Introduction to Metamathematics

Julia B. Robinson

Lecture Notes from Mathematics 225

Stephen J. Garland
Department of Mathematics, University of California at Berkeley

1963-1964

These notes are from Julia Robinson's introductory graduate level course in mathematical logic. In the late 1960s, they were a widely used reference for students preparing for the PhD qualifying examination in logic. Topics include

- the completeness, Skolem-Löwenheim, and Craig interpolation theorems for first-order logic,
- the completeness of various first-order theories, including Presburger arithmetic (shown by elimination of quantifiers), real closed fields (shown by model completeness), and fields of characteristic p (shown by the Łoś-Vaught test),
- weak second order logic,
- hyperarithmetic sets, which are shown to be those that are Herbrand definable and which properly include the arithmetically definable sets (because the satisfaction function for arithmetic is Herbrand definable),
- equivalent definitions of recursive sets (by definability from a finite system of functional equations and by Turing computability),
- primitive recursive and diophantine sets,
- Gödel's incompleteness and second theorems,
- the undecidability of the theory of groups (via the interpretability of R. M. Robinson's essentially hereditarily undecidable theory Q), and
- the exponential diophantine definability of recursively enumerable sets (Davis, Putnam, and Robinson, Annals of Mathematics, 1961) and the existential definable of exponentiation in terms of addition, multiplication, and any infinite set of primes (steps towards the solution of Hilbert's tenth problem).

MATHEMATICS 225

Julia Robinson
1963-64

Notes by Stephen J. Garland

References

Beth, <u>The Foundations of Mathematics</u>
Church, <u>Introduction to Mathematical Logic</u>, I
Kleene, <u>Introduction to Metamathematics</u>
A. Robinson, <u>Introduction to Model Theory and to the Metamathematics of Algebra</u>
Tarski, <u>Logic, Semantics, Metamathematics</u>
Wang, <u>A Survey of Mathematical Logic</u>

Predicate Logic

Symbols: Logical Constants: $\neg$, $\rightarrow$, Λ ($=\forall$)
Individual Symbols
Variables (denumerably infinite set)
Constants
Relation Symbols (predicates)
With each relation symbol π is associated a natural number called the <u>rank</u> of π.

Formulas: defined as usual

Our aim will be to prove the completeness theorem for the basic language given above, and then to expand this language and derive a new completeness theorem as a corollary to the old.

Rules of Inference: For any formulas φ, ψ, and variable α

I. Detachment
From φ and $\varphi \rightarrow \psi$, infer ψ.

II. Generalization
From φ, infer $\Lambda\alpha\,\varphi$.

Axioms: (the first three schemata are due to Łukasiewicz)

A1. $(\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi))$

A2. $(\neg\varphi \rightarrow \varphi) \rightarrow \varphi$

A3. $\varphi \rightarrow (\neg\varphi \rightarrow \psi)$

A4. $\bigwedge\alpha(\phi \to \psi) \to (\phi \to \bigwedge\alpha\psi)$, where α is not a free variable in ϕ.

A5. $\bigwedge\alpha\phi \to \psi$, where ψ is obtained from ϕ by replacing each <u>free</u> occurrence of α by a <u>free</u> occurrence of a variable β or by an occurrence of a constant θ.

Remarks: Parentheses are not included as symbols of the language, but are merely employed to simplify notation. They may be eliminated entirely by writing formulas as $\to\phi\psi$, $\to\to\phi\neg\psi\chi$, etc. By induction one may show that there exists at most one formula beginning with any given symbol of such a string.

Similarly, commas between formulas in a proof are also superfluous.

Let Σ, θ be a set of formulas. A <u>proof</u> of θ from Σ is a finite sequence of formulas of which the last formula is θ and such that each formula is either an axiom, a formula of Σ, or is obtained from earlier formulas in the proof by detachment or generalization upon a variable which has no free occurrence in any formula of Σ_0.

θ is a <u>theorem</u> of Σ ($\Sigma \vdash \theta$) iff there is a proof of θ from some finite subset Σ_0 of Σ.

ERROR

See next page.

Note the necessity of Σ_0 in order for $\Sigma \vdash \alpha,\ \Sigma \subseteq \Gamma \Rightarrow \Gamma \vdash \alpha$ to hold. This detail was overlooked in Henkin's original formulation.

Our notion of proof still does not avoid all difficulties. For instance, if we are given two proofs of $\Sigma \vdash \phi$ and $\Sigma \vdash \phi \to \psi$, we would like to construct a proof for ψ from Σ by combining the given proofs and then using detachment. However this may not be done in general since different finite subsets Σ_0, Σ_1 may have been used in the proofs of ϕ, $\phi \to \psi$, and at some point in the proof of ϕ from Σ_0 we may have generalized upon a variable occurring in Σ_1.

To avoid this difficulty we must modify the notion of proof. One method would be to follow Kleene by adding a list of variables generalized upon to the sequence of formulas in the proof. However this is too cumbersome, and we choose the following definition:

ϕ is a <u>formal theorem</u> (<u>theorem of logic</u>) ($\vdash \phi$) iff there exists a finite sequences of formulas, the last of which is ϕ, such that each formula is either an axiom or derived from previous formulas by detachment or generalization.

ϕ is a <u>theorem</u> of Σ ($\Sigma \vdash \phi$) iff there is a finite sequence of formulas, the last of which is ϕ, such that each formula is either a formal theorem, in Σ, or obtained from earlier formulas by detachment.

From this definition we may derive our original rule of inference: (assuming the Deduction Theorem which follows)

IV. If α does not occur free in Γ and $\Gamma \vdash \phi$, then $\Gamma \vdash \Lambda\alpha\,\phi$.

<u>Proof</u>: It is sufficient to prove IV for finite Γ, and we do this by induction on the number of formulas in Γ. If Γ has no formulas, then $\vdash \phi$ and also $\vdash \Lambda\alpha\,\phi$. Suppose the theorem is true if Γ has n formulas.

$\{\phi_0, \ldots, \phi_n\} \vdash \phi$	hypothesis
$\{\phi_0, \ldots, \phi_{n-1}\} \vdash \phi_n \to \phi$	Deduction Theorem
$\{\phi_0, \ldots, \phi_{n-1}\} \vdash \Lambda\alpha\,(\phi_n \to \phi)$	inductive hypothesis
$\{\phi_0, \ldots, \phi_{n-1}\} \vdash \phi_n \to \Lambda\alpha\,\phi$	A4, I
$\{\phi_0, \ldots, \phi_n\} \vdash \Lambda\alpha\,\phi$	I

Derived Rule of Inference

III. From $\phi \to \psi$ and $\psi \to \chi$, infer $\phi \to \chi$.

<u>Deduction</u> <u>Theorem</u>. Let Σ be a set of formulas and let ϕ, ψ be formulas. If $\Sigma, \phi \vdash \psi$, then $\Sigma \vdash \phi \to \psi$.

<u>Proof</u>: Let $\sigma_0, \ldots, \sigma_n = \psi$ be a proof of ψ from Σ, ϕ, and let Σ_0 be the set of formulas of Σ which occur in this proof. We prove that $\Sigma \vdash \phi \to \psi$ by induction on the number of formulas in the proof of ψ from Σ_0, ϕ.

Case I. σ_n is ~~an axiom~~ a formal theorem or in Σ_0

$\Sigma_0 \vdash \psi$

$\vdash \psi \to (\phi \to \psi)$ (tautology)*

$\Sigma_0 \vdash \phi \to \psi$ I

Case II. $\sigma_n = \phi$

$\vdash \phi \to \phi$ (tautology)

$\Sigma_0 \vdash \phi \to \phi$

Case III. $\sigma_k = \sigma_j \to \sigma_n$, where $j, k < n$

$\Sigma_0 \vdash \phi \to \sigma_j$ } Inductive

$\Sigma_0 \vdash \phi \to \sigma_k$ } Hypothesis

$\vdash (\phi \to (\sigma_j \to \sigma_n)) \to ((\phi \to \sigma_j) \to (\phi \to \sigma_n))$ (tautology)

$\Sigma_0 \vdash \phi \to \sigma_n$ I, I

Unnecessary with revised notion of proof. {

Case IV. $\sigma_n = \Lambda\alpha\,\sigma_j$, where $j < n$ and α is not free in Σ_0 or in ϕ

$\Sigma_0 \vdash \phi \to \sigma_j$

$\Sigma_0 \vdash \Lambda\alpha(\phi \to \sigma_j)$ II

$\Sigma_0 \vdash \phi \to \Lambda\alpha\,\sigma_j$ A4, I

}

* For proofs of tautologies, see pp. 89-95.

