules. In particular, if R is an n-ary rule on X that assigns values only to arguments in X', and if $Y \subset X^n$, the restriction of R to Y, denoted R/Y, is defined by letting $(R/Y)(x_1,\ldots,x_n) = R(x_1,\ldots,x_n)$ for all $(x_1,\ldots,x_n) \varepsilon X' \cap Y$. Notice that R/Y is also a rule on X.

In some treatments, rules are defined to include those taking infinite sequences as arguments. When a distinction is made between rules that are infinitary and finitary, the methods employing such rules are correspondingly so called. And within the context of a formal system, the rules and methods of proof are of concern. This thesis considers only formal systems whose rules of proof are finitary.

If $Y \subset Z$ and ρ is a set of rules on Z, then a class X can be defined by a generalized inductive definition as follows: (i) let $Y \subset X$, (ii) for each R in ρ, if $x_1,\ldots,x_n$ are in X and R assigns a value to $(x_1,\ldots,x_n)$, let $R(x_1,\ldots,x_n)$ be in X, and (iii) let nothing be in X except as required by (i) and (ii). Usually, what Z and ρ are will be determinable from the context. The analogue of (iii) will never be written, but will always be tacitly assumed. An example of how all this can be used was met in Chapter 1 with the definition of the primitive recursive functions. A simpler example will appear shortly.

Where X is defined as above, to show that its members have some property P, one uses a proof by induction on the members of X. He shows that: (i) if $x \varepsilon Y$, then x has the property P, (ii) for each $R \varepsilon \rho$, if $x_1,\ldots,x_n \varepsilon X$ and R assigns a value to $(x_1,\ldots,x_n)$ and each x_i has the property P, then $R(x_1,\ldots,x_n)$ has the property P. The condition that the $x_1,\ldots,x_n \varepsilon X$ and R assigns a value to $(x_1,\ldots,x_n)$ and each x_i has the property P is called the induction hypothesis.

Example. Let $Y=\{0\}$ and let R be the prime function, $\_'$, that yields, for each natural number x, the successor of x. Then a set X of the successors of 0 can be defined by a generalized induction: (i) $0 \varepsilon X$, (ii) if $x \varepsilon X$, then $x' \varepsilon X$. (Notice that here it is implicit that Z is the set of natural numbers.) In this case, "proof by induction" and "induction hypothesis" clearly have their usual meanings.

Remark. As a beginning student of mathematical logic and having to rely primarily on textbooks for his information, this author was more than once distressed by the amount of confusion that characteristically surrounds the simplest and perhaps most important concept in the subject, that of a symbol. To be sure, most writers of textbooks attempt to make this concept clear, but usually through a kind of semi-mathematical and semi-philosophical heurism that includes such words as "concrete" and "abstract", "formalism", "metalanguage", "syntax", "constructive", "interpretation", and so on, and only ends by leaving the reader awe struck or, at best, amid a nebulous heap to sort out for himself. Others will brush the matter aside on the pretext that the idea is obvious and that any one who can't understand it should best ply himself to another trade. Now these people should be reminded that it was several thousand years from the time that numerals were first introduced to the advent of the variable quantity, and several centuries more before the discovery of symbols per se; and that no matter how simple the concept is in retrospect,it is certainly not one that is easily obtained. Still others will begin straightway, saying that what is meant will become clear. But how long is it until the student realizes that the idea is in fact simple and that much of his trouble could have been saved with a few carefully worded paragraphs? After all, if the idea is clear to the author, why doesn't he at least try to make it clear to the student?

After some inquiry the difficulties begin to reveal themselves. First, although there are volumes of philosophical analyses of the nature of ordinary language and its multiplicity of uses, there is no universally accepted rendering of this central idea. Apparently, this is because any completely comprehensive definition must be self-requisite. One cannot define it except by means of itself. Thus, it is frequently taken as basic, and generously explained. Carnap [3] is an example of this. Second, for the purposes of mathematics, it is possible to be precise in a definition. One merely sets aside a collection of independently existing objects and "calls" them symbols. But in doing so he necessarily loses the motivation that initially had been supplied by the philosophical analyses. However, this author will contend that the philosophy should be separated from the mathematics, so that each may be presented in its own light. Further it is claimed that this can be done with sufficient clarity, and moreover, with profit.

Concerning the philosophy, suppose we begin with the following nondefinitions: A "statement" is a sentence that has meaning; where a "sentence" is a concrete, syntactical object that may be thought of as consisting of marks on paper; while a "meaning" is an abstract, semantical object that cannot be written down, but is somehow "bound" to a sentence that "asserts" that meaning. Then a"theory", considered as a body of knowledge, is a collection of statements together with a specified subcollection of"acceptable" statements, and in mathematical theories acceptable statements are called "theorems".

By using this as an overview, one can proceed to the problem. In both philosophy and mathematics, symbols might advantageously be thought of as the marks, but "idealized". The philosopher's symbols are the letters and punctuation of ordinary languages, and are to be distinguished from the actual marks on paper that, by common agreement, serve to "call up" these symbols. Mathematician's symbols are just things, as we have said, that are set aside and called symbols; and, in further contrast with the linguistic philosopher, when he says that "x is a symbol", he does not mean that the letter "x" is being used as a symbol, but that it is taken to stand for some member of the collection of symbols. One can see that this manner of speaking is no more unusual than to say that "x is a natural number", with which the student should be familiar.

The concrete-abstract relationship is relative. It is worth mentioning that in linguistics the symbols are the second most concrete objects at hand, and that in mathematics they are third.

Since, by analogy, mathematics calls the things made up of symbols "linguistic" or "syntactical" objects, it is only proper to call the things used to denote these objects "meta-linguistic" objects.

Continuing in this way of drawing parallels (once the context in which the parallels live has been described): "Closed terms" are like noun phrases. "Formulas" with "free variables" are like sentences with empty noun spaces and, as such, can have meaning only when these spaces are filled with closed terms. "Structures" or "interpretations" consist of a collection of"referents" for the closed terms together with a prescription for assigning a "truth value" to closed formulas. Closed formulas are clearly the only ones of which it can be asked whether they are true or false. The logical connectives do not have referents in the structures. The method of as-signing truth values goes to their usual "truth table" interpretation and is precise in principle. But to actually determine if a given formula is true under a given interpretation of its terms, in practice one usually relies on his own understanding of the words, "not" and "implies" say, that are associated with the given connectives. The meaning of a formula is thus not written down, and to what extent it is captured by the interpretation is subject to question. "Formal theory", "theorem", "proof", "valid formula" and "model"may also be discussed in this way.

"Constructive" methods are those that deal with syntactical objects independently of any interpretation. One "builds" formulas and proofs, say, out of concrete objects in much the same way that a man would build a house of wood and stone. And by this analogy, constructive methods are usually required to be finitary, for reasons comparable to the impossibility of building an infinite house. Infinitary constructive methods have been considered however. "Semantical" methods involve structures,and hence abstract objects, and are therefore "non-constructive". And so on.

One may recall the paradigm:

Let 1 be a number.

Let x be a symbol.

Let x be a number.

Let 1 be a symbol.

To ensure having enough symbols, some authors take the class of ordinal numbers. Any proper class will suffice.

§ 2.2 Free-Variable Theories in General

Let X be a proper class and call its members symbols. Let $\sim$ and $\rightarrow$ denote two distinct symbols and let $X_1, X_2, X_{3,1}, X_{3,2}, \ldots, X_{4,1}, \ldots$ constitute a partition of $X-\{\sim,\rightarrow\}$ into mutually disjoint proper classes. Call the members of X_1 (individual) variables and, in some order, denote $\aleph_0$ of them by $x_0, x_1, \ldots$. Call the members of X_2 constants and, for each $n \geq 1$, call the members of $X_{3,n}$ and $X_{4,n}$ respectively n-ary function symbols and n-ary predicate symbols. Choose a certain member of $X_{3,2}$ as the equality symbol and denote it by =. Let the symbols $\sim$ and $\rightarrow$ be the logical connectives. Let strings be finite sequences of symbols and require that, as such, they be written without the separating commas, so that $x_0=x_0$ denotes a string, while $x_0,=,x_0$ does not.

The letters u and v denote strings, x,y and z denote variables, c a constant, f,g and h function symbols, and p and q predicate symbols. Also t should be a term, and P and Q and (rarely) R should be formulas. Convene that, if u is $u_1 \ldots u_n$ and v is $v_1 \ldots v_m$ where the u_i and v_j are symbols, then uv is $u_1 \ldots u_n v_1 \ldots v_m$ and is thereby distinguished from the two element sequence u,v. Convene also that some frequently appearing kinds of strings may be abbreviated as follows: $\rightarrow PQ$ by $(P \rightarrow Q)$, $(\sim P \rightarrow Q)$ by $(P \vee Q)$, $\sim(P \rightarrow \sim Q)$ by $(P \& Q)$, and $((P \rightarrow Q) \& (Q \rightarrow P))$ by $(P \leftrightarrow Q)$, and utt' by (tut') if u is binary, and $\sim$(tpt') by (t$\not p$t'). Omit parentheses when they are not required to determine grouping. And in this regard, agree that $\rightarrow$ and $\leftrightarrow$ have priority over $\vee$ and &, and adopt a convention of associating to the right. For example, read $P\leftrightarrow Q\&R$ as $(P\leftrightarrow(Q\&R))$ rather than $((P\leftrightarrow Q)\&R)$, and read $P_1\rightarrow\cdots\rightarrow P_n$ as $(P_1\rightarrow\cdots\rightarrow(P_{n-1}\rightarrow P_n)\cdots)$.

Every string has a finite <u>length</u>. Each member or finite sequence of consecutive members of a string is said to <u>occur</u> in that string. Observe that a symbol or string may have more than one <u>occurrence</u> in the same string. For example, $u_1u_2u_1u_1u_2$ contains three occurrences of u_1 and two of u_1u_2. The total number of occurrences of $\sim$ and $\rightarrow$ in a string is called its <u>height</u>. A string in which some variable occurs is <u>open</u>. Strings that are not open are <u>closed</u>.

The expression $u(v_1',\ldots,v_n'/v_1,\ldots,v_n)$, it being tacit that $v_i\neq v_j$ if $i\neq j$, denotes the <u>substitution of</u> $v_1',\ldots,v_n'$ <u>for</u> $v_1,\ldots,v_n$ <u>in</u> u: the string obtained from u by, for each i, replacing every occurrence of v_i by an occurrence of v_i' as long as this is possible. (For such replacements it is understood that the necessary adjustments are made regarding length. So a replacement is impossible only if either v_i does not occur in u, or it happens that an occurrence of v_i in u shares a symbol occurrence with a distinct occurrence of some v_j in u. Hence the definition implies that, if some one of these two conditions holds for every i, then $u(v_1',\ldots,v_n'/v_1,\ldots,v_n)$ is just u. Note that the substitution may differ from $u(v_1'/v_1)\cdots(v_n'/v_n)$ if some v_i occurs in v_j' for

for some $j<i$.) Such a substitution in u will be called a (substitution) instance of u only if each v_i is a variable and each v_i' is a term.

The terms are defined by a generalized induction: (i) variables and constants are terms, (ii) if $u_1,\ldots,u_n$ are terms and f is an n-ary function symbol, then $fu_1\ldots u_n$ is a term. And likewise the formulas: (i) if $t_1,\ldots,t_n$ are terms and p is an n-ary predicate symbol, then $pt_1\ldots t_n$ is a formula, called an elementary formula, (ii) if u is a formula, then $\sim u$ is a formula, and (iii) if u and v are formulas, then $\rightarrow uv$ is a formula. A sentence is a closed formula.

Unique Readability Theorem. For any term t, either (i) t is a variable, (ii) t is a constant, or (iii) t is $ft_1\ldots t_n$ for exactly one f and one finite sequence $t_1,\ldots,t_n$ of terms; and for any formula P, either (iv) P is $pt_1\ldots t_n$ for exactly one p and one finite sequence $t_1,\ldots,t_n$ of terms, (v) P is $\sim Q$ for exactly one formula Q, or (vi) P is $\rightarrow QR$ for exactly one pair of formulas Q,R; and these six cases are mutually exclusive.

Shoenfield's proof of the "formation theorem" in [39] will serve as a proof of this. (The mutual exclusiveness is implied by the partitioning of the symbols.) Once and for all, this theorem is used in every proof and definition by induction on the length of terms or on the length or height of formulas.

Proposition. $t(t_1,\ldots,t_n/x_1,\ldots,x_n)$ is a term and $P(t_1,\ldots,t_n/x_1,\ldots,x_n)$ is a formula.

This proposition is proved, for an arbitrary n, by induction on the length of terms and the height of formulas. For the sake of notational briefness, assume that n=1. If t is a variable (either x_1 or not) or a constant, then by definition, $t(t_1/x_1)$ is a term. Suppose that t is $ft'_1\ldots t'_m$ for some f and some sequence of terms $t'_1,\ldots,t'_m$. Then $t(t_1/x_1)$ is $ft'_1(t_1/x_1)\ldots t'_m(t_1/x_1)$. The induction hypothesis is that $t'_i(t_1/x_1)$ is a term for each i. Hence, by definition, $t(t_1/x_1)$ is a term. Now this proves that, if P is $pt''_1\ldots t''_k$ for some p and finite sequence $t''_1,\ldots,t''_k$, then $P(t_1/x_1)$ is a formula. Suppose that P is $\sim Q$ for some formula Q. Then $P(t_1/x_1)$ is $\sim Q(t_1/x_1)$ and the induction hypothesis is that $Q(t_1/x_1)$ is a formula. Suppose that P is $\rightarrow QR$. Consider the induction hypothesis. Conclude. □

A free-variable language L has (i) a set of symbols of L consisting of (a) the logical connectives, (b) a set of variables that includes $\mathfrak{x}_0,\mathfrak{x}_1,\ldots$, (c) a set of constants, (d) for each $n\geq 1$, a set of n-ary function symbols, (e) for each $n\geq 1$, a set of n-ary predicate symbols; and (ii) a set of formulas of L consisting of all and only those formulas that can be built up from the symbols of L.

If every symbol of L is a symbol of some language L', then L' is an extension of L. A symbol that is not a symbol of L is said to be *new to* L.

Note. The symbols of a language comprise a set, and the union of the members of a set of sets is a set. Hence, given any set of languages, each member of the partition of the class of all symbols contains a proper class of symbols that are new to every language in this set.

An *n-ary rule* (*of proof*) will be a class of (n+1)-tuples of formulas. Each member of a rule is called an *instance* or *application* of the rule, the first n members being the *hypotheses* of the instance and the last member being the *conclusion*. There will be two *logical rules*: *modus ponens*, consisting of all triples $(P, P \to Q, Q)$, and the *substitution rule*, consisting of all pairs $(P, P(t/x))$. All the formulas of the forms $P \to Q \to P$, $(P \to Q \to R) \to (P \to Q) \to P \to R$, $(\sim Q \to \sim P) \to P \to Q$, $x = x$, $x_1 = y_1 \to \cdots \to x_n = y_n \to f x_1 \ldots x_n = f y_1 \ldots y_n$, and $x_1 = y_1 \to \cdots \to x_n = y_n \to p x_1 \ldots x_n \to p y_1 \ldots y_n$ are *logical axioms*. Axioms of the first three kinds are known as *propositional axioms*, and the others are the *axioms for equality*. Any such axioms that are formulas of some language L are said to be *of* L, and a rule instance that consists exclusively of formulas of L is said to be *in* L.

Notation. (For example.) Whenever convenient, $\bar{u}$ will be written for $u_1, \ldots, u_n$. Moreover, $\bar{u}'$ (say) abbreviates $u_1', \ldots, u_n'$, and not $\{u_1, \ldots, u_n\}'$ say.

Definition 2.1. A *free-variable theory* T has: (i) a free-variable language, denoted L(T), (ii) a set of *axioms of* T consisting of the logical axioms of L(T) and (possibly) some other formulas of L(T) called nonlogical axioms of T, (iii) a set of rules of T consisting of the logical rules and (possibly) some further rules called nonlogical rules of T, (iv) a set of theorems of T that is defined by generalized induction: (a) the axioms of T are theorems of T, (b) if $(\bar{P}, R(\bar{P}))$ is an instance in L(T) of a rule of T, and each P_i is a theorem of T, then $R(\bar{P})$ is a theorem of T. A finite sequence $\bar{P}$ of formulas of L(T) is a proof of a formula P in T if P is P_n and, for each i, either P_i is an axiom of T, or there exist $i_1, \ldots, i_m < i$ such that $(P_{i_1}, \ldots, P_{i_m}, P_i)$ is an instance of a rule of T. $T \vdash P$ indicates that there is a proof of P in T. Sometimes we just say that T proves P.

Proposition. A formula P is a theorem of a theory T if and only if $T \vdash P$.

$\Rightarrow$: This is proved by an induction on the theorems of T. If P is an axiom of T, then the one element sequence P is a proof of P in T. Suppose that, for some rule R of T, P is $R(\bar{P})$ where each P_i has a proof, say $P_{i,1}, \ldots, P_{i,k_i} = P_i$, in T. Then the sequence $P_{1,1}, \ldots, P_{1,k_1}, \ldots, P_{n,1}, \ldots, P_{n,k_n} = P$ is a proof of P in T.

$\Leftarrow$: This is an easy induction on the length of proofs in the theory T. ▯

Remark. How free-variable theories differ from first-order theories is evident. In this remark we offer the most likely reason that first-order theories should not have nonlogical rules.

Let T be a first-order theory. Let T' be obtained from T by adding some rule R. Let T" be the theory that is obtained from T by adding, as nonlogical axioms, all the formulas $P_1'\&\cdots\&P_n' \rightarrow R(\bar{P})'$ where $(\bar{P}, R(\bar{P}))$ is an instance of R in L(T') (=L(T)), and where the primes indicate universal closure. Then every theorem of T' is a theorem of T". For suppose that $T' \vdash P$. To complete an induction on the theorems of T', we need only show that, if P is the conclusion in an instance $(\bar{P}, R(\bar{P}))$ of R such that $T'' \vdash P_i$ for all i, then $T'' \vdash P$. This is easy. By the closure theorem, our hypothesis yields that $T'' \vdash P_i'$ for all i, so T" proves $P_1'\&\cdots\&P_n'$ by the tautology theorem. In turn, this and the corresponding nonlogical axiom yields $T'' \vdash P'$. Hence $T'' \vdash P$ by the closure theorem.