<u>Generalization Theorem.</u> Suppose c is a constant which does not occur in any formula of Σ, ϕ, and let $\phi(c)$ be obtained from ϕ by replacing each free occurrence of α in ϕ by c. If $\Sigma \vdash \phi(c)$, then $\Sigma \vdash \Lambda\alpha\,\phi$.

<u>Proof:</u> Let $\sigma_0, \ldots, \sigma_n = \phi(c)$ be a proof of $\phi(c)$ from a finite subset Σ_0 of Σ, and let γ be a variable which does not occur in Σ_0 or in any formula of the proof. It may be shown by induction that $\sigma_0(\gamma), \ldots, \sigma_n(\gamma)$ is a proof from Σ_0, where $\sigma(\gamma)$ is the formula obtained by replacing all occurrences of c by γ. Hence

Σ_0	$\vdash \phi(\gamma)$	
Σ_0	$\vdash \Lambda\gamma\,\phi(\gamma)$	III
	$\vdash \Lambda\gamma\,\phi(\gamma) \to \phi$	A5
	$\vdash \Lambda\alpha\,(\Lambda\gamma\,\phi(\gamma) \to \phi)$	IV
	$\vdash \Lambda\gamma\,\phi(\gamma) \to \Lambda\alpha\,\phi$	A4, I
Σ_0	$\vdash \Lambda\alpha\,\phi$	I

Σ is called <u>consistent</u> iff there exists no formula θ such that both $\Sigma \vdash \theta$ and $\Sigma \vdash \neg\theta$.

<u>Lemma.</u> (a) If Σ is not consistent, the $\Sigma \vdash \phi$ for any ϕ.
(b) If Σ is consistent, then so is either Σ, ϕ or $\Sigma, \neg\phi$.
(c) If Σ, ϕ is not consistent, then $\Sigma \vdash \neg\phi$.

<u>Proof:</u> (a) By hypothesis, there is a θ such that
$\Sigma \vdash \theta$ and $\Sigma \vdash \neg\theta$.
$\vdash \neg\theta \to (\theta \to \phi)$ (tautology)
Applying detachment, we obtain $\Sigma \vdash \phi$.

(b) Suppose Σ, ϕ and $\Sigma, \neg\phi$ are both inconsistent. Then by (a), $\Sigma, \phi \vdash \neg\phi$ and $\Sigma, \neg\phi \vdash \phi$. By the Deduction Theorem,

$$\Sigma \vdash \phi \to \neg\phi$$
$$\Sigma \vdash \neg\phi \to \phi.$$
$$\vdash (\phi \to \neg\phi) \to \neg\phi \qquad \text{tautology}$$
$$\Sigma \vdash \neg\phi \qquad \text{I}$$
$$\Sigma \vdash \phi \qquad \text{I.}$$

But this contradicts the consistency of Σ.

(c)
$$\Sigma, \phi \vdash \neg\phi \qquad \text{since } \Sigma, \phi \text{ is inconsistent}$$
$$\Sigma \vdash \phi \to \neg\phi \qquad \text{Deduction Theorem}$$
$$\vdash (\phi \to \neg\phi) \to \neg\phi \qquad \text{tautology}$$
$$\Sigma \vdash \neg\phi \qquad \text{I}$$

<u>Completeness</u> <u>Theorem</u>. Let S be a predicate logic, and suppose T is a consistent set of sentences. Then T can be simultaneously satisfied in a domain of individuals of the same cardinality as the set of symbols of S.

<u>Proof</u>: Let S' be the predicate logic obtained from S by adjoining a set $\mathcal{C}$ of additional constants, $\mathcal{C}$ having the same cardinality as the set of symbols of S. We shall show that there is a set T' of sentences of S' such that

(a) $T \subseteq T'$
(b) T' is consistent
(c) For every sentence θ in S', either θ or $\neg\theta$ is in T'.
(d) If $\forall\alpha\,\phi \in T'$, then for some $c \in \mathcal{C}$, $\phi(c) \in T'$.

We demonstrate the existence of such a T' in the case S has denumerably many symbols. The general case is proved in an analogous fashion.

Let $\{\phi_1, \phi_2, \dots\}$ be an enumeration of the sentences of S' and let $C = \{c_0, c_1, \dots\}$. Let $T' = \bigcup_{r<\omega} T_r$, where

$T_0 = T$

I. If T_n, ϕ_n is inconsistent, then $T_{n+1} = T_n$.

II. If T_n, ϕ_n is consistent and ϕ_n is not of the form $\bigvee\alpha\phi$, then $T_{n+1} = T_n \cup \{\phi_n\}$.

III. If T_n, ϕ_n is consistent and $\phi_n = \bigvee\alpha\phi$, then let r be the least natural number such that c_r does not occur in T_n, ϕ_n. Let $T_{n+1} = T_n \cup \{\phi_n, \phi(c_r)\}$.

We show that T' satisfies properties (a)-(d).

(a) $T = T_0 \subset \bigcup_{n<\omega} T_n = T'$

(b) It is sufficient to show that T_{n+1} is consistent if T_n is consistent. Cases I and II are obvious.

<u>Lemma</u>. If $\Sigma, \bigvee\alpha\phi$ is consistent and c does not occur in any formula of Σ, ϕ, then $\Sigma, \bigvee\alpha\phi, \phi(c)$ is consistent.

<u>Proof</u>: If $\Sigma, \bigvee\alpha\phi, \phi(c)$ is inconsistent, then

$\Sigma, \bigvee\alpha\phi \vdash \neg\phi(c)$ — preceeding lemma

$\Sigma, \bigvee\alpha\phi \vdash \bigwedge\alpha\neg\phi$ — Generalization Thm

$\Sigma, \bigvee\alpha\phi \vdash \neg\neg\bigwedge\alpha\neg\phi$ — tautology, I

$\Sigma, \bigvee\alpha\phi \vdash \neg\bigvee\alpha\phi$ — definition of $\bigvee$,

which is a contradiction.

The lemma establishes Case III.

(c) Since T' is consistent so is either T', θ or $T', \neg\theta$. Let ϕ_n be the formula which is consistent with T. Then $\phi_n \in T_{n+1} \subseteq T'$.

(d) Clear by construction.

Hence T' has the required properties in the denumerable case.

In general let $\varkappa$ be the cardinality of the set of symbols of S and set $C = \{c_\mu\}_{\mu<\varkappa}$. Then the set of sentences of S' has cardinality $\varkappa$ and may be indexed $\{\varphi_\mu\}_{\mu<\varkappa}$. Define $\Gamma' = \bigcup_{\mu<\varkappa} T_\mu$, where the T_μ are defined as before with the added condition that if μ is a limit ordinal then $T_\mu = \bigcup_{\lambda<\mu} T_\lambda$. The proof that (a)-(d) hold is obviously still valid.

We assumed in the construction of Γ' that Γ being consistent in S implied Γ was consistent in S'. For suppose Γ is inconsistent in S'. Then $\Gamma \vdash \theta$ and $\Gamma \vdash \neg\theta$, where we can take θ in S. If we write down proofs of θ and $\neg\theta$ and then replace all constants in C by variables, the result will be proofs of θ and $\neg\theta$ from Γ in S. Hence Γ would be inconsistent in S, contradicting our hypothesis.

We now construct a model for S', taking as the domain of individuals the constants of S' and defining a valuation V as follows: for all sentences φ, ψ,

(i) If φ is an atomic sentence, $V(\varphi) = T$ iff $\Gamma \vdash \varphi$.

(ii) $V(\neg\varphi) = T$ iff $V(\varphi) = F$.

(iii) $V(\varphi \to \psi) = F$ iff $V(\varphi) = T$ and $V(\psi) = F$.

(iv) ~~If φ~~ $= \forall\alpha\, \chi$, $V(\varphi) = T$ iff for every element in the domain of individuals $V(\chi(c)) = T$, where $\chi(c)$ is obtained from χ by substituting c for all free occurrences of α.

It may be demonstrated by induction that there is exactly one such valuation V.

<u>Lemma</u>. For every sentence ϕ of S', $T' \vdash \phi$ iff $V(\phi) = T$.

<u>Proof</u>: We prove the lemma by induction on the length of ϕ. If ϕ is an atomic sentence, $T' \vdash \phi$ iff $V(\phi) = T$, by definition.

<u>Case I</u>. a) $\phi = \neg\psi$ and $V(\psi) = T$

$T' \vdash \psi$	inductive hypothesis
not $T' \vdash \neg\psi$	since T' is consistent

b) $\phi = \neg\psi$ and $V(\psi) = F$

not $T' \vdash \psi$	inductive hypothesis
$T' \vdash \neg\psi$	since T' is complete

<u>Case II</u>: $\phi = \psi \to \chi$

a) $V(\psi) = F$

$T' \vdash \neg\psi$	inductive hypothesis
$\vdash \neg\psi \to (\psi \to \chi)$	tautology
$T' \vdash \phi$	I
$V(\phi) = T$	definition of V

b) $V(\chi) = T$

$T' \vdash \chi$	inductive hypothesis
$\vdash \chi \to (\psi \to \chi)$	tautology
$T' \vdash \phi$	I
$V(\phi) = T$	definition of V

c) $V(\psi) = T$ and $V(\chi) = F$

$T' \vdash \psi$	} inductive hypothesis
$T' \vdash \neg\chi$	}
$\vdash \psi \to (\neg\chi \to \neg(\psi \to \chi))$	tautology
$T' \vdash \neg\phi$	I, I
not $T' \vdash \phi$	T consistent
$V(\phi) = F$	def. of V.

Case III. $\phi = \bigwedge \alpha\, \psi$

a) Suppose $\Gamma' \vdash \bigwedge\alpha\,\psi$.

$\Gamma' \vdash \psi(c)$, for every c	AS, I
$V(\psi(c)) = T$, for every c	inductive hypothesis
$V(\bigwedge\alpha\,\psi) = T$	def. of V

b) Suppose not $\Gamma' \vdash \bigwedge\alpha\,\psi$.

$\Gamma' \vdash \neg \bigwedge\alpha\,\psi$	since Γ' is complete
$\vdash \neg\bigwedge\alpha\,\psi \rightarrow \bigvee\alpha \neg\psi$	tautology
$\Gamma' \vdash \bigvee\alpha\neg\psi$	I
$\Gamma' \vdash \neg\psi(c)$	for some $c \in \mathcal{C}$ by construction
$V(\psi(c)) = F$	inductive hypothesis
$V(\bigwedge\alpha\,\psi) = F$	def. of V

The lemma concludes the proof of the completeness theorem since it shows that the set Γ' is simultaneously satisfiable by V in the model constructed.

Problems on the size of models

Let Γ be a set of sentences of a predicate logic S.

1. If Γ has a model then it has a model of the same cardinality as its set of symbols.
2. If Γ has a model of cardinality μ, then for every $\nu > \mu$, Γ has a model of cardinality ν.
3. For every infinite cardinal ν there exists a predicate logic of ν symbols such that for some Γ no model with fewer than ν elements exists.
   a) Demonstrate such a predicate logic with no constants.
   b) Demonstrate such a predicate logic with a finite number of relation symbols.
4. How large can a set Γ of ν sentences force a model to be?

Sketches of solutions:

1. Γ has a model $\Rightarrow$ Γ consistent; use completeness theorem

2. Duplicate one individual ν times.

3. a) Take ν relations $\{F_\mu\}_{\mu<\nu}$ and let Γ contain all instances of $\bigvee x F_\mu x$, $\bigwedge x (F_\mu x \to \neg F_\nu x)$, where $\mu \neq \nu$.

   b) Take ν constants $\{c_\mu\}_{\mu<\nu}$ and one relation F. Let Γ contain all instances of $F c_\mu c_\mu$, $\neg F c_\mu c_\nu$, where $\mu \neq \nu$.

4. If ν is infinite, there exists a model of cardinality ν - form a sub-predicate logic containing only the constants and predicates of Γ.

   If ν is finite, the model may still have to be infinite. E.g., take

$$\Gamma = \begin{cases} \bigwedge x \neg Fxx \\ \bigwedge x \bigvee y\, Fxy \\ \bigwedge xyz\, (Fxy \to (Fyz \to Fxz)). \end{cases}$$

Predicate Logic with Identity

To our original system of predicate logic we add a relational constant '=' and the following axioms:

A6. $\alpha = \alpha$

A7. $\alpha = \beta \to (\phi \to \psi)$, where ψ is obtained from ϕ by replacing one free occurrence of α by a free occurrence of β

For the proof of the following theorem, the subscript = will indicate a notion of the predicate logic with identity; non-subscripted notions refer to the former predicate logic.

Completeness Theorem for Predicate Logic with Identity

Let Γ be a $\text{consistent}_=$ set of sentences of a predicate logic S with equality. Then Γ has a $\text{model}_=$ with cardinality at most that of the set of symbols of S.

Proof: Let S_0 be the predicate logic without identity, but with a binary relation =. Let Δ be the set of sentences obtained by generalization of A6, A7. Then $\Delta \vdash \phi$ for every instance ϕ of A6, A7 by A5. Also, if $\theta \in \Delta$, $\vdash_= \theta$. Hence if Γ is $\text{consistent}_=$, then $\Gamma \cup \Delta$ is consistent.

Let S have ν symbols and let M be a model of cardinality ν of $\Gamma \cup \Delta$. The relation = will go into some binary relation E in the model M. E is an equivalence relation since

$\vdash_= \alpha = \alpha$	A6
$\vdash_= \alpha = \beta \to \beta = \alpha$	use A7 twice
$\vdash_= \alpha = \beta \to (\beta = \gamma \to \alpha = \gamma)$	use A7

Now let M' be a model whose domain consists of the equivalence classes of M determined by E. It is a matter of routine to check that M' is a model= for Γ and that M' has no more than ν elements.

<u>Skolem-Lowenheim Theorem</u>

If S is a denumerable logic and Γ is a set of sentences of S, then if Γ has an infinite model, Γ has a denumerable model (and in fact a model of any cardinality).

<u>Proof</u>: Adjoin to S a set $\mathcal{C} = \{c_\mu\}_{\mu<\nu}$ of new constants, and let $\Delta = \{c_\lambda \neq c_\mu : \mu \neq \lambda\}$. Then $\Gamma \cup \Delta$ is consistent since Γ has an infinite model and the constants occuring in any finite subset of Δ may be mapped 1-1 into that model.

Hence $\Gamma \cup \Delta$ has a model of cardinality at most ν, and Δ guarantees that this cardinality is at least ν.

Lowenheim proved the theorem in 1915 in the case that Γ was finite. Skolem generalized the result in 1920. Note that the proof applies equally to the following theorem:

If Γ has arbitrarily large finite models, then Γ has an infinite model.

Tarski's Predicate Logic with Identity

Archiv Math. Logik **7** 1965, p. 61, 81

Symbols: Logical constants: $\wedge, \neg, \rightarrow, =$
Variables: $v_0, v_1, \ldots$
Relation symbols

Definitions: The Quine closure of a formula ϕ with exactly the free variables $v_{i_0}, \ldots, v_{i_{n-1}}$, where $i_0 < \ldots < i_{n-1}$, is the sentence $\wedge v_{i_0} \cdots \wedge v_{i_{n-1}} \phi$ and is denoted by $[\phi]$.

$R(\phi, \psi, \alpha, \beta)$ iff ψ is obtained from ϕ by replacing one free occurrence of α in ϕ by a free occurrence of β.

$S(\phi, \psi, \alpha, \beta)$ iff ψ is obtained from ϕ by replacing all free occurrences of a in ϕ by free occurences of β.