Now suppose that T' satisfies the deduction theorem. (Note that the theorem is not automatic, since its proof is by an induction on theorems, which cannot be completed for T' without some further information about R.) Then every theorem of T" is a theorem of T'. For this we need only show that, for each instance of R in L(T'), the corresponding axiom of T" is a theorem of T'. Consider the instance (R,R(P)). For any formula P, if $T'(\bar{P})$ (Notation: see the following) proves P, then $T'(P_1', \ldots, P_n')$ proves P' by the closure theorem; whence $T'(P_1'\&\cdots\&P_n')$ proves P'by the tautology theorem; so that T' proves $P_1'\&\cdots\&P_n' \rightarrow P'$ by the deduction theorem.

Today, there are no known worthwhile R such that a first-order theory plus R fails to satisfy the deduction theorem. Thus, at least for now, when dealing with first-order theories, there is nothing to gain by considering nonlogical rules.

A theory T is *consistent* if no formula P of L(T) is such that both P and ~P are theorems of T. Otherwise T is *inconsistent*. A formula P is *decidable in* T if at least one of P and ~P is a theorem of T. A formula that is not decidable is *undecidable*. A formula P is *refutable in* T when some (not necessarily closed) substitution instance of ~P is a theorem of T.

Definition 2.2. A consistent theory T is *sententially complete* if every sentence of L(T) is decidable in T. A consistent theory T is *complete* if every formula of L(T) that is not a theorem of T is refutable in T. If T is not complete, it is *incomplete*.

Notes. (i) Complete theories are sententially complete. (ii) A consistent theory T whose language contains a constant is complete if and only if it is sententially complete and a formula of L(T) all of whose closed instances in L(T) are theorems of T is also a theorem of T. (iii) We shall sometimes make use of (i) and (ii) without mention. By the way, item (ii) shows that Definition 2.2 generalizes the notion of completeness as found in [16] for the system $\mathcal{R}$.

Remark. It is not difficult to see that, when it is stated for first-order theories, our definition of completeness implies the usual one (every (first-order) closed formula is decidable). On the other hand, a complete first-order theory containing a constant is complete in our sense, and one without a constant has a conservative extension that is complete in our sense. (This is the corresponding Henkin theory. See Shoenfield [39].) Thus, it is remarkable that the free-variable theories of arithmetic, A and A^-, whose languages contain a constant, are incomplete (§2.3). For this shows that there are systems of weaker expressional strength, but with stronger rules of proof, than the first-order theory of number theory (see [39]),which are nevertheless incomplete in precisely the same sense.

A theory T' is an <u>extension</u> of T if the symbols, axioms, and rules of T' include all those of T. Where X is a set of symbols, T(X) denotes the extension of T obtained by including the members of X among the symbols of L(T) (by <u>adjoining</u> them to T). Where E is a set of formulas of L(T(X)) and ρ is a set of rules, $T(X,E,\rho)$ denotes the extension of T(X) obtained by adjoining E to the axioms of T(X), and ρ to its rules. If any of X, E or ρ is empty, it is omitted, and sometimes their members are just listed.

Although not absolutely necessary, it will be convenient to have the following well-known theorem. Its proof is the same as the one due to Kalmár (1935) as found in Margaris [30], even though its statement here is for theories with a free-variable rather then a first-order language. For the statement, one requires some further terminology. A <u>truth</u>

value assignment (tva) for a language L is a function V from the elementary formulas of L to the set {0,1} where 0 and 1 are the truth values. With each tva V there is an unique extension V* that maps the formulas of L to {0,1} according to: (i) if P is an elementary formula, then V*(P)=V(P), (ii) if P is ~Q for some Q, then V*(P)=0 iff (if and only if) V*(Q)=1, (iii) if P is →QR, then V*(P)=0 iff V*(Q)=1 or V*(R)= 0. It is easy to see that each V* acts on abbreviated formulas in the expected way. A formula P of a language L is a tautology if V*(P)=0 for every tva V for L. If a sequence $\bar{P}$ of formulas of L is such that V*(P)=0 whenever V*(P_i)=0 for every i, then P is a tautological consequence of $\bar{P}$.

Now every formula P determines an unique language L_P whose symbols are those common to every free-variable language together with just those occurring in P; and every language determines an unique theory having no nonlogical axioms or rules. It happens that, when considered as a formula of any extension of L_P, P is a tautology if and only if it is a tautology with respect to L_P. Hence, since P is a theorem of a theory T if it is already a theorem of a theory that T extends, it should be clear what is meant in the following.

Tautology Theorem. Every tautology is a theorem.

As the above considerations also apply to a sequence $\bar{P}$,P, one can also state without loss the

Corollary. If $P_1,\ldots,P_n$ are theorems and P is a tautological consequence of $\bar{P}$,then P is a theorem.

In the future, both the theorem and the corollary will be referred to as the theorem.

Note. To demonstrate that a formula is a tautology, it is usually easiest to argue by contradiction. For example, suppose that some tva V is such that $V^*(Q \to Q \vee (P \& Q)) = 1$. Then $V^*(Q)=0$ and $V^*(Q \vee (P \& Q))=1$, the latter of which implies that $V^*(Q)=1$.

Note that $T \vdash P$ and $T \vdash Q$ implies that $T \vdash P \& Q$, and conversely. Note also that, for any formula Q, $P \& {\sim} P \to Q$ is a tautology and, hence, a theorem. It follows by modus ponens that T is inconsistent if and only if every formula of L(T) is a theorem of T.

A rule R is valid in a theory T if $T(\bar{P}) \vdash R(\bar{P})$ for every instance $(\bar{P}, R(\bar{P}))$ of R in L(T). The proofs of all the following are but slight modifications of the proofs of their correspondents in Shoenfield [39]. T is any theory.

Substitution Rule. The rule consisting of all pairs $(P, P(\bar{t}/\bar{x}))$ is valid in T. (In the sequel, it will always be clear which substitution rule is being refered to. Note that the earlier one is included here as a special case.)

Symmetry Theorem. $T \vdash x=x' \leftrightarrow x'=x$.

Equality Theorem. Let t' be obtained from t by replacing some (any) occurrences of $t_1, \ldots, t_n$ by $t_1', \ldots, t_n'$ respectively, and let P' be similarly obtained from P. Then $T \vdash t_1 = t_1' \to \cdots \to t_n = t_n' \to t = t'$ and $T \vdash t_1 = t_1' \to \cdots \to t_n = t_n' \to P \leftrightarrow P'$.

Equivalence Theorem. Let P' be obtained from P by replacing some (any) occurrences of $P_1, \ldots, P_n$ by $P_1', \ldots, P_n'$ respectively. If $T\vdash P_i \leftrightarrow P_i'$ for each i, then $T\vdash P\leftrightarrow P'$.

Let us now see how some of this can be applied.

§ 2.3 The Theories $\underline{A}$ and A^-.

Throughout this section, most of the functions and predicates are number theoretic, that is, functions from the set of natural numbers to itself and predicates on the set of natural numbers. In addition to the notational conventions already laid down, we'll now proceed to mix them. For example, 0 is used for both the number 0 and the constant (symbol) zero, and S denotes either the successor function or the successor function symbol. The theory whose sets of symbols, axioms, and rules are the unions of the corresponding sets in the members of some sequence $T_0, T_1, \ldots$ of theories will be denoted by $\bigcup_i T_i$. We expect the meanings of our further nonstandard uses of set theoretic notations to be clear. To increase the readability of certain expressions, we'll often write $f(x_1,\ldots,x_n)$, say, instead of $fx_1\ldots x_n$.

Definition 3.3. Let $f_1, f_2, \ldots$ be a sequence of $\aleph_0$ function symbols such that, for each $n\geq 1$, infinitely many of the f_i are n-ary. We first define a theory A_k^j for each $k\geq 0$ and $0\leq j\leq 3$. Let A_0^0 be the theory whose language contains the constant 0 and the first two unary f_i (henceforth S and Z), whose single nonlogical axiom is $Z\chi_0=0$, and which has no nonlogical rules. Set $A_0^j = A_0^0$ for $1\leq j\leq 3$.

Now suppose that we have A_{k-1}^j for all $j\leq 3$.

(i) Let $A_k^0 = A_{k-1}^3$.

(ii) Let $f^1, \ldots, f^k$ be the first k k-ary f_i not in $L(A_k^0)$ and set

$$L(A_k^1) = L(A_k^0) \cup \{f^i\}_{i=1}^k,$$

$$Ax(A_k^1) = Ax(A_k^0) \cup \{f^i(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_k) = \underset{\sim}{x}_i\}_{i=1}^k$$

(where $Ax(T)$ is the set of axioms of T).

(iii) Let $\{S_r\}_{r=1}^{k'}$ be a listing of the distinct sequences g, $h_1, \ldots, h_m$ from $L(A_k^0)$ such that $m \leq k$, g is m-ary, and each h_i is n-ary for some $n \leq k$. For each r, select f^r by: if the h_i in S_r are s-ary, then f^r is the first s-ary f_i not in $L(A_k^1) \cup \{f^i | i < r\}$. Set

$$L(A_k^2) = L(A_k^1) \cup \{f^r\}_{r=1}^{k'},$$

$$Ax(A_k^2) = Ax(A_k^1) \cup \{f^r(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) = g(h_1(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n), \ldots,$$

$$h_m(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)) | g, h_1, \ldots, h_m \text{ is } S_r\}_{r=1}^{k'}.$$

(iv) Let $\{R_r\}_{r=1}^{k''}$ be a listing of the distinct pairs g,h from $L(A_k^0)$ such that g is n-ary and h is (n+2)-ary with $1 \leq n \leq k-1$, and for each r, select f^r by: if g is s-ary, then f^r is the first (s+1)-ary f_i not in $L(A_k^2) \cup \{f^i | i < r\}$. Set

$$L(A_k^3) = L(A_k^2) \cup \{f^r\}_{r=1}^{k''},$$

$$Ax(A_k^3) = Ax(A_k^2) \cup \{f^r(0, \underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) = g(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) \text{ and}$$

$$f^r(S\underset{\sim}{x}_0, \underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) = h(\underset{\sim}{x}_0, \underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n, f^r(\underset{\sim}{x}_0, \underset{\sim}{x}_1,$$

$$\ldots, \underset{\sim}{x}_n)) | g, h \text{ is } R_r\}_{r=1}^{k''}.$$

This completes the definition of the A_k^j. Henceforth, if it is not inconvenient, A_k^0 is shortened to A_k. We may now define the theory A^- of primitive recursive arithmetic as $(\bigcup_k A_k)(I)$ where I is the induction rule consisting of all the triples $(P(0/x), P \rightarrow P(Sx/x), P)$. By the theory A of Peano arithmetic we shall mean the theory $A^-(Sx_0 \neq 0)$.

Notes. (i) In the sequel, it is often said for example, that $Sx \neq 0$ is an axiom of A, when the formula is actually a substitution instance of an axiom of A.

(ii) For future reference, suppose that for each $n \geq 1$, we have a sequence $f_{n,1}, f_{n,2}, \ldots$ of $\aleph_0$ n-ary function symbols. Then the sequence that is formed by ordering the $f_{i,j}$ lexicographically is a listing of the kind we've called for in the above definition (where $(i,j) \leq (i',j')$ lexicographically if either $i < i'$ or $i = i'$ and $j \leq j'$).

Note. It can be shown that, except for the second-order induction, all of Peano's axioms have proofs in A, and that these necessitate a proof of $S0 \neq 0$. However (see §3.1), this formula is not a theorem of A^- by the validity theorem, since A^- has a one element model described as follows: let the domain of M be {0} and, for each n-ary f, let M(f) be the n-ary constant zero function. It is immediate that the axioms of A^- and the induction rule are valid in M. Hence it follows that M is a model of A^- by an induction on theorems.

Let k_x be the numeral $S \cdots S0$ with x occurrences of S.

Usually 0 and 1 will be written for k_0 and k_1. A function symbol f of L(A) is said to represent a number theoretic function F in A if, for each choice of numbers $x_1,\ldots,x_n,y$ we have that $F(x_1,\ldots,x_n)=y$ implies that $A\vdash f(k_{x_1},\ldots,k_{x_n})=k_y$. A number theoretic function F is representable in A whenever such f exist.

Theorem 2.1. (Representation Theorem) A number theoretic function is representable in A if and only if it is primitive recursive.

In one direction this is proved by an induction on the set of primitive recursive functions. Suppose that F is the successor function. Then S represents F in A because, for each x, $S(k_x)$ and $k_{x'}$ are the same term. Clearly, if F is the constant zero function, then Z represents F in A; and if F is I_i^n for some i and n, then $f^i \varepsilon L(A_n^1)$ represents F in A. Suppose that F is $S_m^n(G,H_i)$ where G and $H_1,\ldots,H_m$ are represented in A by g and $h_1,\ldots,h_m$ respectively. Then for some r, $g,h_1,\ldots,h_m$ is S_r and, for some least k, S_r is contained in A_k, so that $f^r \varepsilon L(A_k^2)$ represents F in A. Similarly, if F is $R^n(G,H)$ where G and H are represented by g and h then, for some r and least k, $f^r \varepsilon L(A_k^3)$ represents F in A.

The other direction should be clear. If f represents F in A, then the defining axioms for f provide an explicit definition of F. □

Remark. It is evident that the theory A was defined with this proof in mind. We merely copied the formulation of the primitive recursive functions that was presented in Chapter 1. It should be clear, however, that if we had started with a different formulation of primitive recursion, and then defined A by copying that one, we would arrive at essentially the same theory. The function symbols would only be introduced in a different order, and the defining equations for a symbol representing a specific function would be "written" differently.

Let us now use Theorem 2.1 to see how the system $\mathcal{R}$ of [16] may be "formalized" as the formal system R of primitive recursive arithmetic that is defined as follows: the language of R is L(A) less the logical connectives (so that the formulas of R are equations); the axioms of R are just the nonlogical axioms of A^-; and the rules of R are just the schemata Sb_1, Sb_2, T and U_1 written as rules of proof (so that, for example, Sb_1 is now the class of all pairs $(f(x_1,\ldots,x_n)=g(x_1,\ldots,x_n),$ $f(t_1,\ldots,t_n)=g(t_1,\ldots,t_n))$. (It is worth noting that the technically more difficult task of writing the schema U as a collection of ordered pairs is avoided here by using U_1, which, as was said in Chapter 1, is equivalent to U.)

The observation to be made is that instead of the language of $\mathcal{R}$ provided in [16], Chapter VIII, we could assume L(R) and thereby view $\mathcal{R}$ as the ordered pair (R,I) where I is the natural interpretation of R. It is obvious that $\mathcal{R}$ and (R,I) have equivalent rules of proof. By inspecting the proof of Theorem 2.1, one sees that we could read "R" in place of "A". Thus, from the fact that every primitive recursive function is representable in R we have that every function and axiom of $\mathcal{R}$ is in (R,I); and the reverse inclusion holds because every function symbol of R represents some primitive recursive function.

These considerations make it clear that any equation that is known to be provable in $\mathcal{R}$ also has a proof in R, and hence also in A and A^-. We shall have occasion to make use of this fact.

Theorem 2.2. The theory A^- represents R; that is, for each formula (equation) P of L(R), $R \vdash P$ if and only if $A^- \vdash P$.

This theorem will follow by three lemmas, of which two will make use of the following notational device:

For each formula P of L(A), let P* denote the equation $P^0=0$, where P^0 is defined by an induction on the height of P: (i) if P is an equation, say $t_1=t_2$, let P^0 be $|t_1,t_2|$ (Note. Whenever convenient, the notation for a familiar primitive recursive function is used to abbreviate expressions containing a symbol that represents that function in A.), (ii) if P is $\neg Q$ for some Q, let P^0 be $1 \dot{-} Q^0$, (iii) if P is $Q \to R$ for some Q and R, let P^0 be $(1 \dot{-} Q^0)\cdot R^0$.

Lemma 1. $R \vdash |t,t'|=0 \Leftrightarrow R \vdash t=t'$.

This was proved in [16].

Lemma 2. For all formulas P of L(R), $R \vdash P \Rightarrow A^- \vdash P$.

By the definition of R, all the axioms of R are axioms of A^-. So the lemma follows by an induction on the theorems of R, once we have that the rules of R are valid in A^-. We have that Sb_1 is valid in A^- because it is a subclass of the substitution rule. Sb_2 is valid in A^- because $A^- \vdash t_1=t_2 \to f(t_1)=f(t_2)$ by the equality theorem, which means that given that $A^- \vdash t_1=t_2$, it will follow that $A^- \vdash f(t_1)=f(t_2)$ by modus ponens. And T is valid in A^- because $t_1=t_1$ and $t_1=t_2 \to t_1=t_2 \to t_1=t_1 \to t_2=t_3$ are substitution instances of axioms of A^-, which means that from $A^- \vdash t_1=t_2$ and $A^- \vdash t_1=t_3$ it follows that $A^- \vdash t_2=t_3$ by modus ponens. Suppose that the formulas $f(0)=g(0)$, $f(Sx)=h(x,f(x))$ and $g(Sx)=h(x,g(x))$ are theorems of A^-. Then $h(x,f(x))=h(x,g(x)) \to f(Sx)=g(Sx)$ is a theorem of A^-. Hence, since $f(x)=g(x) \to h(x,f(x))=h(x,g(x))$ is a theorem of A^- by the equality theorem, it follows that $f(x)=g(x) \to f(Sx)=g(Sx)$ is a theorem of A^- by the tautology theorem. Whence $f(x)=g(x)$ is a theorem by the induction rule, and A^- validates U_1. ▯

Note. This also shows that Sb_1, Sb_2, T and U_1 are valid in A.

Lemma 3. For all formulas P of L(A), $A^- \vdash P \Rightarrow R \vdash P^*$.

There is a method for transforming any proof of P in A^- into a proof of P^* in R, because (i) if P is an axiom of A^-, then $R \vdash P^*$, and (ii) if $(\bar{P}, R_0(\bar{P}))$ is an instance in $L(A^-)$ of a rule R_0 of A^-, then $R(\overline{P^*}) \vdash (R_0(\bar{P}))^*$. The assertions (i) and (ii) are easily proved, using the results of [16]. ▯

Proof of Theorem 2.2. Let P be a formula of L(R). $\Rightarrow$: If $R \vdash P$, then $A^- \vdash P$ by Lemma 2. $\Leftarrow$: If $A^- \vdash P$, then $R \vdash P^*$ by Lemma 3. Hence, supposing that P is $t=t'$, P^* is $|t,t'|=0$, by the definition of P^*, and $R \vdash P$ by Lemma 1. ▯

This theorem enables one to attribute almost any of the known properties of R to A^-, and vice versa. In particular, we have the following by Rose [37].

Corollary. A^- is incomplete.

Note. Since R is logic-free, one cannot simply adjoin the formula $\sim S0=0$ to R and then repeat the above proof to obtain that A is incomplete. Furthermore, adjoining the corresponding equation, namely $1\dot{-}|S0,0|=0$, would not help; for the latter is already a theorem of A^-.

The next theorem asserts that every formula of L(A) is **logically** equivalent (in A) to an equation of L(A). Moreover, it may be viewed as asserting that within the context of A, the logical constants of [16] are logically equivalent to the classical logical connectives. Most of the technicalities are absorbed in the following two Lemmas. The lemmas cited in the proof of Lemma 1 are the foregoing lemmas for Theorem 2.3.

Lemma 1. $A^-\vdash |x,y|=0\leftrightarrow x=y$.

This amounts to examining Goodstein's proof of Lemma 1 and showing in certain places that $A^-\vdash P\leftrightarrow Q$ where he shows that $R\vdash P\leftrightarrow R\vdash Q$. We'll supply the details. By the symmetry theorem, we have that

$$A^-\vdash |x,y|=0\leftrightarrow 0=|x,y|. \tag{1}$$

Since $A^-\vdash 1\dot{-}0=1\rightarrow 0=|x,y|\rightarrow 1\dot{-}|x,y|=1$ by the equality theorem, and since $1\dot{-}0=1$ is an instance of the first defining axiom for $\dot{-}$, we have that

$$A^-\vdash 0=|x,y|\rightarrow 1\dot{-}|x,y|=1 \tag{2}$$

by modus ponens. It is known that the equation $(1\dot{-}|x,y|)\cdot x$

$=(1\dot{-}|x,y|)\cdot y$ is derivable in R. So it is a theorem of A^- by Lemma 2. By noting that $1\dot{-}|x,y|=1\rightarrow(1\dot{-}|x,y|)\cdot x=(1\dot{-}|x,y|)\cdot y\rightarrow 1\dot{-}|x,y|=1\rightarrow 1\cdot x=1\cdot y$ by the equality theorem, one sees that

$$A^-\vdash 1\dot{-}|x,y|=1\rightarrow 1\cdot x=1\cdot y \qquad (3)$$

by modus ponens. Finally, $1\cdot x=x\rightarrow 1\cdot y=y\rightarrow 1\cdot x=1\cdot y\rightarrow x=y$ is an instance of a logical axiom, and one can surely prove $1\cdot x=x$ in A^-, so

$$A^-\vdash 1\cdot x=1\cdot y\rightarrow x=y \qquad (4)$$

by modus ponens. Hence $A^-\vdash|x,y|=0\rightarrow x=y$ by (1) through (4) and the tautology theorem.

So there remains to show that $A^-\vdash x=y\rightarrow|x,y|=0$. This is done as follows. Suppose one has that

$$A^-\vdash x=y\rightarrow x\dot{-}y=0. \qquad (1)$$

Then $A^-\vdash y=x\rightarrow y\dot{-}x=0$ by substitution, and $A^-\vdash x=y\leftrightarrow y=x$ by the symmetry theorem, so

$$A^-\vdash x=y\rightarrow y\dot{-}x=0 \qquad (2)$$

by the tautology theorem. The desired result then follows by (1) and (2) and the defining axiom for $|\ ,\ |$. So we must prove (1). First of all, $A^-\vdash x=y\rightarrow x\dot{-}x=0\rightarrow x\dot{-}y=0$ by the equality theorem, whence $A^-\vdash x\dot{-}x=0\rightarrow x=y\rightarrow x\dot{-}y=0$ by the tautology theorem. We'll show that

$$A^-\vdash x\dot{-}x=0. \qquad (3)$$

By the induction rule, this reduces to showing that

$$A^-\vdash x\dot{-}x=0\rightarrow Sx\dot{-}Sx=0, \qquad (4)$$

since we already have that $A^-\vdash 0\dot{-}0=0$ by the defining axioms for $\dot{-}$. Since $A^{-}\vdash x\dot{-}y=Sx\dot{-}Sy\rightarrow 0=0\rightarrow x\dot{-}y=0\rightarrow Sx\dot{-}Sy=0$ by the equality theorem, and since $0=0$ is an instance of a logical axiom, (4) will follow from

$$A^{-}\vdash x\dot{-}y=Sx\dot{-}Sy \qquad (5)$$

by modus ponens and the substitution rule. Fortunately, it is known that $x\dot{-}y=Sx\dot{-}Sy$ is a theorem of R; so (5) follows by Lemma 2. □

Lemma 2. $A\vdash 1\dot{-}x=0\rightarrow x\neq 0$.

By the equality theorem, we have that $A\vdash 1\dot{-}0=1\rightarrow 1\neq 0\leftrightarrow 1\dot{-}0\neq 0$. Since $1\neq 0$ is an axiom, and $1\dot{-}0=1$ is an instance of the first defining axiom for $\dot{-}$, it follows that $A\vdash 1\dot{-}0\neq 0$. Thus $A\vdash 0=0\rightarrow 1\dot{-}0\neq 0$, so that

$$A\vdash 1\dot{-}0=0\rightarrow 0\neq 0,$$

by the tautology theorem. We'll show that

$$A\vdash Sx\neq 0.$$

We have that $A\vdash S0\neq 0$, so we need that $A\vdash Sx\neq 0\rightarrow SSx\neq 0$. By the tautology theorem, this reduces to $A\vdash SSx=0\rightarrow Sx=0$. Since $A\vdash SSx\dot{-}1=Sx$ and $A\vdash 0\dot{-}1=0$ by the defining axioms for $\dot{-}1$, this follows by noting that $A\vdash SSx=0\rightarrow SSx\dot{-}1=0\dot{-}1$ by the equality theorem. Now we can obtain

$$A\vdash (1\dot{-}x=0\rightarrow x\neq 0)\rightarrow (1\dot{-}Sx=0\rightarrow Sx\neq 0)$$

by the tautology theorem; and an application of the induction rule completes the proof. □

Theorem 2.3. $A\vdash P\leftrightarrow P^{*}$.

By definition, P^{*} is $P^{0}=0$. If P is an equation, then $A\vdash P\leftrightarrow P^{0}=0$ by Lemma 1. Suppose that P is $\sim Q$ for some formula Q.

The induction hypothesis is that $A \vdash Q \leftrightarrow Q^*$. Hence, since $A \vdash \sim\sim Q \leftrightarrow Q$ by the tautology theorem, it follows by the equivalence theorem that $A \vdash \sim Q \leftrightarrow \sim Q^*$, i.e., $A \vdash \sim Q \leftrightarrow Q^0 \neq 0$. Moreover, since $(\sim Q)^0$ is $1 \dot{-} Q^0$, we have that $A \vdash (\sim Q)^0 = 0 \leftrightarrow Q^0 \neq 0$ by Lemma 2. Hence $A \vdash P \leftrightarrow P^0 = 0$ by the tautology theorem. Suppose that P is $Q \rightarrow R$ for some formulas Q and R. The induction hypothesis is that $A \vdash Q \leftrightarrow Q^*$ and $A \vdash R \leftrightarrow R^*$. Hence, by the tautology theorem and the equivalence theorem, we have that $A \vdash P \leftrightarrow (Q^* \rightarrow R^*)$. Thus, we must show that $A \vdash (Q^* \rightarrow R^*) \leftrightarrow P^*$. This result may be sketched as follows:

$A \vdash P^* \leftrightarrow (1 \dot{-} Q^0) \cdot R^0 = 0$ (by the definition of P^*)

$\leftrightarrow 1 \dot{-} Q^0 = 0 \vee R^0 = 0$ (*) (see the following)

$\leftrightarrow Q^0 \neq 0 \vee R^0 = 0$ (by Lemma 2)

$\leftrightarrow Q^0 = 0 \rightarrow R^0 = 0$.

The verification of (*) is best accomplished by showing generally that $A \vdash x \cdot y = 0 \leftrightarrow (x = 0 \vee y = 0)$, i.e., that $A \vdash x \cdot y = 0 \leftrightarrow (x \neq 0 \rightarrow y = 0)$. This is an induction on x, wherein, by the equivalence theorem and the fact that $A \vdash y = 0 \rightarrow (Sx \neq 0 \rightarrow y = 0)$ by the tautology theorem, the induction step reduces to showing that $A \vdash Sx \cdot y = 0 \leftrightarrow y = 0$. That $A \vdash y = 0 \rightarrow Sx \cdot y = 0$ is direct. That $A \vdash Sx \cdot y = 0 \rightarrow y = 0$ uses an induction on y, whose induction step amounts to showing that $A \vdash Sx \cdot Sy \neq 0$. Hence the proof is completed via the defining axioms for $\cdot$ and +, by showing that $A \vdash Sx \cdot Sy = S(Sx \cdot y + x)$ and using the fact that $A \vdash Sx \neq 0$. □

Remark. Suppose that we form the first-order theory P_0 by adjoining the function symbols and nonlogical axioms of A to the first-order theory P of Peano Arithmetic. Then we would have that every free-variable (quantifier-free) formula of $L(P_0)$ is logically equivalent (in P_0) to an equation, save for the fact that $L(P_0)$ contains the symbol $<$, which has no defining axiom. More exactly, we can have this property in a theory P_1 that is obtained from P_0 by adjoining the formula $t<t' \leftrightarrow St \dot{-} t'=0$, or for that matter, by adjoining any free-variable definition of $<$ in terms of the function symbols. This could become of interest when we see in §3.2 that P_0 is a conservative extension of P.

Our next task is to show that A and A^- are consistent theories. Our proof will be along the lines of Gödel's well-known proof [14] that P is consistent. More precisely, we follow the proof as it is recorded in [39]; but it is after Gödel that we call such proofs "constructive".

In [39] an auxiliary, free-variable language Y for a theory of"primitive recursive functionals of finite type" is established, and then augmented by considering "generalized formulas" consisting of formulas of Y preceded by zero or more universal and existential quantifiers. Subsequently, each formula of L(P) is "interpreted" as a generalized formula; that is, a generalized formula is assigned to each formula of P, in such a way that the two formulas "have the same meaning"; and it is seen that a generalized formula has in turn, a "quantifier-free meaning" in terms of the functionals. (By the way, it is worth emphasizing that the idea of meaning serves only to guide the intuition, and does not enter explicitly into the proof.)

Primitive recursive functionals are eliminable in the same sense as are primitive recursive functions. Hence one can define some "true" and "valid" generalized formulas, similarly as we do below for the formulas of L(A). Then, by proving that a formula of L(P) is a theorem of P only if its corresponding generalized formula is valid (which, indeed, is long and difficult), and observing that the interpretation of S0=0 is not valid, one concludes that P is consistent. Our proof is simpler because (i) L(A) does not contain quantifiers, and (ii) A is a theory of primitive recursion; for together, these mean that L(A) already has the properties that one requires of an auxiliary language.

In the present terminology, the notion of eliminability takes the following form: given a closed term t of L(A), one can find, in finitely many mechanical steps, a unique numeral k_n such that $A \vdash t = k_n$. This may also be expressed by saying that a closed term of L(A) is reducible in A to a unique numeral, and this particular instance, by saying that t reduces to k_n in A. The fact that every closed term of L(R) is reducible in R to a unique numeral has been proved by Goodstein. Therefore, this carries over to A^-, and hence to A, by Theorem 2.2.

The true and false sentences P of L(A) are defined by an induction on the height of P. If P is an elementary formula, then it is true if the terms on either side of the equality symbol reduce to the same numeral. Otherwise it is false. If P is $\sim Q$, then P is true if Q is false, and false if not. If P is $Q \to R$, then P is true if either Q is false or R is true, and false if not. A sentence of the form $P(\bar{k}_y/\bar{x})$ is called a <u>numeral instance</u> of P, and a formula P is said to be <u>valid</u> (verifiable) if all of its numeral instances are true. Thus, since every formula is provable in an inconsistent theory, and since $S0=0$ is not valid, it follows that A is consistent if only we have

<u>Theorem 2.4</u>. If $A \vdash P$ then P is valid.

That each propositional axiom is valid follows by the definition of true. The validity of an axiom of the form $x=x$ is obvious. Since each numeral instance of a term reduces uniquely, a formula of the form $x_1=y_1 \to \cdots \to x_n=y_n \to fx_1 \ldots x_n=fx_1 \ldots x_n$ is valid by the definition of true. Since = is the only predicate symbol, the validity of each formula $x_1=y_1 \to \cdots \to x_n=y_n \to px_1 \ldots x_n \to px_1 \ldots y_n$ is clear. It is obvious that $S0 \neq 0$ is valid. And for any other nonlogical axiom, each numeral instance is a theorem of A; so the axiom is valid by the transitivity of equality and the uniqueness of reducibility.

Suppose that P is inferred from some valid theorems Q and $Q \to P$ by modus ponens. Then, for each numeral instance $P(\bar{k}_y/\bar{x})$ of P, we have that $Q(\bar{k}_y/\bar{x})$ and $(Q \to P)(\bar{k}_y/\bar{x})$ is valid, and so $P(\bar{k}_y/\bar{x})$ is true by definition. Suppose that Q is valid and that P is $Q(t/x)$. Then $P(\bar{k}_y/\bar{x})$ is true because, where k_m is the numeral that $t(\bar{k}_y/\bar{x})$ reduces to, the sentence

$P(k_m/x)(\bar{k}_y/\bar{x})$ is true. Suppose that $P(0/x)$ and $P \rightarrow P(Sx/x)$ are valid. Then the truth of $P(k_m,\bar{k}_y/x,\bar{x})$ follows by the definition of true and the truth of the formulas $P(k_0,\bar{k}_y/x,\bar{x}) \rightarrow P(k_1,\bar{k}_y/x,\bar{x}),\ldots,P(k_{m-1},\bar{k}_y/x,\bar{x}) \rightarrow P(k_m,\bar{k}_y/x,\bar{x})$. $\square$

Our next project is to establish a Gödel numbering of the theory A that will enable us to prove it is undecidable. For this is required some further information about primitive recursion and some more notations.

Usually, we'll adhere to the customary practice of having "$P(x_1,\ldots,x_n)$ holds" mean that $(x_1,\ldots,x_n) \varepsilon P$ (i.e., $K_P(x_1,\ldots,x_n)=0$) and having $F(x_1,\ldots,x_n)$ and $P(x_1,\ldots,x_n)$ standing alone denote respectively a function and a predicate. What follows here is well-known. For the most part our reference is [39], but this may also be found in [37]. The binary relations $=$, $<$ and $\leq$ are primitive recursive. (For example, $K_{=}(x,y)=1 \dot{-} (1 \dot{-} |x,y|)$.) Given any two (say unary) primitive recursive relations $P(x)$ and $Q(x)$, their complements $\neg P(x)$ and $\neg Q(x)$ (with respect to the set of natural numbers), their union $P \vee Q(x)$, and their intersection $P \& Q(x)$ are primitive recursive. (For clearly $K_{\neg P}(x)=1 \dot{-} K_P(x)$, $K_{P \vee Q}(x)= K_P(x) \cdot K_Q(x)$ and $K_{P \& Q}(x)=1 \dot{-} (1 \dot{-} (K_P(x)+K_Q(x)))$.) If P and F are primitive recursive then $\exists y \leq F(x)(P(y))$ (there exist $y \leq F(x)$ such that $P(y)$ holds) and $\forall y \leq F(x)(P(y))$ (for all $y \leq F(x)$, $P(y)$ holds) are primitive recursive relations, and $\mu y \leq F(x)(P(y))$ (the smallest $y \leq F(x)$ such that $P(y)$ holds) is a primitive recursive function. Due to Gödel we have a binary primitive recursive function β such that $\beta(x,i) \leq x \dot{-} 1$ for all x and i, and such that, for any sequence $x_0, \ldots, x_{n-1}$, there is a number x such that $\beta(x,i)=x_i$ for all $i<n$. For each sequence $x_1, \ldots, x_n$, $<x_1, \ldots, x_n>$ denotes the smallest x such that $\beta(x,0)=n$ and $\beta(x,i)=x_i$ for $0<i\leq n$; and for each n, $< >$ is primitive recursive when it is considered as a function of $x_1, \ldots, x_n$. This least x is known as the Gödel (or sequence) number of the sequence. It happens that $<\phi>=0$. It is convenient to define $lh(x)=\beta(x,0)$ and $(x)_i=\beta(x,i+1)$ so that, in the preceding case, $lh(x)=n$ and $(x)_i=x_i$ for $0<i\leq n$.

With these as tools we can begin. What we'll do is list all the required steps but, to dispense with uninformative details, only be precise enough in crucial places, so that the reader can go to [27] or [39] for the necessary means to fill in the gaps.

1. A function SN from the set of symbols of L(A) to N is defined as follows: (i) $SN(\mathfrak{x}_n)=3n$ for all n, (ii) where $f_{1,1}$, $f_{2,1}$, $f_{1,2}, \ldots$ is the listing noted at the end of Definition 2.3, and where OP is the ordered pair function defined by $OP(x,y)=(x+y)\cdot(x+y)+x+1$, $SN(f_{i,j})=3\cdot OP(i,j)+1$, (iii) $SN(\sim)=2$, $SN(\rightarrow)=5$, $SN(=)=8$ and $SN(0)=11$. For each u, SN(u) is its symbol number.