All universally valid sentences of this logic can be derived from the following axioms by detachment. Furthermore, the axioms are independent. (α, β variables; ϕ, ψ, χ formulas)

Axioms:
- B1. $[(\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\phi \rightarrow \chi))]$
- B2. $[(\neg \phi \rightarrow \phi) \rightarrow \phi]$
- B3. $[\phi \rightarrow (\neg \phi \rightarrow \psi)]$
- B4. $[\wedge\alpha \wedge\beta\, \phi \rightarrow \wedge\beta \wedge\alpha\, \phi]$
- B5. $[\wedge\alpha (\phi \rightarrow \psi) \rightarrow (\wedge\alpha\, \phi \rightarrow \wedge\alpha\, \psi)]$
- B6. $[\wedge\alpha\, \phi \rightarrow \phi]$
- B7. $[\phi \rightarrow \wedge\alpha\, \phi]$, where α is not free in ϕ
- B8. $[\neg \wedge\alpha \neg\, \alpha = \beta]$, where α and β are not the same variable
- B9. $[\alpha = \beta \rightarrow (\phi \rightarrow \psi)]$, where ψ is atomic and $R(\phi, \psi, \alpha, \beta)$

The advantages of Tarski's system is that it avoids substitution, and thereby leads to an easier arithmetization. A law of substitution may be derived, however, to aid in proving theorems, for if $S(\phi, \psi, \alpha, \beta)$, then $\vdash \psi \leftrightarrow \wedge\alpha (\alpha = \beta \rightarrow \phi)$. ($\vdash$ in old system)

Proof:
$\vdash \beta = \alpha \to (\psi \to \phi)$ — by repeated use of A7
$\vdash \alpha = \beta \to (\psi \to \phi)$ — A7
$\vdash \psi \to (\alpha = \beta \to \phi)$ — tautology
$\vdash \Lambda\alpha\,(\psi \to (\alpha = \beta \to \phi))$ — II
$\vdash \psi \to \Lambda\alpha\,(\alpha = \beta \to \phi)$ — A4
$\vdash \Lambda\alpha\,(\alpha = \beta \to \phi) \to (\beta = \beta \to \psi)$ — A5
$\vdash \beta = \beta \to (\Lambda\alpha\,(\alpha = \beta \to \phi) \to \psi)$ — tautology
$\vdash \Lambda\alpha\,(\alpha = \beta \to \phi) \to \psi$ — A6, I

Lemmas:
1. $\vdash [\phi \to \psi]$, $\vdash [\phi] \Rightarrow \vdash [\psi]$ ($\vdash$ in new sense)
2. $\vdash [\phi] \Rightarrow \vdash [\Lambda\alpha\,\phi]$
3. $\vdash [\phi \to \psi]$, $\vdash [\psi \to \chi] \Rightarrow \vdash [\phi \to \chi]$
4. If ϕ is tautological, then $\vdash [\phi]$.
5. $\vdash [\Lambda\alpha\,(\phi \to \psi) \to (\phi \to \Lambda\alpha\,\psi)]$ if α is not free in ϕ
6. $\vdash [\alpha = \alpha]$
7. $\vdash [\alpha = \beta \to \beta = \alpha]$
8. $\vdash [\beta = \alpha \to (\phi \to \psi)] \Rightarrow \vdash [\alpha = \beta \to (\neg\psi \to \neg\phi)]$
9. $\vdash [\beta = \alpha \to (\phi \to \psi)] \Rightarrow \vdash [\alpha = \beta \to ((\psi \to \chi) \to (\phi \to \chi))]$
10. $\vdash [\alpha = \beta \to (\phi \to \psi)] \Rightarrow \vdash [\alpha = \beta \to ((\chi \to \phi) \to (\chi \to \psi))]$
11. $\vdash [\alpha = \beta \to (\phi \to \psi)]$, $\alpha, \beta \neq \gamma \Rightarrow \vdash [\alpha = \beta \to (\Lambda\gamma\,\phi \to \Lambda\gamma\,\psi)]$
12. $R(\phi, \psi, \alpha, \beta) \Rightarrow \vdash [\alpha = \beta \to (\phi \to \psi)]$
13. $S(\phi, \psi, \alpha, \beta) \Rightarrow \vdash [\alpha = \beta \to (\phi \to \psi)]$
14. $S(\phi, \psi, \alpha, \beta)$ & $\alpha \neq \beta \Rightarrow \vdash [\Lambda\alpha\,\phi \to \psi]$

Tarski's system is complete, for any proof of ϕ in the old system can be transformed into a proof of $[\phi]$ in the new one. Axioms A1-A7 are axioms B1-B3 and lemmas 5, 15, 6, 12 respectively.

Lemmas 1 and 2 are proved by induction: 1 by induction on the number of free variables in $\phi \to \psi$. The remainder of the proofs are routine.

Number Theory

Let N be the predicate logic with identity and
Constants: 0, 1
Relations (or operations): +, ·.
Let Γ be the set of all sentences which hold in the arithmetic of natural numbers.

Now let N' be formed from N by adding a new constant c, and let $\Gamma' = \Gamma \cup \{c \neq 0, c \neq 1, c \neq 1+1, \ldots\}$. Γ' is consistent since any finite subset of $\{c \neq 0, c \neq 1, \ldots\}$ is consistent with Γ. Hence Γ' has a denumerable model.

Thus no set of sentences characterizes the natural numbers, since a model for Γ' is not isomorphic to a model for Γ. This result on <u>non-standard models</u> was shown by Skolem in 1934.

A <u>mathematical structure</u> or <u>relational structure</u> consists of a domain A and certain relations (operations, constants). For example, the arithmetic of natural numbers is $\langle \omega, +, \cdot, 0, 1 \rangle$.

A set $S \subseteq A$ is <u>definable</u> iff there is a formula φ with one free variable such that $Sx \leftrightarrow \phi(x)$. Similarly, a relation $R \subseteq A \times A$ is definable iff there is a formula φ of two free variables such that $R(x,y) \leftrightarrow \phi(x,y)$.

Examples:

x is a square	$\leftrightarrow$	$\bigvee y\,(y \cdot y = x)$
$x \leq y$	$\leftrightarrow$	$\bigvee z\,(x + z = y)$
$x \dot{-} y = z$	$\leftrightarrow$	$y + z = x \lor (z = 0 \land \bigvee_w (x + w = y))$
$x \mid y$	$\leftrightarrow$	$\bigvee z\,(x \cdot z = y)$
x Pow 2	$\leftrightarrow$	$\neg \bigvee z[(z + z + 3) \mid x]$
x is a prime	$\leftrightarrow$	$x \neq 0 \land x \neq 1 \land \neg \bigvee y, z\,[x = (y+2) \cdot (z+2)]$

Nonstandard models for number theory: Denumerable Case

The natural numbers 0, 1, 1+1, 1+1+1, ... will be abbreviated by $\Delta_0, \Delta_1, \Delta_2, \ldots$

What can be said about the "unnatural" numbers with respect to the ordering '<'? Their position may be determined by noting that any statement which holds in the standard model must hold in every non-standard model. E.g.,

$$\neg \bigvee x \, (x < 0)$$

$$\bigwedge x \, (x \leq \Delta_n \leftrightarrow x = \Delta_0 \vee x = \Delta_1 \vee \cdots \vee x = \Delta_n)$$

Thus any unnatural number must come 'after' all natural numbers.

Let α be any unnatural number. We know that

$$x \neq 0 \rightarrow \bigvee y \, (x = y+1) \wedge \bigvee z \, (z = x+1).$$

Hence α belongs to a "row" $\ldots \alpha \dot{-} \Delta_2, \alpha \dot{-} \Delta_1, \alpha, \alpha + 1, \alpha + \Delta_2, \ldots$ which extends infinitely in both directions. Rows are not interleaved under < since

$$\bigwedge x \neg \bigvee y \, (x < y < x+1).$$

There are denumerably many rows since $[\frac{\alpha}{2}] < \alpha < \alpha + \alpha$, where $$y = [\tfrac{x}{2}] \leftrightarrow x = y+y \vee x = y+y+1.$$
These rows are distinct by virtue of the definition of [ ], for otherwise we could show that a natural number belonged to one of these rows. Likewise between any two rows is another row: $\alpha < [\frac{\alpha+\beta}{2}] < \beta$.