2. To each term t and formula P we assign the expression numbers $\ulcorner t \urcorner$ and $\ulcorner P \urcorner$ as follows: $\ulcorner \mathfrak{x}_n \urcorner = <SN(\mathfrak{x}_n)>$, $\ulcorner 0 \urcorner = <SN(0)>$, $\ulcorner ft_1 \ldots t_n \urcorner = <SN(f), \ulcorner t_1 \urcorner, \ldots, \ulcorner t_n \urcorner>$, $\ulcorner t_1 = t_2 \urcorner = <SN(=), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner>$,

$\ulcorner \sim Q \urcorner = \langle SN(\sim), \ulcorner Q \urcorner \rangle$ and $\ulcorner Q \rightarrow R \urcorner = \langle SN(\rightarrow), \ulcorner Q \urcorner, \ulcorner R \urcorner \rangle$.

3. Let Vble(x) hold if and only if $x = \langle (x)_0 \rangle \& \exists y \le x((x)_0 = 3y)$ holds, so that Vble$=\{x \mid x = \ulcorner x_n \urcorner$ for some n$\}$.

4. Let Fn(x) hold if and only if $\exists y \le x(x = 3y+1 \& \exists i \le y(\exists j \le y (y = OP(i,j))))$ holds, so that Fn$=\{x \mid x = SN(f_{i,j})$ for some i and j$\}$.

5. Let $Fn_n(x)$ hold if and only if $\exists y \le x(x = 3y+1 \& \exists j \le y(y = OP(n,j)))$ holds, so that $Fn_n = \{x \mid x = SN(f)$ for some n-ary f$\}$.

6. By some fairly routine combinatorics, one can find a binary primitive recursive function $M_n(k)$ such that, for each k, $M_n(k)$ is $\ge$ all the numbers of the n-ary function symbols in $L(A_k)$. (Recall that necessarily $n \le k$.) It follows that the predicate $Fn_{n,k}(x)$, which holds if and only if $x = SN(f)$ for some n-ary f in $L(A_k)$, is primitive recursive.

7. Let $Term_k(x)$ hold if and only if $Vble(x) \vee x = \ulcorner 0 \urcorner \vee \exists n \le k (x = \langle SN(f), (x)_1, \ldots, (x)_n \rangle \& Fn_{n,k}(SN(f)) \& \forall i < n(Term_k((x)_{i+1})))$ holds, so that $Term_k = \{x \mid x = \ulcorner t \urcorner$ for some term t of $L(A_k)\}$.

8. Let Term(x) hold if and only if $\exists k \le x(Term_k(x))$ holds.

The binary predicate $Term_k(x)$ is primitive recursive; and for all t, $\ulcorner t \urcorner$ is greater than the least k such that $Term_k(\ulcorner t \urcorner)$ holds. Hence Term(x) is primitive recursive, and holds exactly if $x = \ulcorner t \urcorner$ for some t.

Finding primitive recursive definitions of the following should now be straightforward.

9. EFor$=\{\ulcorner P \urcorner \mid P$ is an elementary formula of $L(A)\}$.

10. For$=\{\ulcorner P \urcorner \mid P$ is a formula of $L(A)\}$.

11. Sub(x,y,z) such that Sub($\ulcorner$t$\urcorner$,$\ulcorner$t'$\urcorner$,$\ulcorner$x$\urcorner$)=$\ulcorner$t(t'/x)$\urcorner$ and Sub($\ulcorner$P$\urcorner$,$\ulcorner$t'$\urcorner$,$\ulcorner$x$\urcorner$)=$\ulcorner$P(t'/x)$\urcorner$.

12. LAx={$\ulcorner$P$\urcorner$|P is a logical axiom of A}.

13. MP={($\ulcorner P_1\urcorner$,$\ulcorner P_2\urcorner$,$\ulcorner P_3\urcorner$)|(P_1,P_2,P_3) is an instance in L(A) of modus ponens}.

14. Subst={($\ulcorner P_1\urcorner$,$\ulcorner P_2\urcorner$)|(P_1,P_2) is an instance in L(A) of the substitution rule}.

15. Ind={($\ulcorner P_1\urcorner$,$\ulcorner P_2\urcorner$,$\ulcorner P_3\urcorner$)|(P_1,P_2,P_3) is an instance in L(A) of the induction rule}.

Now suppose we are given NLAx={$\ulcorner$P$\urcorner$|P is a nonlogical axiom of A}. Then we can define:

16. Ax=LAx$\cup$NLAx,

17. Prf={x|x=<$\ulcorner P_1\urcorner$,...,$\ulcorner P_n\urcorner$> and P_1,...,P_n is a proof in A},

18. Pr={(x,$\ulcorner$P$\urcorner$)|x is the Gödel number of a proof of P in A};

and it follows that, if NLAx is primitive recursive, then so is Pr. We will produce the needed definition of NLAx.

First note that by further refinements of the kind made in 6, there is a 4-ary primitive recursive predicate $Fn_{n,k,j}(x)$ which holds if and only if x=SN(f) for some n-ary f in A_k^j. Notice also that there is a primitive recursive function V such that V(i)=SN($\underset{\sim}{x}_i$). Define as follows:

1. Let $NLAx_0$(x) hold if and only if x=$\ulcorner Z\underset{\sim}{x}_0=0\urcorner$ $\vee$x=$\ulcorner\sim$S0=0$\urcorner$ holds.

Assume that some k is given.

2. Let $NLAx_{k,1}$(x) hold if and only if x=<SN(=),SN(f),

$SN(x_1),\ldots,SN(x_k),V(i)>\&1\leq i\leq k\&Fn_{k,k,1}(x)$ holds. (Recall that the new f in $L(A_k^1)$ are k-ary.)

3. Let $NLAx_{k,2}(x)$ hold if and only if $\exists n\leq k(\exists m\leq k(x= <SN(=),SN(f),SN(\mathfrak{x}_1),\ldots,SN(\mathfrak{x}_n),SN(g),SN(h_1),SN(\mathfrak{x}_1),\ldots, SN(\mathfrak{x}_n),\ldots,SN(h_m),SN(\mathfrak{x}_1),\ldots,SN(\mathfrak{x}_n)>\&1\leq m,n\leq k\&Fn_{n,k,2}(SN(f)) \&Fn_{n,k,2}(SN(h_1))\&\cdots\&Fn_{n,k,2}(SN(h_m))\&Fn_{m,k,2}(SN(g))$ holds. (All new f in $L(A_k^2)$ are $\leq$ k-ary.)

4. Let $NLAx_{k,3}(x)$ hold if and only if ... . (Left to the reader.)

5. Let $NLAx_{k+1}(x)$ hold if and only if $NLAx_k(x)\vee NLAx_{k,1}(x)\vee NLAx_{k,2}(x)\vee NLAx_{k,3}(x)$ holds.

Then so defined for each k, $NLAx_k$ is the set of Gödel numbers of the nonlogical axioms of A_k; and we have shown that the binary predicate $NLAx_k(x)$ is primitive recursive. Thus, since, for each nonlogical axiom P, $\ulcorner P \urcorner$ is strictly greater than the least k such that $NLAx_k(\ulcorner P\urcorner)$ holds, it follows that NLAx(x) holds if and only if $\exists k\leq x(NLAx_k(x))$ holds; so this is the required definition.

For a first application of this Gödel numbering, and to help motivate our undecidability proof, we have the following.

Theorem 2.5. The theory A is incomplete.

Once and for all, let us observe that, if f is a symbol that represents the characteristic function of an n-ary predicate P in A, then, for each choice of numbers $x_1,\ldots,x_n$, we have that $P(x_1,\ldots,x_n)$ holds if and only if $A\vdash f(k_{x_1},\ldots,k_{x_n})=0$. The "only if" part is immediate by the definition of "representable in A". Suppose that $P(x_1,...,x_n)$ does not hold. Then $A\vdash f(k_{x_1},...,k_{x_n})=1$ by the definition of "representable in A". But then 1 is the unique numeral to which the closed term $f(k_{x_1},...,k_{x_n})$ is reducible in A, so it follows that $A\nvdash f(k_{x_1},...,k_{x_n})=0$. To avoid burdensome circumlocutions, this fact will henceforth be regarded as part of the definition of "representable in A".

By the representation theorem, let g be a symbol that represents the characteristic function of the binary predicate $\neg Pr(x_0, Sub(x_1, \ulcorner k_{x_1}\urcorner, \ulcorner \underset{\sim}{x}_1\urcorner))$ in A. Let $p=\ulcorner g(\underset{\sim}{x}_0,\underset{\sim}{x}_1)=0\urcorner$ and consider the formula $g(\underset{\sim}{x}_0,k_p)=0$. Let q be the Gödel number of this formula, and notice that $q=Sub(p,\ulcorner k_p\urcorner,\ulcorner \underset{\sim}{x}_1\urcorner)$.

We have that $A\vdash g(k_n,k_p)=0$ for every n. For suppose not. Say that $A\nvdash g(k_m,k_p)=0$. Then, on the one hand, it is certainly the case that $A\nvdash g(\underset{\sim}{x}_0,k_p)=0$, for otherwise we would have a contradiction by the substitution rule. Hence $\neg Pr(n,q)$ holds for all n by the definition of Pr, so that, in particular, $\neg Pr(m,q)$ holds. But on the other hand, the symbol g is such that $\neg Pr(m, Sub(p,\ulcorner k_p\urcorner,\ulcorner \underset{\sim}{x}_1\urcorner))$, i.e., $\neg Pr(m,q)$, does not hold by the definition of "representable in A".

Hence, since every closed term of L(A) is reducible in A to a unique numeral, we now have that every closed instance of $g(\underset{\sim}{x}_0,k_p)=0$ is a theorem of A. Yet $A\nvdash g(\underset{\sim}{x}_0,k_p)=0$. For otherwise, a proof of it would have some Gödel number, say r, and $Pr(r,q)$ would hold by the definition of Pr, while $Pr(r,q)$ would not hold by the definition of "representable in A". Thus L(A) contains an irrefutable formula which is not a theorem of A, and A is incomplete. ▯

The *recursive functions* may be defined as follows (see Shoenfield [39], Chapter 6, Problem 1): (i) primitive recursive functions are recursive, (ii) if F is recursive and, for each choice of numbers $x_1, \ldots, x_n$, there exist y such that $F(x_1, \ldots, x_n, y) = 0$, then $\mu y(F(x_1, \ldots, x_n, y) = 0)$ is recursive (where μ is the least number operator). If a predicate P is such that F is K_P, one normally writes the latter function $\mu y P(x_1, \ldots, x_n, y)$. A predicate P is a *recursive predicate* if K_P is a recursive function. Intuitively, a function F is recursive if there is a uniform mechanical procedure M such that, for each n, the application of M to n yields F(n). Common phraseology is that a recursive function is "effectively computable", and that one can "effectively determine whether a given sequence is in" a recursive predicate, or that a recursive predicate is "decidable".

Suppose we have a standard enumeration of a formal system S, that is, an ennumeration such that, given any number, we can effectively determine if it is a number of something in S, and in case it is, we can effectively determine what it is a number of. Then S is *decidable* if the set of Gödel numbers of its theorems is recursive, and *undecidable* if not.

Theorem 2.6. The theories **A** and A^-, and the system R are undecidable.

We shall prove only that A is undecidable. The proof for

A^- is exactly the same, once the Gödel numbering of A is modified so that the number of ~S0=0 is not in NLAx. The proof for R is essentially the same, once further modifications are made to obtain a numbering for R. It is worth mentioning that, in the latter case, Theorem 2.3 is of considerable value for adapting the following proof, but is by no means necessary.

For a primitive recursive function F, i is an A-index of F if i=SN(f) for some function symbol f that represents F in A.

Lemma 1. The set of A-indices of the unary primitive recursive functions F for which there exist n such that F(n)=0 is not recursive.

We assume some familiarity with the beginning chapters of Rogers [36], and as well, with Kleene's primitive recursive predicates T_m as they are found in [39] or [27]. In particular, the reader should know two things: (i) A "partial recursive function" is a function for which there is a mechanical procedure M such that, given n, M applied to n either yields F(n) in finitely many steps, or continues indefinitely; or less precisely, it is a function whose domain is a subset of the natural numbers, and which is recursive on its domain. (ii) An m-ary function F is partial recursive if and only if there is a number e such that F and $(\mu z T_m(e,x_1,\ldots,x_m,z))_0$ have the same domain and are equal on that domain. Such a number e is called an "index" of F, but to avoid confusion with the above, we will call it a "K-index" of F. It is clear that every e is the K-index of a unique m-ary partial recursive function, namely, the function just defined in terms of T_m.

Let $W_0, W_1, \ldots$ be a standard enumeration of the recursively enumerable sets. W_e is the range of the unary function with K-index e. We make use of the well-known fact that $P=\{e \mid 0 \varepsilon W_e\}$ is not recursive.

For each e, set $F^e(n)=(\mu z \leq n+1(T_1(e,(n)_0,z) \vee ((z)_0=1 \& \neg \exists w \leq n+1 (T_1(e,(n)_0,w)))))_0$. F^e is a primitive recursive function that enumerates the members of $W_e \cup \{1\}$. By virtue of this definition, there is a uniform mechanical procedure by which one can compute an A-index of F^e for any e; or more exactly, there is a recursive function φ such that, for all e, $\varphi(e)$ is an A-index of the function F^e.

Now let F_e denote the function whose A-index is e (assuming that e is indeed an A-index), and set $U=\{e \mid \exists n F_e(n)=0\}$. Then we have: $e \varepsilon P$ iff $0 \varepsilon W_e$ iff $\exists n F^e(n)=0$ iff $\exists n F_{\varphi(e)}(n)=0$ iff $\varphi(e) \varepsilon U$; which means that, if U were recursive, then P would also be recursive. Hence U is not recursive. □

Let F be a unary primitive recursive function. Define F' by $F'(0)=1$, $F'(Sx)=SSx$ if $F(x)$ and $F'(x)$ are both nonzero, and $F'(Sx)=0$ if not. Then $F'(x)=0$ if there exist $y<x$ such that $F(y)=0$, and $F'(x)=Sx$ if not. It is easy to see that F' is primitive recursive. Let f' be a symbol that represents F' in A. Let g be a symbol that represents the characteristic function of the binary predicate $\neg Pr(F'(x_0), Sub(x_1, \ulcorner k_{x_1} \urcorner, \ulcorner \underset{\sim}{x}_1 \urcorner))$ in A, and set $p=\ulcorner g(f'(\underset{\sim}{x}_0), \underset{\sim}{x}_1)=0 \urcorner$.

<u>Lemma 2</u>. If F is a unary primitive recursive function, and f'

is a symbol which represent F' in A, then $A\vdash g(f'(\underset{\sim}{x}_0),k_q)=0$ if and only if there exist n such that $F(n)=0$.

Suppose we have a proof of $g(f'(\underset{\sim}{x}_0),k_p)=0$ in A. Then where q is the number of this formula, and r is the number of the proof, $Pr(r,q)$ holds by the definition of Pr. Note that every numeral instance of the formula is a theorem of A by the substitution rule, and observe that $q=Sub(p,\ulcorner k_p\urcorner,\ulcorner \underset{\sim}{x}_1\urcorner)$. By the definition of "representable in A", it follows that $\neg Pr(F'(F'(n)),q)$ holds for all n, by which it is immediate that there is no n such that $F'(F'(n))=r$. By the definition of F', this means that there is no n such that $F'(n)=r\dot{-}1$, which in turn, means that there exist $n<r\dot{-}1$ such that $F(n)=0$ provided that $r>1$. To see that $r\neq 0$, note that 0 is the number of the empty sequence, and hence is not the number of a proof. To see that $r\neq 1$, note that the number of a sequence is strictly greater than each of its members, so that: since 0 is the number of the empty sequence, it is not the number of a formula, and 1 also is not the number of a proof.

Now suppose that n is such that $F(n)=0$. Without loss of generality, n is least. Then $F'(n+1)=0$ and $F'(q)=q+1$ for all $q\leq n$ by the definition of F'. Whence $A\vdash f'(k_{n+1})=0$ and $A\vdash f'(k_q)=k_{q+1}$ for all $q\leq n$ by the definition of "representable in A". Let P be the formula $f'(\underset{\sim}{x}_0)=k_0\vee\cdots\vee f'(\underset{\sim}{x}_0)=k_{n+1}$. We claim that $A\vdash P$. For the moment, let us assume that this is proved. Let Q be the formula $g(f'(\underset{\sim}{x}_0),k_p)=0$, and suppose for a contradiction that $A\nvdash Q$. Then $\neg Pr(q,\ulcorner Q\urcorner)$ holds for all q by the definition of Pr, so we certainly have that $\neg Pr(F'(q), \ulcorner Q \urcorner)$ holds for all q. Since $\ulcorner Q \urcorner = Sub(p, \ulcorner k_p \urcorner, \ulcorner x_1 \urcorner)$, it follows that $A \vdash g(k_q, k_p) = 0$ for all q by the definition of "representable in A". We have that $A \vdash k_q = f'(\chi_0) \rightarrow g(k_q, k_p) = 0 \rightarrow Q$ by the equality theorem. Hence $A \vdash g(k_q, k_p) = 0 \rightarrow f'(\chi_0) = k_q \rightarrow Q$ by the symmetry theorem and the tautology theorem. So $A \vdash f'(\chi_0) = k_q \rightarrow Q$ by modus ponens. Since this is for each q, $A \vdash (f'(\chi_0) = k_0 \rightarrow Q) \& \cdots \& (f'(\chi_0) = k_{n+1} \rightarrow Q)$ by the tautology theorem. But then $A \vdash P \rightarrow Q$ by the tautology theorem, so our claim implies that $A \vdash Q$.