The above arguments show that the order type of any denumerable nonstandard model is $\omega + (\omega^* + \omega)\eta$.

<u>Theorem</u>. There are exactly $2^{\aleph_0}$ denumerable, non-isomorphic nonstandard models for arithmetic.

<u>Proof</u>: There are no more than $2^{\aleph_0}$ models for arithmetic since there are only $2^{\aleph_0}$ ways in which the relations + and · may be assigned in a denumerable domain.

On the other hand there are at least $2^{\aleph_0}$ models. For let S be any subset of the natural numbers. Define a constant c_S and a set Δ_S of formulas

$$\Delta_S = \begin{cases} p_n \mid c_S & \text{whenever } n \in S \\ p_n \nmid c_S & \text{whenever } n \notin S, \end{cases}$$

where p_n is the n^{th} prime. Any finite subset of Δ_S is consistent with the set Γ of true sentences of arithmetic, and thus $\Gamma \cup \Delta_S$ is consistent. By the completeness theorem, there is a denumerable model $\mathfrak{M}_S$ for $\Gamma \cup \Delta_S$.

Now a given model $\mathfrak{M}_S$ can satisfy only a denumerable number of sets Δ_T. For if $S \neq T$, $c_S \neq c_T$ in the model, and $\mathfrak{M}_S$ has only denumerably many elements. Since there are $2^{\aleph_0}$ subsets of the natural numbers, there must be $2^{\aleph_0}$ models to satisfy all the Δ_S.

As a corollary to the proof of the preceeding theorem, we see that we can construct a non-standard model with cardinality $2^{\aleph_0}$; i.e., take a model for $\Gamma \cup \bigcup_S \Delta_S$.

Problems

1. Is there a number other than 0 which is divisible by all natural numbers in any non-standard model of arithmetic?

2. Is there an unnatural prime π such that $\pi+2$ is also prime?

3. Is there a row each number of which is composite? Is there a row each number of which is divisible by a natural number greater than 1?

4. Does every unnatural number have an unnatural prime divisor?

5. Show that every definable set of natural numbers can be defined by a formula of the form

$$Sx \leftrightarrow Q\alpha_0 Q\alpha_1 \dots Q\alpha_n \; P = 0,$$

where P is a polynomial with integer coefficients.

Size of Models

Let S be a predicate logic with ν symbols and T be a set of sentences with an infinite or arbitrarily large finite models. Then we know T has models of every cardinality $\geq \nu$. We cannot do much better than this, for there is a predicate logic of $2^{\aleph_0}$ symbols which has arbitrarily large finite models but no infinite models of cardinality $< 2^{\aleph_0}$. I.e., choose constants $\{c_\lambda\}_{\lambda \leq \omega}$ and let $N_k = \bigvee_{x_1,\dots,x_k} (x_1 \neq x_2 \wedge \dots \wedge x_{k-1} \neq x_k)$. Now let T be the set of all sentences of the form

$$N_{2^k} \rightarrow c_\alpha \neq c_\beta \quad , \quad \text{where} \quad \alpha \cap \{1,\dots k\} \neq \beta \cap \{1,\dots,k\}.$$

For every integer k_0 there is a model for T with 2^{k_0} elements since there are only 2^{k_0} subsets of $\{1,\dots,k\}$. But any infinite model satisfies all the N_k, and hence the number of constants must be $2^{\aleph_0}$.

We have seen that there are $2^{\aleph_0}$ non-isomorphic denumerable models of arithmetic. Some of this complexity may be eliminated by strengthening the requirements on the model. I.e., let $\{S_\nu\}_{\nu < 2^{\aleph_0}}$ be all unary relations on ω and let T be the set of true sentences of the structure $\mathfrak{a} = \langle \omega, <, S_0, S_1, \dots, S_\nu, \dots \rangle$. Then all denumerable models for T are isomorphic. We first establish the following lemma:

<u>Lemma</u>. There is a class $\mathcal{C}$ of subsets of ω with cardinality $2^{\aleph_0}$ such that $S, T \in \mathcal{C} \Rightarrow S \cap T$ is finite.

<u>Proof</u>: For each real number α such that $1 \leq \alpha < 10$ let $F_\alpha(n) = [\alpha \cdot 10^n]$ and set S_α equal to the range of F_α. Any two S_α have a finite intersection since their decimal expansions of α and β for $\alpha \neq \beta$ agree for only a finite initial segment.

<u>Theorem</u>. Let S be a predicate logic with $2^{\aleph_0}$ unary relations $\{S_\nu\}_{\nu<2^{\aleph_0}}$ and a binary relation $<$. Suppose $\mathfrak{A} = \langle \omega, <, S_0, \ldots \rangle$, where the S_ν exhaust all unary relations on ω, and let Σ be the set of true sentences of $\mathfrak{A}$. Then all denumerable models of Σ are isomorphic.

<u>Proof</u>: The standard model for $\mathfrak{A}$ is precisely the standard model of arithmetic since we can define the natural numbers by

$$x = \Delta_0 \leftrightarrow \bigwedge_y (x \le y)$$

$$x = \Delta_1 \leftrightarrow \bigwedge_y (y \ne \Delta_0 \rightarrow x \le y) \wedge x \ne \Delta_0, \text{ etc.}$$

Now suppose that Σ has an unnatural model. For every infinite set S_ν the sentence

$$\bigwedge_x \bigvee_y (y \ge x \wedge S_\nu y)$$

is true. Hence every infinite set S_ν contains an unnatural number. But the sentence

$$\bigwedge_x (S_\alpha x \wedge S_\beta x \rightarrow x < \Delta_n)$$

is in Σ whenever S_α and S_β are in the class $\mathcal{C}$ of the lemma since $S_\alpha \cap S_\beta$ is finite in that case. Hence no two sets in $\mathcal{C}$ have an unnatural number in common, so that there must be at least $2^{\aleph_0}$ elements in any nonstandard model.

<u>Problem</u>: Given a set Γ of sentences in an arbitrary predicate logic, show that if Γ has arbitrarily large finite models, then Γ has an infinite model of $2^{\aleph_0}$ elements.

Well-Ordered Predicate Logics

Let $\mathcal{L}$ be a (well-ordered) predicate logic with a well-ordered set of relation symbols. A structure $\mathcal{R} = \langle A, R, S, \ldots \rangle$ is called a <u>structure</u> <u>of</u> $\mathcal{L}$ iff the relations of $\mathcal{R}$ are well-ordered of the same type as the relation symbols of $\mathcal{L}$ and such that corresponding relations of $\mathcal{L}$ and $\mathcal{R}$ are of the same rank.

If $\mathcal{R} = \langle A, R, \ldots \rangle$ and $\mathcal{S} = \langle B, S, \ldots \rangle$ are structures of $\mathcal{L}$, $\mathcal{R}$ is a <u>substructure</u> of $\mathcal{S}$ iff $A \subseteq B$ and if R, S are corresponding relations, $R = S \upharpoonright A$, the restriction of S to A. We also say that $\mathcal{S}$ is an <u>extension</u> of $\mathcal{R}$ and write $\mathcal{R} \leq \mathcal{S}$ or $\mathcal{S} \geq \mathcal{R}$.

A sentence ϕ of $\mathcal{L}$ is <u>true</u> in a structure $\mathcal{R}$ of $\mathcal{L}$ iff ϕ is true in the domain of $\mathcal{R}$ under the interpretation that each relational symbol of $\mathcal{L}$ denotes the corresponding relation of $\mathcal{R}$.

A structure $\mathcal{R}$ of $\mathcal{L}$ is a <u>model</u> of a set Γ of sentences of $\mathcal{L}$ iff every sentence of Γ is true in $\mathcal{R}$.

Two structures $\mathcal{R}$ and $\mathcal{S}$ of $\mathcal{L}$ are

(i) <u>arithmetically</u> <u>equivalent</u> ($\mathcal{R} \equiv \mathcal{S}$) iff every sentence of $\mathcal{L}$ which is true in $\mathcal{R}$ is true in $\mathcal{S}$*

(ii) <u>isomorphic</u> ($\mathcal{R} \cong \mathcal{S}$) iff there is a 1-1 mapping of the domain of $\mathcal{R}$ onto the domain of $\mathcal{S}$ which preserves all relations.