Proof of claim: For each q, let k^*_q be the term that is obtained from k_q by replacing 0 by χ_0. We begin by showing that $A \vdash f'(k^*_{n+1}) = 0$. We already have that $A \vdash (f'(k^*_{n+1}) = 0)(0/\chi_0)$, since this is just another way of writing $A \vdash f'(k_{n+1}) = 0$. One may assume that the defining axioms for f' are $f'(0) = S0$ and $f'(S\chi_0) = (SS\chi_0) \cdot h(\chi_0)$ where h represents the characteristic function of $\neg\{x | F(x) = 0$ and $F'(x) = 0\}$ in A. Without writing the definition of h in detail, it should be clear that $A \vdash f'(x) = 0 \rightarrow h(x) = 0$ and that $A \vdash h(x) = 0 \rightarrow f'(Sx) = 0$. Then $A \vdash f'(x) = 0 \rightarrow f'(Sx) = 0$ by the tautology theorem, so that $A \vdash f'(k^*_{n+1}) = 0 \rightarrow (f'(k^*_{n+1}) = 0)(S\chi_0/\chi_0)$ by the substitution rule. Hence $A \vdash f'(k^*_{n+1}) = 0$ by the induction rule.

Using this one can easily show, via the tautology theorem, that $A \vdash P(k^*_{n+1}/\chi_0)$. From this the claim follows by a series of n+1 applications of the induction rule, of which we shall supply only one as an example (Strictly speaking, of course, we are inducting on n.): It followed by our first hypothesis that

$f'(k_n)=k_{n+1}$ is a theorem of A. So $A \vdash P(k_n^*/\underset{\sim}{x}_0)(0/\underset{\sim}{x}_0)$ by the tautology theorem. We have that $P(k_n^*/\underset{\sim}{x}_0)(S\underset{\sim}{x}_0/\underset{\sim}{x}_0)$ is a theorem of A, since this formula is just $P(k_{n+1}^*/\underset{\sim}{x}_0)$. Whence $A \vdash P(k_n^*/\underset{\sim}{x}_0) \rightarrow P(k_n^*/\underset{\sim}{x}_0)(S\underset{\sim}{x}_0/\underset{\sim}{x}_0)$ by the tautology theorem. Hence $A \vdash P(k_n^*/\underset{\sim}{x}_0)$ by the induction rule. ▯

Proof of Theorem 2.6. Exactly as in Lemma 1, let U be the set $\{e \mid \exists n F_e(n)=0\}$. Let G be the set of Gödel numbers of the formulas $g(f'(\underset{\sim}{x}_0),k_p)=0$. Let T be the set of Gödel numbers of the theorems of A. Then $U=G \cap T$ by Lemma 2. Since G is clearly recursive by virtue of the Gödel numbering, and since the intersection of recursive sets is recursive, this means that T is recursive only if U is recursive. Hence, by Lemma 1, T is not recursive, and A is undecidable. ▯

Chapter 3

Semantic Analysis of Free-Variable Theories

In the first section of this chapter, we introduce terminology, and define the notions of "model" and "strong model" for free-variable theories. The second section begins by showing that the chosen definition of "model" provides and"adequate semanticas" for free-variable theories in general. Then a class "admissible theories" is described, and it is proved that strong models are adequate for admissible theories. As an application, we have that the strong semantics is adequate for A and A^{-}, the primary motivating examples. In section three, further applications reveal interesting facts about provability in open first-order theories, and in first-order systems with nonlogical rules.

§ 3.1 Structures, Models and Strong Models

Most semantical notions for free-variable theories are natural counterparts of corresponding notions for first-order theories; exceptions arise from the need to consider nonlogical rules.

A structure S for a free-variable language L consists of a nonempty set dom(S), called the domain of S, together with a function, also denoted by S, that satisfies: (i) for each constant c of L, S(c) is in dom(S), (ii) for each function symbol f of L, if f is n-ary, then S(f) is an n-ary function from dom(S) to itself, (iii) for each predicate symbol p of L, if p is n-ary, then S(p) is an n-ary predicate on dom(S) and, in particular, S(=) is $\{(s,s) \mid s \text{ is in dom}(S)\}$.

Members of dom(S) are <u>individuals of</u> S. If L' is an extension of L and S' is a structure for L', then the (unique) structure S such that dom(S)=dom(S') and such that the function S is the restriction of S' to the set of constants, function symbols and predicate symbols of L is called <u>the restriction of</u> S' <u>to</u> L and is denoted by S'/L. And in this case, S' is called an <u>expansion of</u> S <u>to</u> L'.

Let L be a language and D be a set. For each s in D, we may choose a new (to L) and distinct constant $\underline{s}$ as the <u>name of</u> s. L(D) will denote the extension of L that is obtained by adjoining the names of the members of D to L. When D is the domain of a structure S, one normally writes L(S). With each structure S there is a function S* mapping the closed terms of L(S) to dom(S) and the sentences of L(S) to {0,1} that is defined inductively as follows:

(i) if t is a constant of L, then S*(t)=S(t),

(ii) if t is a name, say $\underline{s}$, then S*(t)=s,

(iii) if t is $ft_1 \ldots t_n$ (say), then $S^*(t)=S(f)(S^*(t_1),\ldots, S^*(t_n))$,

(iv) if P is $pt_1 \ldots t_n$, then $S^*(P)=0$ iff $(S^*(t_1),\ldots,S^*(t_n))$ is in S(p),

(v) if P is $\sim Q$, then S*(P)=0 iff S*(Q)=1,

(vi) if P is $Q \rightarrow R$, then S*(P)=0 iff S*(Q)=1 or S*(R)=0.

As long as confusion will not result, the function S*, and the structure for L(S) consisting of dom(S) and S*, is henceforth denoted simply by S. The reader may easily verify that the function S acts on formulas abbreviated by $\vee$, & and $\rightarrow$ in the expected way.

Proposition 3.1. Let $\underline{s}$ be the name of S(t), where t is a closed term of L(S). If t' is a term of L(S) and no variable other than x occurs in t', then $S(t'(t/x))=S(t'(\underline{s}/x))$. If P is a formula of L(S) and no variable other than x occurs in P, then $S(P(t/x))=S(P(\underline{s}/x))$.

This is proved by induction on the length of terms and the height of formulas. The reader may supply the details. The proposition will readily extend to finite sequences of terms and variables.

Suppose that P is a formula of a language L and that S is a structure for L. An S-instance of P is any sentence of the form $P(\bar{\underline{s}}/\bar{x})$ where the $\underline{s}_i$ are the names of individuals of S. We say that the formula P is valid in S (or that S models P) (Notation: $S\models P$) if $S(P')=0$ for every S-instance P' of P. We adopt the following convention on names: If L' is an extension of L, S' and S are structures for L' and L respectively, and if s is in $dom(S')\cap dom(S)$, then the same constant is used as a name for s in both L'(S') and L(S). The following is immediate.

Proposition 3.2. Let P be a formula of L, and let L' be an extension. If S is a structure for L' such that $S\models P$, then S/L models P. If S is a structure for L such that $S\models P$, then any expansion of S to L' models P.

Since whenever S is a structure for L, and L' is an extension of L, then there is an expansion S' of S to L', it follows that a formula P is valid in every structure for a given language L that contains P if and only if it is valid in every structure for the language determined by P. We say that P is logically valid when either of these conditions holds.

A rule R is valid in a structure S for a language L (S models R) if, for every instance $(\bar{P},R(\bar{P}))$ of R in L, we have that $S\models\bar{P}$ implies that $S\models R(\bar{P})$. Proposition 3.2 asserts that S and S' validate the same formulas of L, so it follows that they also validate the same rules. Thus, while R is said to be logically valid if it is valid in every structure for every L, one notes that, for each instance of R, he can restrict his view to any L such that the instance is in L.

Proposition 3.3. The logical axioms and logical rules are logically valid.

We prove this only for the axiom $P\to Q\to P$, the axiom $x=x$, and the instance $(P,P(t/x))$ of the substitution rule. This will cover the various methods involved in proving the rest. Let L be a language that contains these formulas and let S be a structure for L. Suppose that, for some S-instance $P'\to Q'\to P'$, we have $S(P'\to Q'\to P')=1$. Then $S(P')=0$ and $S(Q'\to P')=1$, which implies that $S(Q')=0$ and $S(P')=1$. Since this is impossible, it follows that $P\to Q\to P$ is valid in S. To see that an S-instance $\underline{s}=\underline{s}$ of $x=x$ is valid in S, only note that (s,s) is in $S(=)$ for every individual s of S. Suppose that $S\models P$ and let $x_1,\ldots,x_n$ be the distinct variables occurring in $P(t/x)$. Consider the S-instance $P(t/x)(\bar{\underline{s}}/\bar{x})$. Now let t' denote $t(\bar{\underline{s}}/\bar{x})$ and let s' be the name of $S(t')$. Then $P(t/x)(\bar{\underline{s}}/\bar{x})$ and $P(t'/x)(\bar{\underline{s}}/\bar{x})$ are just two ways of writing the same formula. Since t' is closed, the latter is just $P(t',\bar{\underline{s}}/x,\bar{x})$ and, since x is not one of the x_i, this may also be written $P(\bar{\underline{s}}/\bar{x})(t'/x)$. Furthermore, since x is not one of the x_i, $P(\bar{\underline{s}}/\bar{x})(\underline{s}'/x)$ may be written $P(\underline{s}',\bar{\underline{s}}/x,\bar{x})$. By proposition 3.1, it follows that $S(P(t/x)(\bar{\underline{s}}/\bar{x}))=S(P(s',\bar{\underline{s}}/x,\bar{x}))=0$. □

By an induction on theorems, this proposition implies that every structure for the language of a theory having no nonlogical axioms or rules is a model, in fact a strong model, of that theory, in the sense of the following.

Definition 3.1. Let T be a free-variable theory. A structure S for L(T) is a *model of* T if S validates every theorem of T. If S is a model of T, and S furthermore validates the rules of T, then S is a *strong model of* T. A formula of L(T) that is valid in every model of T is said to be *valid in* T.

The following is immediate.

Validity Theorem. Every theorem of T is valid in T.

And we also have the

Corollary. If T has a model, then T is consistent.

If T is inconsistent, then $T \vdash x \neq x$. □

Note. By the *standard model of arithmetic* we shall mean the structure N having dom(N) as the natural numbers, N(0) as the number zero, and for each f in L(A), N(f) as the function that is represented by f in A. It is easy to see that N is a model of A. First observe that, for each n, $N(k_n)=n$. This makes it obvious that the axioms of A are valid in N. The induction rule is valid in N by the principle of mathematical induction (whose truth we of course assume). Hence, if $A \vdash P$, then $N \models P$, by induction on the theorems of A.

<u>Remark</u>. It is worth mentioning that there is a stronger notion of "model" for free-variable theories. This is where each rule instance $(\bar{P}, R(\bar{P}))$ has the property: if $x_1, \ldots, x_m$ are the distinct variables in that instance, then $S(R(\bar{P})(\underline{s}_1, \ldots, \underline{s}_m/x_1, \ldots, x_m))=0$ whenever $S(P_i(\underline{s}_1, \ldots, \underline{s}_m/x_1, \ldots, x_m))=0$ for all i. Now, every logical rule has this property in every structure; but it turns out that the induction rule does not have the property even in N. For in N it is certainly not the case that the validity of $P(0/x)$ and $P(S0/x) \to P(SS0/x)$, say, implies the validity of $P(S0/x)$. Thus, this notion of "model" is in fact too strong for our interests, and shall not be considered any further in this thesis.

We conclude this section with a list of examples that will be called upon in the section to follow. The reader may refer to that section now for statements of the theorem on constants and the deduction theorem.

Let T be the minimal theory. Select distinct constants c and c'. By Proposition 3.3 and an induction on the theorems of T, every structure for L(T) is a model of T. T satisfies the theorem on constants by Theorem 3.2. This means that every expansion of a model of T to a structure for the language of $T'=T(c,c')$ is a model of that theory. Hence every structure for $L(T')$ is a model of T' by Proposition 3.2. Let $T''=T'(R)$ where $R=\{(c\neq c', c\neq c), (e=e, e\neq e)\}$ and e is a constant new to $L(T')$. The formula $e=e$ is clearly not a theorem of T'. Let S_0 be any structure for $L(T')$ such that $S_0(c)=S_0(c')$. Then S_0 is a model of T' in which $c\neq c'$ is not valid. So $c\neq c'$ is not a theorem of T' by the definition of "model". Thus T' and T'' have the same theorems, and every structure for $L(T'')$ $(=L(T'))$ is a model of T''.

(i) T'' does not satisfy the theorem on constants. This is obvious, since $T''(e)$ is inconsistent.

(ii) T'' does not satisfy the deduction theorem. We have that $T''(c\neq c')\vdash c\neq c$. Let S_1 be any structure for $L(T'')$ such that $S_1(c)\neq S_1(c')$. Then S_1 is a model of T'' and $S_1\nvDash c\neq c'\rightarrow c\neq c$. So $T''\nvdash c\neq c'\rightarrow c\neq c$ by the definition of "model".

(iii) S_0 is a strong model of T''; S_1 is not. Both of $c\neq c'$ and $c\neq c$ are false in S_0. In S_1, $c\neq c'$ is true.

(iv) $c\neq c'\rightarrow c\neq c$ is a nontheorem of T'' that is valid in every strong model of T''. Firstly, the formula is not valid in the model S_1 of T''. Secondly, if S is a strong model of T'', then $c\neq c'$ must be false, making the formula true.

(v) Let $R'=\{(c=c', c\neq c)\}$. It is easy to see that every structure for $L(T''(R'))$ is a model of $T''(R')$, and that no such models are strong.

§ 3.2 The Main Results

For discussing systems with more than one kind of model, it is convenient to speak in terms of a "semantics" for a system or class of systems. This avenue is taken by Thomason in his recent papers on modal logics, starting with [43]. To be precise, one could say that a semantics for the systems is a class of structures for the languages of the systems, together with a specified subclass of models. A semantics is said to be adequate for a system if, for each formula of the language of the system that is not a theorem, there is a model in that semantics in which the formula is not valid. Since each notion of model naturally induces a notion of validity in systems (cf. Definition 3.1), one readily sees that this is equivalent to saying that we have a "completeness theorem" (if P is valid in the system, then it is a theorem of the system) under that notion of validity. In this thesis, the semantics provided by the notions of 'model' and 'strong model' are correspondingly called the usual semantics and the strong semantics for free-variable theories, and the main semantical results are two such completeness theorems, the first of which we are now in a position to state.

Theorem 3.1. The usual semantics is adequate for all free-variable theories.

Remark. At first, this theorem seems to be an immediate consequence of the first-order completeness theorem; for each free-variable theory T has exactly the same models as a corresponding first-order theory T*, where T* has the same nonlogical axioms as T, and L(T*) is L(T) plus quantification. However, on further examination, one sees that the result does not follow in this manner unless it is known that, for all P in L(T), $T\nvdash P$ implies that $T^*\nvdash P$, which, it turns out, is essentially what we are trying to prove.

Motivation. Our proof of Theorem 3.1 is along the lines of Henkin's well known proof of the completeness theorem for first-order theories [24] in that we build models out of syntactical materials. Thus it is in order to briefly sketch Henkin's proof, and then see how our proof compares. The reader may go to [39] for all undefined terminology and unstated theorems.

Let T be a first-order theory and suppose that Q is a formula of L(T) that is not a theorem of T. We exibit a model of T in which Q is not valid, as follows. An extension T_H of T, called a "Henkin theory", is established such that, for each formula of $L(T_H)$ of the form $\exists xP$, $L(T_H)$ contains a distinct constant e_P, and the formula $\exists xP \rightarrow P(e_P/x)$ is an axiom of T_H. It is proved that T_H is a "conservative extension" of T - e.i., no new formulas of L(T) are theorems of T_H - which implies that Q is not a theorem of T_H. Then the closure Q' of Q is not a theorem of T_H, by the closure theorem; and $T_H(\sim Q')$ is thus consistent, by the corollary to the reduction theorem for consistency (or equivalently, by the deduction theorem). Then, by Lindenbaum's theorem, $T_H(\sim Q)$ has a complete simple extension, say T'. We may observe that the canonical structure exists for T' - i.e., has a nonempty domain –, since T' contains a constant; and in fact, that the canonical structure fo T' is a model of T', since T' is a complete Henkin theory. It follows that the restriction of this structure to L(T) is a model of T; and since it validates ~Q', it invalidates Q, as required.

Now, a direct modification of the above proof fails for for free-variable theories on several counts. Of primary importance are (i) if T has nonlogical rules, then the deduction theorem may fail for T, so that T will not necessarily have a complete simple extension, and (ii) if T furthermore is devoid of constants, then the canonical structure does not exist for T, and the theorem on constants may fail, so that T will not necessarily have a conservative extension for which the canonical structure does exist.

However, we have found a way to build something like the canonical structures for theories that do not necessarily contain constants, and it turns out that for one of these to be a model it is sufficient that T is consistent. Briefly, this is done by allowing an ultrafilter in the Lindenbaum-Tarski algebra for T to take the part of a complete simple extension of T.

So much for the motivation. Let us begin by listing some needed information about Boolean algebras.

A Boolean algebra is a set Γ that is closed with respect to the two binary operations, ∪ and ∩, and the one unary operation, –, which satisfy: (i) $\alpha\cup\beta=\beta\cup\alpha$, (ii) $\alpha\cup(\beta\cup\gamma)=(\alpha\cup\beta)\cup\gamma$, (iii) $(\alpha\cap\beta)\cup\beta=\beta$, (iv) $\alpha\cap(\beta\cup\gamma)=(\alpha\cap\beta)\cup(\alpha\cap\gamma)$, (v) $(\alpha\cap-\alpha)\cup\beta=\beta$, and (vi) the equalities obtained by exchanging $\cup$ for $\cap$ and vice versa in (i) through (v). A nonempty subset Δ of Γ is a <u>filter</u> in Γ if for all $\alpha,\beta\varepsilon\Gamma$ we have: (i) $\alpha,\beta\varepsilon\Delta$ implies $\alpha\cap\beta\varepsilon\Delta$, and (ii) $\alpha\varepsilon\Delta$ implies $\alpha\cup\beta\varepsilon\Delta$. A filter Δ in Γ is <u>proper</u> if $\Delta\neq\Gamma$. A proper filter is <u>maximal</u> or an <u>ultrafilter</u> if for every proper filter Δ' such that $\Delta'\supset\Delta$ we have $\Delta'=\Delta$. As far as we know, Rasiowa and Sikorski [35] is the only single place that one can find proofs of all of the following <u>facts</u>:

(i) Γ contains the <u>unit element</u>, denoted 1, characterized by $\alpha\cup 1=1$ and $\alpha\cap 1=\alpha$, and the <u>zero element</u>, denoted 0, characterized by $\alpha\cup 0=\alpha$ and $\alpha\cap 0=0$. (In fact, $1=\alpha\cup-\alpha$ and $0=\alpha\cap-\alpha$ for all $\alpha\varepsilon\Gamma$.) (ii) Every subset Δ of Γ <u>generates</u> a filter in Γ, the intersection of all filters containing Δ. (iii) A filter is proper if and only if it does not contain 0. (iv) If Δ is a proper filter and $\alpha\notin\Delta$, then the filter generated by $\Delta\cup\{-\alpha\}$ is proper. (v) Every proper filter is contained in an ultrafilter. (vi) An ultrafilter Δ is characterized by the fact that for all $\alpha\varepsilon\Gamma$, exactly one of $\alpha\varepsilon\Delta$ and $-\alpha\varepsilon\Delta$. (vii) A subset Δ of Γ is a filter if and only if $1\varepsilon\Delta$ and $\alpha,\alpha\Rightarrow\beta\varepsilon\Delta$ implies $\beta\varepsilon\Delta$, where $\alpha\Rightarrow\beta$ denotes $-\alpha\cup\beta$, the <u>complement of</u> α <u>relative to</u> β. (viii) A nonempty subset Δ of Γ is a filter if and only if $\alpha\cap\beta\varepsilon\Delta$ exactly when $\alpha,\beta\varepsilon\Delta$.

<u>Note</u>. Not all the above are referred to, but all will be needed. One can see (vii) once he has (a) $\alpha\cap\beta=\alpha\cap(\alpha\Rightarrow\beta)$, (b) $\alpha\Rightarrow(\beta\Rightarrow\alpha\cap\beta)=1$, and (c) $\alpha\Rightarrow\alpha\cup\beta=1$. Proof: In one direction: if Δ is a filter, we have that $1=\alpha\cup-\alpha\varepsilon\Delta$ (for any $\alpha\varepsilon\Delta$) and, by

hypothesis, that $\alpha\cap(\alpha\Rightarrow\beta)\varepsilon\Delta$. By (a), the latter yields that $\alpha\cap\beta\varepsilon\Delta$, so it follows that $\beta=(\alpha\cap\beta)\cup\beta\varepsilon\Delta$. In the other direction: $\alpha,\beta\varepsilon\Delta$ implies that $\alpha\cap\beta\varepsilon\Delta$ by (b) and the hypothesis, so that $\alpha\varepsilon\Delta$ implies that $\alpha\cup\beta\varepsilon\Delta$ by (c) and the hypothesis.

Let T be a theory and, for formulas P and Q of L(T), let $P\sim Q$ mean that $T\vdash P\leftrightarrow Q$. Define $[P]=\{Q|P\sim Q\}$, $\Gamma_T=\{[P]|P$ is a formula of L(T) $\}$, and $\Delta_T=\{[P]|T\vdash P\}$. Each of the following may be verified by means of the tautology theorem: (i) $\sim$ is an equivalence relation on the set of formulas of L(T), (ii) Γ_T is a Boolean algebra with respect to the operations $\cup,\cap$ and $-$ defined by $[P]\cup[Q]=[P\vee Q]$, $[P]\cap[Q]=[P\&Q]$ and $-[P]=[\sim P]$ (This is well-known. Γ_T is called the <u>Lindenbaum-Tarski algebra for</u> T.), (iii) Δ_T is a filter in Γ_T, (iv) Δ_T is a proper filter in Γ_T (in fact, $\Delta_T=\{1\}$) if and only if T is consistent. Note that every filter contains 1 by fact (vii).

<u>Definition 3.2</u>. (Due to S. K. Thomason) Let T be a consistent theory, and let Δ be an ultrafilter in Γ_T. The <u>Δ-canonical structure for</u> T, denoted by $S_{\Delta,T}$, is defined as follows:

(i) $\mathrm{dom}(S_{\Delta,T})=\{[t]|t$ is an (open or closed) term of L(T)$\}$ where $[t]=\{t'|[t=t']\varepsilon\Delta\}$,

(ii) $S_{\Delta,T}(c)=[c]$ for every constant c in L(T),

(iii) $S_{\Delta,T}(f)([t_1],\ldots,[t_n])=[ft_1\ldots t_n]$,

(iv) $([t_1],\ldots,[t_n])\varepsilon S_{\Delta,T}(p)$ if and only if $[pt_1\ldots t_n]\varepsilon\Delta$.

As a notational convenience we let $\underset{\sim}{t}$ denote the name of the equivalence class [t].

Note. It is a routine matter to verify that $[t=t']\varepsilon\Delta$ describes an equivalence relation on the set of terms of L(T), and that the definition of $S_{\Delta,T}(f)$ and $S_{\Delta,T}(p)$ do not depend on the particular representatives t_i chosen from each $[t_i]$. For example: Suppose that $[t_i]=[t_i']$ for i=1,...,n. By the equality theorem, $T\vdash t_1=t_1'\to\cdots\to t_n=t_n'\to pt_1\ldots t_n\to pt_1'\ldots t_n'$; so the class $[t_1=t_1']\Rightarrow\cdots\Rightarrow[t_n=t_n']\Rightarrow[pt_1\ldots t_n\to pt_1'\ldots t_n']$ which is $[t_1=t_1'\to\cdots\to pt_1\ldots t_n\to pt_1'\ldots t_n']$ is in Δ. Since $[t_i]=[t_i']$ means that $[t_i=t_i']\varepsilon\Delta$, it follows that $[pt_1\ldots t_n\leftrightarrow pt_1'\ldots t_n']\varepsilon\Delta$ by fact (vii). Since the latter is equal to $([pt_1\ldots t_n]\Rightarrow[pt_1'\ldots t_n'])\cap([pt_1'\ldots t_n']\Rightarrow[pt_1\ldots t_n])$, facts (viii) and (vii) show that $[pt_1\ldots t_n]\varepsilon\Delta$ if and only if $[pt_1'\ldots t_n']\varepsilon\Delta$. Hence $([t_1],\ldots,[t_n])\varepsilon S_{\Delta,T}(p)$ if and only if $([t_1'],\ldots,[t_n'])\varepsilon S_{\Delta,T}(p)$.

Lemma. Let T be a consistent theory, and let Δ be an ultrafilter in Γ_T. For every $S_{\Delta,T}$-instance $P(\bar{\underset{\sim}{t}}/\bar{x})$ of a formula P of L(T), $S_{\Delta,T}(P(\bar{\underset{\sim}{t}}/\bar{x}))=0$ if and only if $[P(\bar{t}/\bar{x})]\varepsilon\Delta$.

This is proved by induction on the length of terms and the height of formulas. We begin by showing that $S_{\Delta,T}(t)=S_{\Delta,T}(\underset{\sim}{t})$ for every closed term t of L(T). If t is a constant, then $S_{\Delta,T}(t)=[t]$ by the definition of $S_{\Delta,T}$. If t is $ft_1\ldots t_n$ and the t_i are closed terms, then one can show that $S_{\Delta,T}(t)=[t]$ by means of the induction hypothesis and the methods described in the above note. The desired equality follows, since $\underset{\sim}{t}$ names [t].

Now, in order to apply the present notion of truth, we want to know that, for an open t, if $t(\bar{\underset{\sim}{t}}/\bar{x})$ is a closed term of $L(T)(S_{\Delta,T})$, then $S_{\Delta,T}(t(\underset{\sim}{\bar{t}}/\bar{x}))=[t(\bar{t}/\bar{x})]$. If t is a variable, then we are done by the definition of name. Suppose that t is $ft_1'\ldots t_m'$ and that $S_{\Delta,T}(t_i'(\underset{\sim}{\bar{t}}/\bar{x}))=[t_i'(\bar{t}/\bar{x})]$ for i=1,...,m. Then

$$
\begin{aligned}
S_{\Delta,T}(t(\underset{\sim}{\bar{t}}/\bar{x})) &= S_{\Delta,T}(ft_1'(\underset{\sim}{\bar{t}}/\bar{x})\ldots t_m'(\underset{\sim}{\bar{t}}/\bar{x})) \\
&= S_{\Delta,T}(f)(S_{\Delta,T}(t_1'(\underset{\sim}{\bar{t}}/\bar{x})),\ldots,S_{\Delta,T}(t_m'(\underset{\sim}{\bar{t}}/\bar{x}))) \\
&= S_{\Delta,T}(f)([t_1'(\bar{t}/\bar{x})],\ldots,[t_m'(\bar{t}/\bar{x})]) \\
&= [ft_1'(\bar{t}/\bar{x})\ldots t_m'(\bar{t}/\bar{x})]=[t(\bar{t}/\bar{x})].
\end{aligned}
$$

Suppose now that P is an elementary formula; say P is $pt_1'\ldots t_m'$. We have the following: $S_{\Delta,T}((pt_1'\ldots t_m')(\underset{\sim}{\bar{t}}/\bar{x}))=0$

$$
\begin{aligned}
&\text{iff } (S_{\Delta,T}(t_1'(\underset{\sim}{\bar{t}}/\bar{x})),\ldots,S_{\Delta,T}(t_m'(\underset{\sim}{\bar{t}}/\bar{x})))\in S_{\Delta,T}(p) \\
&\text{iff } ([t_1'(\bar{t}/\bar{x})],\ldots,[t_m'(\bar{t}/\bar{x})])\in S_{\Delta,T}(p) \\
&\text{iff } [(pt_1'\ldots t_m')(\bar{t}/\bar{x})]\in S_{\Delta,T}(p).
\end{aligned}
$$

Given this, the rest of the induction is easily completed. Where P is $\sim Q$, merely observe that, since Δ is maximal, fact (vi) yields $[Q(\underset{\sim}{\bar{t}}/\bar{x})]\not\in\Delta$ if and only if $[P(\underset{\sim}{\bar{t}}/\bar{x})]\in\Delta$. And when P is $Q\rightarrow R$, note that $[Q(\underset{\sim}{\bar{t}}/\bar{x})]\not\in\Delta$ or $[R(\underset{\sim}{\bar{t}}/\bar{x})]\in\Delta$ implies $[Q(\underset{\sim}{\bar{t}}/\bar{x})\rightarrow R(\underset{\sim}{\bar{t}}/\bar{x})]=-[Q(\underset{\sim}{\bar{t}}/\bar{x})]\cup[R(\underset{\sim}{\bar{t}}/\bar{x})]\in\Delta$ by the maximality of Δ and the definition of filter; and conversely by the maximality of Δ and fact (vii). □

Remark. We are now in a position to prove Theorem 3.1. One will notice that the use of fact (v) in obtaining an ultrafilter circumvents the need for considering a complete simple extension, and hence subsumes Lindenbaum's Theorem. Fact (iv) plays the part of the reduction theorem for consistency and, since it also applies whether Q is open or closed, it also subsumes the case that the theory in question does not contain constants. It is worth emphasizing that one may have this proof algebraically, not just because this method duplicates the desired metamathematical phenomena, but more because it disregards many of the strictly metamathematical properties that are not directly involved.

Proof of Theorem 3.1. Suppose that some formula Q of L(T) is not a theorem of T. Then T is consistent; and so Δ_T is a proper filter in Γ_T. Hence, by fact (iv), the filter generated by $\Delta_T \cup \{[\sim Q]\}$ is also proper in Γ_T. Let Δ be an ultrafilter containing this latter, and consider the Δ-canonical structure for T. By the lemma, a formula P of L(T) is valid in $S_{\Delta,T}$ if and only if $[P'] \in \Delta$ for every substitution instance P' of P. Since, for every such P', we have $T \vdash P'$ whenever $T \vdash P$, it follows that $S_{\Delta,T}$ is a model of T. Clearly, $S_{\Delta,T}(Q(\bar{\underline{x}}/\bar{x}))=1$. Hence Q is not valid in T. ▯

Corollary. Every consistent theory has a model.

Just take the Δ-canonical structure, where Δ is any ultrafilter in Γ_T. ▯

So much for the usual semantics for free-variable theories. We now turn to the problem of establishing a completeness theorem with respect to the strong semantics, which is more difficult. The situation is this: Examples (iv) and (v) at the end of the preceding section show that the strong semantics is not adequate for every free-variable theory. Thus, what we want is a characterization of those theories for which the strong semantics is adequate. Furthermore, we want a characterization that is useful; that is, it should enable us to determine readily whether a given theory is of the kind so characterized. Since the adequacy of the strong semantics clearly depends on the nature of the nonlogical rules of a theory, this means that the best possible result would be a purely syntactical characterization of those rules which a theory for which the strong semantics is adequate may have.

In what follows we present a partial solution to the above problem. The method of attack, and the final results, have been more or less as follows: (i) Since the strong semantics is adequate for the two theories of arithmetic, A and A^{-},(which is established in the following by Theorem 3.6), an examination of the induction rule yields the notion of an "admissible" free-variable theory, together with a set of "conditions" on the nonlogical rules of a theory that, in various combinations, will ensure that the theory is admissible. (ii) In view of the above mentioned "conditions", it is believed that the notion of "admissibility" encompases any reasonable theories that might eventually be discovered. (iii) While we do not know if the strong semantics is adequate for any nonadmissible theories, it should be pointed out that, other than such elementary examples as were mentioned above, we know of only one nonadmissible theory (to be discussed). (iv) Of the "conditions" on nonlogical rules, few are purely syntactical, while the rest entail the concept of provability in a given theory. Thus clearly, while we have made some gains, it is likely that further gains are to be made.

However, at this point we may rightly be reminded that, so far, the induction rule is our only example of a nonlogical rule that cannot be replaced satisfactorily by a set of axioms, thus making A and A^- our only really interesting applications, and so, the worthwhileness of such a general investigation as is described above may surely be questioned. Thus, to counter this, the author would like to say here that the study began simply because there are two very interesting examples, and the study was carried on, partly in the belief that more such examples would appear, but mainly because he felt that some questions had been posed which should be answered to some degree of satisfaction. And since no new interesting examples have appeared, the author consoles himself for the time being, in that we at least have a semantical analysis of some theories of the arithmetic of the natural numbers, and he believes that any contribution to our knowledge of something as fundamental to mathematics should be able to stand on its own merit.

Since the notion of "admissible" entails some of the "conditions", it is convenient to present all of these first, and while at it, to prove Theorem 3.2, a technical result which will eventually be used to show how the "conditions" serve the acclaimed purpose.

Condition 1. Each instance of a nonlogical rule of T is in L(T).

Condition 2. For each set C of constants that are new to

$L(T)$, if $(P_1,\ldots,P_m)$ is an instance in $L(T(C))$ of a nonlogical rule of T, and if $\bar{e}$ consists of the distinct constants in C that occur in the P_j, then, where $\bar{y}$ is a distinguished sequence of variables of $L(T)$ that do not occur in any P_j, and where P_j' is the formula of $L(T)$ that is obtained from P_j by replacing each e_i by y_i, $(P_1',\ldots,P_m')$ is an instance of that same rule of T. (The sequence $\bar{y}$ is distinguished if $y_i=y_j$ only when $i=j$.)

Condition 3. T satisfies the Theorem on Constants: For every set C of constants that are new to $L(T)$, and for every formula P of $L(T)$, the following are equivalent: (i) $T\vdash P$, (ii) $T(C)\vdash P(\bar{e}/\bar{x})$ for every sequence $\bar{e}$ of constants in C, (iii) $T(C)\vdash P(\bar{e}/\bar{x})$ for some distinguished sequence of constants in C. (Notice that our notational conventions do not imply that $P(\bar{e}/\bar{x})$ need be closed.)

Condition 4. (i) For each formula Q of $L(T)$, and for each instance $(P_1,\ldots,P_m,R(P_1,\ldots,P_m))$ in $L(T)$ of a nonlogical rule of T, we have that $T\vdash Q\rightarrow R(P_1,\ldots,P_m)$ whenever $T\vdash Q\rightarrow P_i$ for all $i=1,\ldots,m$. (ii) For each sequence $\bar{e}$ of constants that are new to $L(T)$, we have that $R(P_1(\bar{e}/\bar{x}),\ldots,P_m(\bar{e}/\bar{x}))$ is $R(P_1,\ldots,P_m)(\bar{e}/\bar{x})$.

Condition 5. Same as Condition 4 (i) except for Q a sentence.

Condition 6. T satisfies the Deduction Theorem: For sentences Q and formulas P of $L(T)$, $T(Q)\vdash P$ if and only if $T\vdash Q\rightarrow P$.

Condition 7. For every set C of constants, the deduction theorem holds for $T(C)$.

Condition 8. (Uniformity Condition) There exists a constant c (where c is in L(T) if T contains some constants) such that, for any extension T' of T(c) whose nonlogical rules are exactly those of T, and for any instance $(\bar{P}, R(\bar{P}))$ in L(T') of one of these rules, if E is the set of closed L(T(c))-instances of the P_i, then we have that every closed L(T(c))-instance of $R(\bar{P})$ is a theorem of T'(E). (An <u>L(T)-instance</u> of P is a formula of the form $P(\bar{t}/\bar{x})$ where the t_i are terms of L(T).)

<u>Theorem 3.2</u>. 1⇒2, 2⇒3, 4⇒5, 5⇒6, 1&6⇒7, 3&4⇒7.

1⇒2: This is clear, since Condition 1 means that no instance of a nonlogical rule of T contains a symbol that is new to L(T).