$\mathcal{R}$ is an <u>elementary</u> <u>substructure</u> (<u>subsytem</u>) of $\mathcal{S}$ ($\mathcal{R} \prec \mathcal{S}$) iff $\mathcal{R}$ is a substructure of $\mathcal{S}$ such that whenever elements $a_0, \ldots, a_{n-1}$ in the domain of $\mathcal{R}$ satisfy a formula ϕ of $\mathcal{L}$ with n free variables, then $a_0, \ldots, a_{n-1}$ satisfy ϕ in $\mathcal{S}$. We also say that $\mathcal{S}$ is an <u>elementary</u> <u>extension</u> of $\mathcal{R}$.

* Note that "and conversely" is superfluous, since for every sentence θ, either θ or $\neg\theta$ is true in $\mathcal{R}$.

Examples.

1. Let NT = natural numbers, IN = integers, and EV = even integers. Then if $\mathfrak{N} = \langle NT, +, \cdot, 0, 1 \rangle$ and if $\mathfrak{A}$ is any non-standard arithmetic,

$$\mathfrak{N} \propto \mathfrak{A} \text{ but not } \mathfrak{N} \cong \mathfrak{A}.$$

$$\mathfrak{N} \leq \mathfrak{A} \wedge \mathfrak{N} \equiv \mathfrak{A} \Rightarrow \mathfrak{N} \propto \mathfrak{A}$$

2. Let $\mathcal{E} = \langle EN, < \rangle$ and $\mathcal{I} = \langle IN, < \rangle$. Then $\mathcal{E} \cong \mathcal{I}$ and $\mathcal{E} \leq \mathcal{I}$, but not $\mathcal{E} \propto \mathcal{I}$ since 0, 2 satisfy $\neg \bigvee_z (x < z < y)$ in $\mathcal{E}$ but not in $\mathcal{I}$.

Theory of Fields

Let $\mathcal{L}$ be the predicate logic with 0, 1, +, ·. A structure $\mathfrak{F} = \langle F, 0, 1, +, \cdot \rangle$ is a field iff the following sentences are true in $\mathfrak{F}$

$[(x+y)+z = x+(y+z)]$

$[x+y = y+x]$

$[(x \cdot y) \cdot z = x \cdot (y \cdot z)]$

$[x \cdot y = y \cdot x]$

$[x \cdot (y+z) = x \cdot y + x \cdot z]$

$[0 \neq 1]$

$[x+0 = x]$

$[x \cdot 1 = x]$

$\bigwedge_x \bigvee_y (x+y=0)$

$\bigwedge_x (x \neq 0 \rightarrow \bigvee_y (x \cdot y = 1))$

NB: The definition of a structure may be modified in the obvious manner to include constants and operations. For simplicity's sake, however, we shall omit them from proofs, as the additional details are routine. Alternatively, we could omit them altogether and include additional axioms to treat 0, 1, +, · as relations.

Let RT = rational numbers. Then a structure $Q = \langle RT, 0, 1, +, \cdot \rangle$ is a rational field, and if $Q' = \langle Q', 0, 1, +, \cdot \rangle$ is such that $Q \leq Q'$ and $Q \equiv Q'$, but not $Q \cong Q'$, we could call Q' a non-standard rational field. There exist denumerable non-standard rational fields, for let $\mathcal{L}'$ be a predicate logic obtained from $\mathcal{L}$ by adjoining a constant ε and let Δ be the set of sentences

$$\Delta_p \cdot \varepsilon \neq \Delta_q \quad \text{for } p \neq 0,\ p, q \in NT.$$

Δ is consistent with the set T of sentences of $\mathcal{L}$ which are true in $\mathcal{Q}$. Hence there exists a denumerable structure $\mathcal{R} = \langle A, 0, 1, +, \cdot, \epsilon \rangle$ which is a model for $T \cup \Delta$. Letting $\mathcal{R}_0 = \langle A, 0, 1, +, \cdot \rangle$, we have $\bigvee_\epsilon (\Delta_p \cdot \epsilon \neq \Delta_q)$ true in $\mathcal{R}_0$ but not in $\mathcal{Q}$.

However, all non-standard rational fields are elementary extensions of $\mathcal{Q}$: $\mathcal{Q} \leq \mathcal{Q}' \wedge \mathcal{Q} \equiv \mathcal{Q}' \Rightarrow \mathcal{Q} \prec \mathcal{Q}'$. For if $r_1, \ldots, r_n$ satisfy $\phi(x_1, \ldots, x_n)$ in $\mathcal{Q}$, then

$$\bigvee_{x_1,\ldots,x_n} (\Delta_{p_1} \cdot x_1 = \Delta_{q_1} \wedge \ldots \wedge \Delta_{p_n} \cdot x_n = \Delta_{q_n} \wedge \phi(x_1, \ldots, x_n))$$

is true in $\mathcal{Q}$. Hence it is true in $\mathcal{Q}'$, and the same elements $r_1, \ldots, r_n$ satisfy ϕ in $\mathcal{Q}'$.

A <u>complex field</u> $\mathcal{C} = \langle C, 0, 1, +, \cdot \rangle$ satisfies the following schema:

(i) algebraically closed: $\bigwedge_{x_1,\ldots,x_n} \bigvee_y (y^n + x_1 \cdot y^{n-1} + \ldots + x_n = 0)$

(ii) characteristic 0: $1+1 \neq 0, \; 1+1+1 \neq 0, \ldots$

We shall prove that any field satisfying (i) and (ii) is arithmetically equivalent to $\mathcal{C}$. Thus the non-standard complex fields are precisely the <u>algebraically closed fields</u> of characteristic 0.

A <u>real closed field</u> is a maximal real field (in the sense that adjoining i gives $\mathcal{C}$). Real fields are characterized by the sentences

(i) $\bigwedge_{x,y} (x \cdot x + y \cdot y \neq -1), \; \bigwedge_{x,y,z} (x \cdot x + y \cdot y + z \cdot z \neq -1), \ldots$

Real closed fields are characterized by (i) and

(ii) every equation of an odd degree has a root

(iii) every number or its negative has a square root.

It is true that all real closed fields are arithmetically equivalent.

<u>Problem</u>. "If every element of R is definable in $\mathcal{R}$, then $\mathcal{R} \leq \mathcal{S} \wedge \mathcal{R} \equiv \mathcal{S} \Rightarrow \mathcal{R} \prec \mathcal{S}$." Show that this statement is false, and prove the strongest statement possible by restricting the kinds of defining formulas. Hint: look at the formulas in prenex form.

A set T of sentences of $\mathcal{L}$ is <u>complete</u> iff for every sentence θ of $\mathcal{L}$, either $T \vdash \theta$ or $T \vdash \neg\theta$. (syntactical completeness)

A set T of sentences of $\mathcal{L}$ is <u>semantically complete</u> iff for every pair $\mathfrak{R}, \mathfrak{S}$ of structures of $\mathcal{L}$, if every sentence of T is true in both $\mathfrak{R}$ and $\mathfrak{S}$, then $\mathfrak{R} \equiv \mathfrak{S}$.

E.g., the set of sentences for algebraically closed fields of characteristic 0 is complete.

If $\mathcal{S}$ is a class of structures of $\mathcal{L}$, then the <u>theory</u> of $\mathcal{S}$ ($\mathcal{T}h\,\mathcal{S}$) is the set of sentences of $\mathcal{L}$ which are true in every structure of $\mathcal{S}$.

An open problem is whether or not the theory of finite fields can be axiomatized; i.e., whether the set of true sentences of the theory is recursive. This is equivalent to asking if the set is recursively enumerable, since its complement may be enumerated. It is known that the set of true sentences of finite group theory is not r.e.