2⇒3: We always have (i)⇒(ii) by the substitution rule, and it is trivial that (ii)⇒(iii). Thus we need only show that (iii)⇒(i). Suppose that $P_1,\ldots,P_k$ is a proof of $P(\bar{e}/\bar{x})$ in T(C), where $\bar{e}$ is a distinguished sequence of members of C. Let $\bar{y}$ be a distinquished sequence of variables of L(T) that do not occur in any of the P_j. Then, where P_j' is the formula that is obtained from P_j by replacing each e_i respectively by y_i, $P_1',\ldots,P_k'$ is a proof of $P(\bar{y}/\bar{x})$ in T. For consider any P_j. If this formula is an axiom of T(C), then P_j' is clearly an axiom of T, since such a replacement in a logical axiom yields an axiom of the same form, and the nonlogical axioms of T(C) are just those of T, which do not contain symbols that are new to L(T). If P_j' is the conclusion in some instance $(P_{j_1},\ldots,P_{j_m})$ of some rule R of T, then either (i) R is a logical rule, in which case we clearly have that $(P_{j_1}',\ldots,P_{j_m}')$ is an instance in L(T) of the same rule, or (ii) R is a nonlogical rule of T, and we have the same by Condition 2. Since P is just $P(\bar{y}/\bar{x})(\bar{x}/\bar{y})$, it follows that $T\vdash P$ by the substitution rule.

4⇒5: This is trivial.

5⇒6 and 1&6⇒7: These are similar to 3&4⇒7.

3&4⇒7: ⇐: If $T(C)\vdash Q\to P$, then certainly $T(C)(Q)\vdash Q\to P$, so that $T(C)(Q)\vdash P$ by modus ponens. So in this direction we are done.

⇒: Suppose that $T(C)(Q)\vdash P$ where Q is a sentence of $L(T(C))$. We induct on the theorems of $T(C)(Q)$. If P is an axiom, then either it is an axiom of $T(C)$, or it is Q, and in either case, $T(C)\vdash Q\to P$ by the tautology theorem. Suppose that P is the conclusion of an instance $(P_1,\ldots,P_m,R(P_1,\ldots,P_m))$ of some rule R of T, where the P_i are theorems of $T(C)(Q)$. If R is modus ponens, then this instance has the form $(P',P'\to P,P)$, and the induction hypothesis is that $T(C)\vdash Q\to P'$ and $T(C)\vdash Q\to P'\to P$. It follows that $T(C)\vdash Q\to P$ by the tautology theorem. If R is the substitution rule, then the instance has the form $(P',P'(t/x))$, and the induction hypothesis is that $T(C)\vdash Q\to P'$. Then $T(C)\vdash (Q\to P')(t/x)$, and since Q is a sentence, this is just another way of writing $T(C)\vdash Q\to P'(t/x)$. Suppose that R is a nonlogical rule of T. Let $Q',P_1',\ldots,P_m',P'$ be some formulas of $L(T)$, and $\bar{e}$ the members of C, such that Q is $Q'(\bar{e}/\bar{x})$, each P_j is $P_j'(\bar{e}/\bar{x})$ and P is $P'(\bar{e}/\bar{x})$. Then the induction hypothesis is that $T(C)\vdash (Q'\to P_j')(\bar{e}/\bar{x})$ for each j, so it follows that $T\vdash Q'\to P_j'$ for each j by Condition 3. Hence $T\vdash Q'\to R(P_1',\ldots,P_m')$ by Condition 4 (i), which means that $T\vdash Q'\to P'$ by Condition 4(ii). Then $T(C)\vdash Q'\to P'$, so that $T(C)\vdash Q\to P$ by the substitution rule. ▯

Definition 3.3. A theory T is a weakly admissible theory if either (i) T is complete, or (ii) T satisfies the uniformity condition, and where c is the constant of that condition, we have that (a) T(c) satisfies the deduction theorem, and (b) T(c) is consistent provided T is consistent. A theory T is an admissible theory if either (i) T is complete, or (ii) T satisfies the uniformity condition, and where c is the constant of that condition, we have that there exists a set C of $\aleph_0$ constants that are new to L(T(c)) such that (a) T({c}UC) satisfies the deduction theorem, and (b) the three conditions of the theorem on constants are equivalent when CU{c} is taken in place of C.

Notes. (i) For T to be an admissible theory, it is sufficient that it satisfy Conditions 3,7 and 8. Hence Theorem 3.2 shows that it is sufficient that T satisfy Conditions 1,4 and 8, or Conditions 2,4 and 8. In particular, this makes it trivial that theories without nonlogical rules are admissible.

(ii) If T is admissible, then T is weakly admissible. For let c be the constant of the uniformity condition. To see that T(c) satisfies the deduction theorem, let Q be a sentence and P be a formula of L(T(c)) such that $T(c)(Q)\vdash P$. Then, where C is as hypothesized in the definition of "admissible theory", $T(\{c\}\cup C)(Q)\vdash P$, so that $T(\{c\}\cup C)\vdash Q\rightarrow P$ by (a) of the definition. $T(c)\vdash Q\rightarrow P$ then follows by (b). To see that T(c) is consistent if T is, suppose otherwise. Then T({c}UC) is inconsistent, so that $T(\{c\}\cup C)\vdash P\&\sim P$ for some formula P of L(T), which implies that $T\vdash P\&\sim P$ by (b).

We shall consider the following as lemmas for Theorem 3.5. Theorems 3.3 and 3.4 are dealt with first, simply because they also are direct consequences of the lemmas, and lead up to our main theorem in a natural way.

An extension of the form T(E), where E is a set of formulas of L(T), is a simple extension of T. It is a sentential extension of T if every formula in E is a sentence.

Lemma 1. If T satisfies the deduction theorem, then so does every sentential extension of T.

We have already seen that for any T, if $T \vdash Q \to P$ then $T(Q) \vdash P$ by modus ponens. Hence, what we want to show is that, if $T(Q) \vdash P$ implies $T \vdash Q \to P$, then this implication also holds when T is replaced by one of its sentential extensions.

Let E be a set of sentences of L(T), and furthermore let Q be a sentence and P a formula of L(T) such that $T(E)(Q) \vdash P$. Suppose that $Q_1, \ldots, Q_n$ are the members of E that appear in some proof of P in T(E)(Q). Then $T(\bar{Q}, Q) \vdash P$, so $T(Q_1 \& \cdots \& Q_n \& Q) \vdash P$ by the tautology theorem. Hence $T \vdash Q_1 \& \cdots \& Q_n \& Q \to P$, since T satisfies the deduction theorem by hypothesis. Then $T \vdash Q_1 \to \cdots \to Q_n \to Q \to P$ by the tautology theorem, so that $T(\bar{Q}) \vdash Q \to P$ by n applications of modus ponens. Hence $T(E) \vdash Q \to P$. □

Lemma 2. If T satisfies the deduction theorem, then it sa isfies: For sentences Q of L(T), $T \vdash Q$ if and only if $T(\sim Q)$ is inconsistent.

It is clear that for any T, if $T \vdash Q$ then $T(\sim Q)$ is inconsistent. Suppose that $T(\sim Q)$ is inconsistent and that T satisfies the deduction theorem. Then $T(\sim Q)\vdash P$ and $T(\sim Q)\vdash \sim P$ for some formula P of L(T), and it follows that $T\vdash \sim Q\rightarrow P$ and $T\vdash \sim Q\rightarrow \sim P$. But then $T\vdash Q$ by the tautology theorem. ▯

Lemma 3. If T satisfies the uniformity condition, c is the constant of that condition, C is any (possibly empty) set of constants, and E is any (possibly empty) set of formulas of $L(T(\{c\}\cup C)$ such that $T'=T(\{c\}\cup C,E)$ is consistent and satisfies the deduction theorem, then T' has a complete simple extension.

Sublemma. If T is consistent and satisfies the deduction theorem, then T has a sententially complete sentential extension.

We shall use the method of [39] for proving Lindenbaum's Theorem. A set J of subsets of a set A has finite character if, for every subset B of A, we have that B is in J if and only if every finite subset of B is in J. A member B of J is maximal if, for every member B' of J, we have that $B'\supset B$ implies that $B'=B$. We borrow from set theory the Teichmuller-Tukey Lemma: If J is a nonempty set of subsets of a set A and has finite character, then J has a maximal member.

Let $J=\{E|T(E)$ is a consistent sentential extension of $T\}$. Then J has finite character. For, if some E has a finite subset E' not in J, then T(E) is an extension of an inconsistent theory, and E is not in J. And if some set E is not in J, by letting E' be the set of formulas in E that appear in a proof of some contradiction $P\&\sim P$ in T(E), we see that T(E') is inconsistent, and hence that E' is a finite subset of E that is not in J.

Now, since T is consistent, J contains the empty set. So J has a maximal member, say E, by the Teichmuller-Tukey lemma; and clearly, T(E) satisfies the deduction theorem by Lemma 1. Suppose that, for some sentence Q of L(T), $T(E)\nvdash Q$. Then Lemma 2 says that $T(E)(\sim Q)$ is consistent. Since E is maximal, this means that $\sim Q$ is in E. Thus $T(E)\vdash\sim Q$, and T(E) is sententially complete. □

<u>Proof of Lemma 3</u>: The theory T' has a sententially complete sentential extension T" by the sublemma. Let E' be the set of formulas P of L(T") such that every closed L(T")-instance of P is a theorem of T". Then, by Note (ii) immediately following Definition 2.2, T"(E') is the required extension of T', if it is consistent. Since T" is consistent by the definition of "sententially complete", it is sufficient to show that every closed L(T(c))-instance of a theorem of T"(E') is a theorem of T".

We induct on the theorems of T"(E'). Suppose that P is an axiom. If P is an axiom of T", then we are done by the substitution rule. If P is a formula in E', then we are done by the definition of E'. Suppose that P is the conclusion of an instance $(P_1,\ldots,P_m,R(P_1,\ldots,P_m))$ of a rule R of T, where each P_i is a theorem of T"(E'). The induction hypothesis is that every closed L(T(c))-instance of each P_i is a theorem of T". Consider a closed L(T(c))-instance $P(\bar{t}/\bar{x})$ of P. If R is modus ponens, then the rule instance is $(Q,Q\to P,P)$ for some Q. Since $(Q\to P)(\bar{t}/\bar{x})$ is just $Q(\bar{t}/\bar{x})\to P(\bar{t}/\bar{x})$, it is immediate that $(Q(\bar{t}/\bar{x}),$

$(Q \to P)(\bar{t}/\bar{x}), P(\bar{t}/\bar{x}))$ is an instance of modus ponens, and hence that $P(\bar{t}/\bar{x})$ is a theorem of T" by modus ponens. If R is the substitution rule, then, in an analogous manner, $P(\bar{t}/\bar{x})$ is a theorem of T" by that same rule. Suppose that R is a nonlogical rule. Let E" be the set of closed L(T(c))-instances of the P_i. Since T" is an extension of T(c) with nonlogical rules exactly those of T, it follows that $T''(E'') \vdash P(\bar{t}/\bar{x})$ by the uniformity condition. Hence $T'' \vdash P(\bar{t}/\bar{x})$, for the induction hypothesis implies that the theories T" and T"(E") have precisely the same theorems. □

Note. In the proofs of the following Theorems 3.3, 3.4 and 3.5, the easy case - that T is (weakly) admissible because T is complete - is omitted.

Theorem 3.3. A consistent weakly admissible theory that contains a constant has a complete simple extension.

If T is a consistent theory that is weakly admissible then, where c is the constant of the uniformity condition, the hypotheses of Lemma 3 are satisfied by taking C and E empty, so that T'=T(c). Hence, by that lemma, T(c) has a complete simple extension. And since T further contains some constants, the uniformity condition says that T(c)=T. □

A model S of a theory T is a complete model of T if, for for every formula P of L(T), P is valid in S exactly if $T \vdash P$. Complete models are necessarily strong models. For suppose that $(\bar{P}, R(\bar{P}))$ is a rule instance in L(T) such that each P_i is valid in in some complete model S of T. Then $T \vdash P_i$ for each i, by the definition of "complete model"; so $T \vdash R(\bar{P})$ by the definition of "theorem"; and this implies that R is valid in S, because S is a model of T.

<u>Theorem 3.4</u>. A consistent weakly admissible theory has a strong model.

It is clear from the preceding proof that under these conditions, a theory T that does not contain a constant has a complete extension, though not necessarily a simple one. That is, we have a complete simple extension of T'=T(c) where c is the constant of the uniformity condition.

Let T" be a complete extension of T. Then T" is consistent, and therefore has a model by Theorem 3.1. It is easy to show that a model of a complete theory is complete. And we have just seen that complete models are strong. Hence, since the rules of T" are the rules of T, there is a (strong) model of T" whose restriction to L(T) is a strong model of T. □

<u>Theorem 3.5</u>. The strong semantics is adequate for all admissible theories.

Let T be an admissible theory, and suppose that P is a formula of L(T) such that $T \nvdash P$. **Then T is a consistent theory.** Let c and C be as in the definition of "admissible", and let $\bar{e}$ be a distinguished sequence of constants in C such that $P(\bar{e}/\bar{x})$ is closed. Since the theorem on constants holds when C is replaced by {c}∪C, T({c}∪C) is consistent and does not contain a proof of $P(\bar{e}/\bar{x})$; and since T({c}∪C) satisfies the deduction theorem, the theory $T'=T(\{c\}\cup C, \sim P(\bar{e}/\bar{x}))$ satisfies the deduction theorem by Lemma 1, and that T' is consistent by Lemma 2. Hence we are in the conditions of Lemma 3, so that, as in the proof of Theorem 3.4, T' has a complete simple extension T", which in turn has a complete model S such that S/L(T) is a strong model of T. Since an instance of the formula $\sim P$ is an axiom of T", it is clear that $S/L(T) \nvDash P$. ▯

Notes. (i) If T does not satisfy the deduction theorem, then not only is T not admissible, but the strong semantics definitely is not adequate for T. For assume that the strong semantics is adequate for T, and suppose that $T(Q) \vdash P$, where Q is a sentence and P a formula of L(T). If $T \nvdash Q \to P$, then there is a strong model S of T such that $S(Q)=0$ and $S \nvDash P$. But then S models the nonlogical axioms of T(Q), so it follows by induction on the theorems of T(Q), that S does model P. This contradiction shows that $T \vdash Q \to P$, and hence that T satisfies the deduction theorem.

(ii) We have not been able to determine if the theorem on constants is also needed in this same sense. It is clear, however, that at least something like the theorem on constants must be called upon for the purposes of the foregoing proof; and that there is a method of proof which completely bypasses an assumption of this kind seems doubtful.

Theorem 3.6. The theories of arithmetic, A and A^-, are admissible theories.

It is sufficient to deal only with A, since the proof for A^- is exactly the same. We show (i) that A satisfies Condition 2, (ii) that, for any set C of constants, A(C) satisfies Condition 5, and (iii) that A satisfies the uniformity condition. The theorem will then follow by Theorem 3.2.

(i) Consider an instance $(P(0/x), P\to P(Sx/x), P)$ of the induction rule in L(A(C)), where C is a set of constants that are new to L(A). If $\bar{e}$ are the distinct constants in C that appear in this instance, and $\bar{y}$ is a distinguished sequence of variables of L(A) that do not appear in it, then clearly, the triple that is obtained from it by replacing each e_i respectively by y_i, is an instance of the induction rule in L(A).

(ii) Consider an instance $(P(0/x), P\to P(Sx/x), P)$ of the induction rule in L(A(C)), where C is any set of constants. Suppose that Q is a sentence of L(A(C)) such that $A(C)\vdash Q\to P(0/x)$ and $A(C)\vdash Q\to P\to P(Sx/x)$. Then, since Q is a sentence, the former can be written $A(C)\vdash (Q\to P)(0/x)$. And by the tautology theorem, the latter yields that $A(C)\vdash (Q\to P)\to(Q\to P(Sx/x))$, which, since Q is a sentence, can be written $A(C)\vdash (Q\to P)\to(Q\to P)(Sx/x)$. Hence $A(C)\vdash Q\to P$ by the induction rule.

(iii) Since L(A) contains the constant 0 (and no others), we must show that A satisfies the uniformity condition when 0 is taken as the constant of that condition, i.e., when L(A(c))= L(A). Consider the instance $(P(0/x), P\to P(Sx/x), P)$ of the induction rule in L(A). Let E be the set of closed L(A)-instances of $P(0/x)$ and $P\to P(Sx/x)$, and suppose that $P(\bar{t}, t/\bar{x}, x)$ is a closed

$L(A)$-instance of P. We need that $A(E)\vdash P(\bar{t},t/\bar{x},x)$. Recall that, since t is a closed term of $L(A)$, it is reducible in A to a unique numeral, say k_n. It follows that we only need that $A(E)\vdash P(\bar{t},k_n/\bar{x},x)$. Since E contains all the formulas $P(\bar{t},0/\bar{x},x)$, $P(\bar{t},0/\bar{x},x)\rightarrow P(\bar{t},k_n/\bar{x},x),\ldots,P(\bar{t},k_{n-1}/\bar{x},x)\rightarrow P(\bar{t},k_n/\bar{x},x)$, we have it by n applications of modus ponens. $\square$

The general theory of lattices (two good references are _Lattice Theory_ by G. Birkoff and _Lattice Theory_ by T. Donnellan) also provides some examples. By _Lattice Theory_ we shall mean the free-variable theory L whose language contains the binary function symbols $\cap$ and $\cup$, and whose nonlogical axioms are the formulas of $L(L)$ having the forms (i) $x\cap y=y\cap x$, (ii) $x\cap(y\cap z)=(x\cap y)\cap z$, and (iii) $x\cap(x\cup y)=x$, together with their duals, where the _dual_ of an equation is the equation that results from replacing each occurrence of $\cap$ by an occurrence of $\cup$, and vice versa. By L_0 we shall mean the theory with $L(L_0)=L(L)$, whose nonlogical axioms are those of the forms (i), (ii) and (iii) only, and which has as its single nonlogical rule, the _duality rule_, consisting of all pairs (P,P^*) where P^* is the dual of P. It is clear that L and L_0 have the same theorems.