The sentence $\bigwedge_x \bigvee_{y,z} (x = y \cdot y + z \cdot z)$ holds in all rational finite fields but not in all infinite fields. For if the characteristic of the field is 2, every number is a square. If the characteristic is odd, there are $\frac{p^n-1}{2}$ non-zero squares, or $\frac{p^n+1}{2}$ squares. Hence more than half of the elements of the field are squares, so that the sets $\{y^2\}$, $\{x - z^2\}$ must have an element in common. In infinite fields, the most that can be said is that every number is the sum of four squares.

Let $\mathfrak{R}_k = \langle A_k, R_k, \ldots \rangle$ be structures of some predicate logic $\mathcal{L}$ for all $k \in \mathcal{K}$. Then we define

$$\cup \mathfrak{R}_k = \langle \cup A_k, \cup R_k, \ldots \rangle.$$

<u>Example</u>. Let $\mathcal{L}_i = \langle \mathbb{N}_i, < \rangle$, where $\mathbb{N}_i = \{x : x \in \mathbb{N} \wedge x \geq i\}$.

Then $\bigcup \mathcal{L}_i = \langle \mathbb{N}, < \rangle = \mathcal{L}$.

$\mathcal{L}_i \cong \mathcal{L}_j$ for all i, j $\qquad \mathcal{L}_i \equiv \mathcal{L}_j$

$\mathcal{L}_i \leq \mathcal{L}_j$ for all $j \leq i$

$\mathcal{L}_i \leq \bigcup \mathcal{L}_j$

but $\mathcal{L}_i \not\equiv \mathcal{L}$

$\mathcal{L}_i \not\prec \mathcal{L}$.

<u>Lemma</u>. If $\mathcal{K}$ is a family of structures of a p.l. $\mathcal{L}$ such that any two elements of $\mathcal{K}$ have a common extension, then $\bigcup \mathcal{K}$ is an extension of every structure of $\mathcal{K}$.

<u>Proof</u>: Let $\mathcal{S} = \bigcup \mathcal{K} = \langle B, S, \ldots \rangle$ and suppose $\mathcal{R} = \langle A, R, \ldots \rangle \in \mathcal{K}$. $A \subseteq B$ by definition and since $R \subseteq S$, $Rxy \to Sxy$. Conversely, if $x, y \in A$, then Sxy implies there is a $\mathcal{T} = \langle C, T, \ldots \rangle \in \mathcal{K}$ such that $x, y \in C$ and Txy. Let $\mathcal{U}$ be a common extension of $\mathcal{R}$ and $\mathcal{T}$. Then $Txy \Rightarrow Uxy \Rightarrow Rxy$.

<u>Theorem</u>. If $\mathcal{K}$ is a family of structures of a p.l. $\mathcal{L}$ such that any two structures of $\mathcal{K}$ have a common elementary extension, then $\bigcup \mathcal{K}$ is an elementary extension of every structure of $\mathcal{K}$.

<u>Proof</u>: We prove by induction on the length of a formula ϕ of $\mathcal{L}$ that

(*) for any $\mathcal{R} \in \mathcal{K}$ and $a_1, \ldots, a_n \in R$, if $a_1, \ldots, a_n$ satisfy ϕ in $\mathcal{R}$, $a_1, \ldots, a_n$ satisfy ϕ in $\bigcup \mathcal{K}$.

<u>Case 1</u>. If ϕ is an atomic formula, (*) holds by the lemma.

<u>Cases 2, 3</u>. If (*) holds for ψ, χ, then (*) holds for $\neg\psi$, $\psi \to \chi$. (Details straightforward).

<u>Case 4.</u> Suppose (*) holds for ψ and $a_1, \ldots, a_n$ satisfy $\phi = \bigvee_\alpha \psi$ in $\mathfrak{A}$. Then there is an $a \in A$ such that $a_1, \ldots, a_n, a$ satisfy ψ in $\mathfrak{A}$ and hence in $\cup\mathfrak{K}$ by (*). Hence $a_1, \ldots, a_n$ satisfy $\bigvee_\alpha \psi$ in $\cup\mathfrak{K}$. Conversely if $a_1, \ldots, a_n \in A$ satisfy $\bigvee_\alpha \psi$ in $\cup\mathfrak{K}$, then $a_1, \ldots, a_n, b$ satisfy ψ in $\cup\mathfrak{K}$, and there is a $\mathfrak{C} = \langle C, T, \ldots \rangle \in \mathfrak{K}$ such that $b \in C$. By hypothesis, there is a $\mathfrak{C}' \in \mathfrak{K}$ such that $\mathfrak{A}, \mathfrak{C} \propto \mathfrak{C}'$. $a_1, \ldots, a_n, b$ satisfy ψ in $\mathfrak{C}'$ by (*), and hence $a_1, \ldots, a_n$ satisfy $\bigvee_\alpha \psi$ in $\mathfrak{C}'$ and finally in $\mathfrak{A}$ since $\mathfrak{A} \propto \mathfrak{C}'$.

<u>NB</u>: By the preceeding example we see that we cannot prove a similar theorem for $\equiv$ or $\cong$ extensions.

The following theorem gives a test for determining when an extension is elementary:

<u>Theorem.</u> Let $\mathfrak{A} = \langle A, R, \ldots \rangle$ and $\mathfrak{B} = \langle B, S, \ldots \rangle$ be structures of a p.l. $\mathcal{L}$. Then $\mathfrak{A} \propto \mathfrak{B}$ iff $\mathfrak{A} \leq \mathfrak{B}$ and for every sentence ϕ of $\mathcal{L}$ and elements $a_1, \ldots, a_n \in A$, $a_1, \ldots, a_n$ satisfy $\bigvee_\alpha \phi$ in $\mathfrak{B}$ implies there is an $a \in A$ such that $a_1, \ldots, a_n, a$ satisfy ϕ in $\mathfrak{B}$.

<u>Proof</u>: Similar to previous proof.

<u>Theorem</u> (Downwards Lowenheim-Skolem-Tarski)

Let $\mathfrak{A} = \langle A, R, \ldots \rangle$ be a structure of a denumerable predicate logic $\mathcal{L}$, and let C be any infinite subset of A. Then there exists a structure [redacted] $\mathfrak{B} = \langle B, S, \ldots \rangle$ such that $C \subseteq B$, card. C = card. B, and [redacted] $\mathfrak{B} \propto \mathfrak{A}$.

<u>Proof</u>: Well-order A. Let $\mathcal{B}_0 = C$ and $\mathcal{B}_{n+1}$ be the class of all $a \in A$ such that there exists a formula ϕ of $\mathcal{L}$ and elements $b_1, \ldots, b_k \in \mathcal{B}_n$ for which a is the first element in the ordering of A such that $b_1, \ldots, b_k, a$ satisfy ϕ. Set $B = \bigcup \mathcal{B}_n$ and $S = R \upharpoonright B, \ldots$; $\mathcal{S} = \langle B, S, \ldots \rangle$.

card B = card C since $\mathcal{L}$ has only $\aleph_0$ formulas and since there are only card $\mathcal{B}_n$ finite sequences of elements of $\mathcal{B}_n$.

By construction, $\mathcal{S} \subseteq \mathcal{R}$ (routine to check that operations are ok). If $b_1, \ldots, b_k \in B$ satisfy ~~ϕ in $\mathcal{S}$~~ $\bigvee \alpha \phi$ in $\mathcal{R}$, then for some n, $b_1, \ldots, b_k \in \mathcal{B}_n$, and hence there is an $a \in \mathcal{B}_{n+1} \subset B$ such that $b_1, \ldots, b_k, a$ satisfy ϕ in $\mathcal{R}$. Thus by the previous theorem, $\mathcal{S} \propto \mathcal{R}$.

The Downwards LST theorem can be generalized to a p.l. with v symbols, in which case C must have at least v elements. (or card B = max{card C, v}). That this is the best result may be seen by considering the p.l. of $2^{\aleph_0}$ symbols constructed earlier which has no denumerable model.

By the Downwards LST theorem, we may consider a model as the union of its denumerable substructures.

<u>Theorem</u> (Upwards Lowenheim-Skolem)

Let $\mathcal{R} = \langle A, R, \ldots \rangle$ be an infinite structure of a predicate logic $\mathcal{L}$ with v symbols. Then for all $\beta \geq \max\{v, \text{card } A\}$, there exists a structure $\mathcal{S} = \langle B, S, \ldots \rangle$ with card $B = \beta$ and such that $\mathcal{R} \propto \mathcal{S}$ properly; i.e., $A \neq B$.