The duality rule is the formal expression of the well-known "Duality Principle" which asserts that an equation is a theorem of (general) lattice theory if and only if its dual equation is also a theorem. It is worth emphasizing that, while this principle allows us to infer that $L\vdash P$ iff $L\vdash P^*$, it does not tell us, what is usually false, that $L\vdash P\leftrightarrow P^*$.

Now, the theory L is admissible, simply because it has no nonlogical rules. On the other hand, it is easy to see that L_0 satisfies Condition 2 and the uniformity condition; and since $L(L_0)$ does not contain sentences, it is trivial that L_0 satisfies the deduction theorem. However, there is no infinite set C of constants such that $L_0(C)$ satisfies the deduction theorem. To see this observe that (i) every lattice is a model of L, (ii) L and L_0 have the same theorems, and hence the same models, and (iii) since L_0 satisfies the theorem on constants, given any set C of constants, any expansion of a model of L_0 to a structure for $L(L_0(C))$ is a model of $L_0(C)$. It follows that the four-element lattice $\mathcal{L}$ defined by $a_1>a_2,a_3$; a_2 and a_3 are unrelated; and $a_2,a_3>a_4$; together with the assignments of a_1, a_2,a_3 respectively to some distinct constants c_1,c_2,c_3 in a given infinite set C, is a model of $L_0(C)$. Let Q be the sentence $c_2 \cup c_3=c_1$, P be $c_2 \cap c_3=c_1$, and note that $Q \rightarrow P$ is not valid in $\mathcal{L}$. Then $L_0(C)(Q) \vdash P$ by the duality rule, while $L_0(C) \nvdash Q \rightarrow P$.

Hence, by Note (i) following Theorem 3.5, this shows that the strong semantics is not adequate for $L_0(C)$ where C is any infinete set of constants; and since L_0 satisfies the theorem on constants, it follows that the strong semantics is also not adequate for L_0. Thus we have two theories, L and L_0, such that the strong semantics is adequate for one and not the other, even though both theories have exactly the same theorems.

Of course, none of this should be too surprising to anyone familiar with lattices. For first of all, the duality principle is not meant to apply to statements involving named elements of a particular lattice, but only to free-variable statements about lattices in general; and secondly, a strong model of L_0 would have to be a lattice that is self-dual, and one would certainly expect that there are unprovable statements that are nevertheless true about every such lattice. Also, it should not be surprising that L_0 is weakly admissible. We'll omit the proof (that the deduction theorem holds for $L_0(c)$, for any constant c), and merely point out that L_0 has the one element lattice as a strong model.

Regarding the definition of "rule of proof", there are two things that deserve mentioning. Both of them are tied up with Conditions 1 through 8, Theorem 3.2, and the definition of admissibility. First, by now it should be clear why we have not followed the customary practice of describing a rule by means of a "schema", i.e., a law which tells how one may infer a formula of a certain form from some formulas having certain other forms. If one wishes to isolate those characteristics of the rules of a theory which ensure that something about the theory is true, it is best to begin with the most general notion of a rule that is available. Surely, restriction of one's self to only rules that are "schematic" could severely cripple the ensuing investigation.

However, it happens that any "reasonable" rule that one can imagine is describable by means of some schema or set of schemas. Hence, the conditions sought after, once they are found, might well be reduced to some conditions on a rule schema.

Through formalizing the metalanguage one can arrive at a precise and fairly comprehensive notion of a schematic rule. And in the case of the foregoing conditions, he can proceed to describe some "admissible" rule schemas; that is, he can supply some descriptions of schemas such that, if all the rules of a theory are schematic, and moreover, have schemas of certain of these descriptions, then that theory satisfies certain of Conditions 1 through 8. Condition 2 is certainly amenable to such a description. A theory T, and every extension T(C) of T, satisfies Condition 4, if every nonlogical rule R of T has the property that, for sentences Q, if $(\bar{P},R(\bar{P}))$ is an instance of R, then so is $(Q\rightarrow P_1,\ldots,Q\rightarrow P_n,Q\rightarrow R(\bar{P}))$. And a theory T satisfies the uniformity condition if every nonlogical rule R of T has the property that, for sequences of terms $\bar{t}$, if $(P_1,\ldots,P_m, R(P_1,\ldots,P_m))$ is an instance of R, then so is $(P_1(\bar{t}/\bar{x}),\ldots, P_m(\bar{t}/\bar{x}),R(P_1,\ldots,P_m)(\bar{t}/\bar{x}))$. So in these two cases, one can obtain descriptions which would at least imply the corresponding conditions.

However, although such descriptions might be a convenience in some cases, they appear to take us too far from the goal, i.e., the characterization of admissible theories; for our main example, the induction rule, does not have either of these latter two properties. In fact, this is as good reason as any why we should give up looking for a purely syntactical conditions which are necessary for admissibility. (The reader has probably noticed that all of Conditions 4, 5 and the uniformity condition are couched in terms of provability in T.) Surely, any purely syntactical property of a rule should be expressible in terms of a rule schema.

The second point is that, in general, the rules of a theory can take as arguments, or values, formulas outside the language of that theory. Why not, one might ask, just assume that all theories satisfy Condition 1? For the we would have, for all T, that T satisfies the theorem on constants, and that, if T satisfies the deduction theorem, then so does every extension T(C) of T. Thus to show that T is admissible, it would be sufficient to show that T satisfy the deduction theorem and the uniformity condition.

In reply we can say that this is a feasible approach for theories containing a constant. But it might happen that the strong semantics is adequate for some theory T not containing a constant, and that we are unable to verify this simply because the rules do not apply to formulas containing a constant, that is, because T might not satisfy the uniformity condition. Of course, one could compensate for this by building into the definition of "extension" of a theory, a provision for extending its rules. But then there is a question of how these rules are to be extended, so that one would eventually have to go back to the conditions we succeeded in eliminating, and replace them with some conditions governing extensions; and this would not be very different from having things as they now stand.

§ 3.3 Some Applications

We have already applied Theorem 3.2 to obtain Theorem 3.5; and we applied Theorem 3.5 to show that the strong semantics is adequate for the theories of arithmetic A and A^{-}. In this section we study some relationships between free-variable theories and first-order theories, we show that "extensions by primitive recursion" are "conservative", and we derive an interesting fact about provability in first-order Peano arithmetic P.

A first-order language and a free-variable language will be called correspondents (or corresponding) if they differ only in that the former contains quantifiers; and a first-order theory and a free-variable theory will be similarly called if their languages are correspondents and they have the same nonlogical axioms. A first-order theory and a free-variable theory will be associates if their languages are correspondents and the nonlogical axioms of the former are the theorems of the latter. A sequence of formulas is an open proof if it is a proof in a free-variable theory which, until further notice, is assumed to have no nonlogical rules. We shall consider the remark that appears with the statement of Theorem 3.1, where it was pointed out that that result would follow by the first-order completeness theorem if only we had the following.

Fact. For any free-variable theory T, if $T \nvdash P$ then $T^* \nvdash P$, where T* is the associate of T.

Now it is clear that this fact follows by Theorem 3.1. It happens that, recently, by following a renewed age old suggestion by his supervisor, this author has finally seen that the fact can be established through an application of the methods laid down in Problem 2, Chapter 4 of [39]. Instead of writing out this proof, let it only be said that the proof is aided by making the following observations: (i) In a free-variable theory, a formula is a theorem if and only if it is a tautological consequence of some substitution instances of the nonlogical axioms, (ii) in an extension T(c) of a first-order T, where c is a constant that is new to L(T), if a formula P of L(T) is not a tautological consequence of the substitution instances of the axioms of T, then the closed instance $P(c,\ldots,c/\bar{x})$ of P is not a tautological consequence of the substitution instances of the axioms of T(c), (iii) if E is a tautologically consistent set of formulas, and P is not in E, then $E \cup \{\sim P\}$ is tautologically consistent, and (iv) if E is a subset of a tautologically complete set E', then all the tautological consequences of formulas in E are in E'.

Once and for all, let us record this fact in the following way.

Theorem 3.7. In an open first-order theory, every open theorem has an open proof.

Let T be an open first-order theory; let T' be the corresponding free-variable theory; and let T" be the associate of T'. It is obvious the T and T" have the same theorems. Thus, given that $T \vdash P$, we have $T'' \vdash P$; and $T' \vdash P$, i.e. that P has a open proof, follows by the fact's contrapositive. ▯

Corollary. The open theorems of an open first-order theory are exactly the theorems of the corresponding free-variable theory.

We just saw that, if $T \vdash P$ then $T' \vdash P$. The converse statement holds because the substitution rule is valid in all first-order theories, so that proofs in T' are transformable into proofs in T. ▯

Note. The above corollary makes it obvious that, given the theorem, we can derive the fact.

We turn now to an application of Theorem 3.5. We consider formal systems F consisting of an open first-order theory, possibly with nonlogical rules, where by an n-ary rule for such a system is understood a class of (n+1)-tuples of formulas in which no two (n+1)-tuples have the same (n+1)-st member. An example of such a system is the system P' of Peano arithmetic, which is described in [39], p. 214. P' has first-order induction as a rule of proof.

It is clear that by reading "closed first-order formula" in place of "sentence", all of Conditions 1 through 8, and the definition of "admissible" make sense for such formal systems F. For the purposes of the following theorem, an "open proof" might be a proof in a free-variable theory which does have non-logical rules. The Q-instances of a first-order rules are those instances in which some member contains quantifiers.

<u>Theorem 3.8</u>. An open theorem of an admissible system F has an open proof if it has a proof without Q-instances of the nonlogical rules of F.

Let T_* be the free-variable theory with $L(T_*)$ the correspondent of L(F), with nonlogical axioms those of F, and with nonlogical rules those of F less the Q-instances. Then T_* is an admissible free-variable theory. It is sufficient to show that, if an open theorem of F has a proof that does not involve Q-instances, then it has a proof in T_*.

For each instance $(\bar{P},R(\bar{P}))$ of a nonlogical rule of F, let the <u>associated formula</u> be $P_1'\&\cdots\&P_n'\to R(\bar{P})'$ where the primes indicate the universal closure. Then let T* be the first-order theory with L(T*)=L(F), and with nonlogical axioms those of F, together with the formulas associated with the non-Q-instances of the nonlogical rules of F. It is clear that, if P is provable in F without Q-instances, then it is provable in T*. Thus it remains to show that an open theorem of T* is a theorem of T_*. Since every strong model of T_* is a model of T*, this follows by Theorem 3.5. ▯

Concluding Remarks

In conclusion here it is worth noting the following things.

(i) Even though we have found some fairly "nice" theorems about free-variable theories, it is clearly not worth our while to pursue the semantical analysis any further in this generality unless some more free-variable theories with "interesting" non-logical rules are first discovered.

(ii) However, over and above this, there is one question that deserves attention:

Can a free-variable theory for which the strong semantics is adequate have a model that is not strong?

For in application to the two theories of arithmetic, A and A^-, this is to ask if there is a structure for the language of A in which the theorems of either theory are valid, but the induction rule fails.

(iii) The answer to the analogous question about first-order systems F as described in §3.3 is "no". For, if the strong semantics is adequate for F, then F satisfies the deduction theorem, which, in thic case, implies that the formulas associated with the nonlogical rules of F are theorems of F, so that a model of F is a fortiori a strong model.

Bibliography

[1] Ackerman, W.: Zum Hilbertschen Aufbau der reelen Zahlen, Math. Annalen 99 (1928), 118-133.

[2] Birkoff, G.: On the structure of abstract algebra, Proc. Cambridge Phil. Soc. 31 (1935), 433-454.

[3] Carnap, R.: The Logical Syntax of Language, Routledge & Kegan Paul, 1937.

[4] Church, A.: An unsolvable problem of elementary number theory, Amer. J. Math. 58 (1936), 345-363.

[5] Church, A.: Review of "Berkeley 1954", J. Symb. Logic 20 (1955), 286-287.

[6] Church, A.: Binary recursive arithmetic, J. Math. Pures Appl. (9) 36 (1957), 39-55.

[7] Church, A.: Applications of recursive arithmetic to the problem of circuit synthesis, "Summaries of talks presented at the Summer Institute for Symbolic Logic, Cornell University 1957", 2 ed., Institute for Defense Analysis, Princeton, New Jersey, 1960, 3-50.

[8] Cleave, J. P.; Rose, H. E.: $\mathcal{E}^n$-arithmetics, Sets, Models and Recursive Theory, North-Holland, Amsterdam, 1967, 297-308.

[9] Curry, H. B.: A formalization of recursive arithmetic, Amer. J. Math. 63 (1941), 263-282.

[10] Dedekind, R.: Was sind und was sollen die Zahlen?, Brunswick, 1888. Reprinted in 8te unveränderte Aufl. Friedr. Vieweg & Sohn, Braunschweig, 1960.

[11] Fraenkel, A. A.; Bar-Hillel, Y.: Foundations of Set Theory, Studies in Logic and the Foundations of Mathematics, North-Holland, Amsterdam, 1958.

[12] Gödel, K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter System I, Monat. für Math. und Physik 38 (1931), 173-198. † and ††

[13] Gödel, K.: On undecidable propositions of formal mathematical systems, some lecture notes taken by S. C. Kleene and J. B. Rosser at the Institute for Advanced Study, Princeton, New Jersey, 1934. ††

[14] Gödel, K.: Über eine disher noch nicht benutze Erweiterung des finiten Standpunktes, Dialectica 12 (1958), 280-287.

[15] Goodstein, R. L.: Function theory in a axiom-free equation calculus, Proceedings of the London Math. Society (2) 48 (1945), 401-434.

[16] Goodstein, R. L.: Recursive Number Theory, A Developement of Recursive Arithmetic in a Logic-Free Equation Calculus, North-Holland, Amsterdam, 1957.

[17] Goodstein, R. L.: Models of propositional calculi in recursive arithmetic, Math. Scand. 6 (1958), 293-296.

[18] Goodstein, R. L.: A decidable fragment of recursive arithmetic, Z. Math. Logic Grundlagen Math. 9 (1963), 199-201.

[19] Goodstein, R. L.: Multiple successor arithmetics, Formal Systems and Recursive Functions, North-Holland, Amsterdam, 1965, 265-271.

[20] Goodstein, R. L.: A decidable class of equations in recursive arithmetic, Z. Math. Logic Grundlagen Math. 12 (1966), 235-239.

[21] Goodstein, R. L.: Developement of Mathematical Logic, Springer-Verlag, New York, 1971.

[22] Grätzer, G.: Universal Algebra, D. Van Nostrand, 1968.

[23] Heath, I. J.: Omitting the replacement schema in recursive arithmetic, Notre Dame J. Formal Logic 8 (1967), 234-238.

[24] Henkin, L.: The completeness of the first-order functional calculus, J. Symb. Logic 14 (1949), 159-166.

[25] Hermes, H.: Enumerability, Decidability, Computability, An Introduction to the Theory of Recursive Functions, 2nd rev. ed., Die Grundlehren der mathematischen Wissenschaften, Band 127, Springer-Verlag, New York, 1969.

[26] Hilbert, D.; Bernays, P.: Grundlagen der Mathematik, Vol. 1, Springer, Berlin, 1934. Reprinted by J. W. Edwards, Ann Arbor, Michigan, 1944.

[27] Kleene, S. C.: General recursive functions of natural numbers, Math. Annalen 112 (1936), 727-742. ††

[28] Kleene, S. C.: Introduction to Metamathematics, D. Van Nostrand, 1952.

[29] Kreisel, G.: Review of "Rose, H. E.: On the consistency and undecidability of recursive arithmetic", Math. Rev. 25 (1963), 746.

[30] Margaris, A.: First-Order Mathematical Logic, Blaisdell, New York, 1967, 63-71.

[31] Monk, J. D.: Introduction to Set Theory, McGraw-Hill, 1969.

[32] Peano, G.: Arithmeticos principia nova methodo exposita, Turin, 1889. Reprinted in Opere scelte, Vol. 2, Edixioni cremonese, Rome, 1958.

[33] Péter, R.: Recursive Functions, 3rd. ed., Academic Press, 1967.

[34] Pozsgay, L. J.: Gödel's second theorem for elementary arithmetic, Z. Math. Logic u. Grundlagen d. Math. 14 (1968), 67-80.

[35] Rasiowa, H.; Sikorski, R.: Mathematics of Metamathematics, Panstwowe Wydawnicten Nankowe, Warzawa, 1963.

[36] Rogers,H. R.: Theory of Recursive Functions and Effective Computability, McGraw-Hill, 1967.

[37] Rose, H. E.: Ternary recursive arithmetic, Math. Scand. 10 (1962), 201-216.

[38] Russell,B.;Whitehead, A. N.: Principia Mathematica, Cambridge Univ. Press, Vol. 1-3, 1910-1913 and 1925-1927.

[39] Shoenfield, J. R.: Mathematical Logic, Addison-Wesley, 1967.

[40] Skolem, T.: Begründung der elementaren Arithmetik durch die recurierende Denkweise ohne Anwendung schein baurer Veränderlichen mit unendlichen Ausdehnungsbereich, Vid. skrifter I. Math.-natur. Klasse, 6 (1923). †

[41] Skolem, T.: Über die Unmöglichkeit einer Charakterisierung der Zahlenreihe mittles eines endlichen Axiomsystems, Norsk matematisk forenings skrifter, series 2, 10 (1933), 73-82. †††

[42] Skolem, T.: The developement of recursive arithmetic,

C. R. Dixieme Congrès Math. Scandanaves, 1946, 1-16. †††

[43] Thomason, S. K.: Semantic analysis of tense logics, J. Symb. Logic 37 (1972), 150-158.

[44] Van Heijenoort, J., ed.: From Frege to Gödel, A Source Book in Mathematical Logic 1879-1931, Harvard Univ. Press, 1967.

[45] Vuckovič, V.: Partially ordered recursive arithmetics, Math. Scand. 7 (1959), 305-320.

† An English translation is reprinted in [44].

†† The original English or an English translation is in

Davis, M., ed.: The Undecidable, Raven Press, 1965.

††† Reprinted in

Fenstad, J. E., ed.: Selected Works in Logic by Thoralf Skolem, The Norwegian Research Council for Sciences and Humanities, 1970.