Proof: Let $\mathcal{L}'$ be the p.l. obtained from $\mathcal{L}$ by adjoining constants for elements of A in a well-ordered sequence. Let $\mathcal{R}'$ be the structure corresponding to $\mathcal{R}$ in the enriched language, and let T be the set of true sentences of $\mathcal{R}'$. Now let $\mathcal{S}'$ be a structure of card β satisfying T, and let $\mathcal{S}$ be the structure of the original language $\mathcal{L}$ corresponding to $\mathcal{S}'$. $\mathcal{R}' \equiv \mathcal{S}'$ and $\mathcal{R}' \leq \mathcal{S}'$ by construction. Also, since every element of A' has a name in $\mathcal{L}'$, $\mathcal{R}' \propto \mathcal{S}'$.

Again we cannot do better since, for example, any proper extension of $\langle NT, <, S_0, S_1, \ldots \rangle$ (S_ν = subset of NT) has $\geq 2^{\aleph_0}$ elements. Still, we can prove the following slightly stronger theorem:

Theorem. Let $\mathcal{R} = \langle A, R, \ldots \rangle$ be a structure of a p.l. $\mathcal{L}$ with ν symbols. If card $A = \aleph_0$, then there exists a structure $\mathcal{S} = \langle B, S, \ldots \rangle$ of $\mathcal{L}$ such that card $B = 2^{\aleph_0}$ and $\mathcal{R} \propto \mathcal{S}$.

Proof: Since A is denumerable, there are at most $2^{\aleph_0}$ distinct relations in $\mathcal{R}$. Let $\mathcal{R}'$ be obtained from $\mathcal{R}$ by deleting all but the first occurrence of a given relation and let $\mathcal{L}'$ be the p.l. corresponding to $\mathcal{R}'$. $\mathcal{L}'$ has $\mu \leq 2^{\aleph_0}$ symbols, and by the Upwards LS Theorem, there is a structure $\mathcal{S}'$ of $\mathcal{L}'$ such that $\mathcal{R}' \propto \mathcal{S}'$ and card $\mathcal{S}' = 2^{\aleph_0}$. Let $\mathcal{S}$ be the structure of $\mathcal{L}$ corresponding to $\mathcal{S}'$. By construction, card $\mathcal{S} = 2^{\aleph_0}$, $\mathcal{R} \leq \mathcal{S}$. Suppose $a_1 \ldots a_n$ satisfy Φ in $\mathcal{R}$, and let Φ' be the corresponding formula of $\mathcal{L}'$. Then $a_1 \ldots a_n$ satisfy Φ' in $\mathcal{R}'$ and hence in $\mathcal{S}'$ and $\mathcal{S}$. Thus $\mathcal{R} \propto \mathcal{S}$.

Finitization of Theories

General problem: When can a set of sentences be derived from a finite subset?

E.g., later we shall show that Peano's axioms are not finitizable, but that the stronger set theory, in which Peano's axioms may be derived, is finitizable.

Definitions: If Σ is a set of sentences of a p.l. $\mathcal{L}$, then Mod Σ is the class of all structures of $\mathcal{L}$ in which all sentences of Σ hold.

A class $\mathcal{C}$ of structures is elementary iff there is a sentence ϕ such that $\mathcal{C} = \text{Mod}\,\phi$.

A class $\mathcal{C}$ of sentences is elementary in the wider sense iff there is a class Σ of sentences such that $\mathcal{C} = \text{Mod}\,\Sigma$.

Examples

1. The class of infinite fields is elementary in the wider sense. Take Σ to be the field axioms plus the sentences N_k asserting the existence of k distinct elements.

   The class of finite fields is not elementary in the wider sense since if a set Σ of sentences has arbitrarily large finite models, it has an infinite model.

   Hence the class of infinite fields is not elementary, for if it were equal to Mod ϕ, then Mod $\neg\phi$ would be the class of all structures which were not infinite fields, and Mod $\{\neg\phi$, field axioms$\}$ would be the class of finite fields.

2. The class of fields of characteristic 0 is elementary in the wider sense.

The class of fields of non-zero characteristic ~~are~~ is not elementary in the wider sense. For suppose it is equal to Mod Σ. Then $\Delta = \{1+1\neq 0, 1+1+1\neq 0, \ldots\}$ is consistent with Σ, so that $\Sigma \cup \Delta$ has a model of characteristic 0.

Hence the class of fields of characteristic 0 is not elementary.

Complete Theories

We shall develop three methods for determining when a set Γ of sentences is (syntactically) complete: the method of the elimination of quantifiers, Vaught's Test, and the Prime Model Test.

Elimination of Quantifiers

This method was originally developed by Tarski and is the most adaptable to machine computation. It proceeds as follows: Suppose $\mathcal{L}$ is a predicate logic and ϕ is a formula of $\mathcal{L}$ with at least one bound variable. Then we may put ϕ in prenex normal form and distribute the $\neg$, $\vee$, and $\wedge$ in the quantifier free part so that

$$\phi \leftrightarrow Q[\neg]\bigvee_x(\phi_1 \vee \ldots \vee \phi_n),$$

where each ϕ_i is a conjunct of atomic formulas and negations of atomic formulas, Q a (possibly empty) string of quantifiers, and $[\neg]$ indicates that the '$\neg$' may or may not be present depending on the type of the last quantifier. Then

$$\phi \leftrightarrow Q[\neg](\bigvee_x\phi_1 \vee \ldots \bigvee_x\phi_n).$$

Now to show that a set Γ of sentences is complete, it suffices to show first that for every ϕ_i as above, there exists a formula θ with no bound variables and in which x is not free such that $\Gamma \vdash \bigvee_x \phi_i \leftrightarrow \theta$. This first step establishes that every ~~formula~~ sentence ϕ is equivalent to a sentence θ with no bound variables (via the normal form above). Thus it then suffices to show that for every such θ, either $\Gamma \vdash \theta$ or $\Gamma \vdash \neg\theta$.

In carrying out the two main steps of this argument, we will allow ourselves to enrich the language $\mathcal{L}$ by new definitions, provided that we can prove the eliminability of such definitions on the basis of the set Γ. In outline then, the steps of the method are:

I. Start with a set T of sentences of a p.l. $\mathcal{L}$. Formulate a set Δ of definitions (dictated by succeeding steps), and let $\mathcal{L}'$ be the enriched language containing names for the defined objects.

II. Let θ be a typical conjunct of atomic formulas and negations of atomic formulas of $\mathcal{L}'$ (with parameters indicating the number of each type of atomic formula). Reduce the complexity of θ by new definitions if possible.

III. Show $T \cup \Delta \vdash \bigvee_{\alpha} \theta \leftrightarrow \psi$, for some formula ψ of $\mathcal{L}'$ without bound variables and with no additional free variables.

IV. Show that every sentence of $\mathcal{L}'$ without bound variables is decidable from $T \cup \Delta$.

(V). List or prove lemmas needed for steps I-IV. In case T was empty to start with, this provides a set of axioms for the theory involved.

<u>Example</u>: Consider $Th \langle RT, \leq, 0, 1 \rangle$, where RT is the set of rationals in $[0,1]$.

I. We take for T the sentences we know to be true:

$$\bigwedge_{x,y,z} (x \leq y \wedge y \leq z \rightarrow x \leq z) \qquad \bigwedge_{x,y} \bigvee_{z} (x \leq y \wedge x \neq y \rightarrow x \leq z \wedge x \neq z \wedge z \leq y \wedge z \neq y)$$

$$\bigwedge_{x,y} (x \leq y \vee y \leq x) \qquad \bigwedge_{x} (0 \leq x \wedge x \leq 1)$$

$$\bigwedge_{x,y} (x \leq y \wedge y \leq x \rightarrow x = y) \qquad 0 \neq 1$$

For additional definitions, we take

$$\bigwedge_{x,y} (x < y \leftrightarrow x \leq y \wedge x \neq y)$$

$$T \leftrightarrow 0 = 0$$

$$F \leftrightarrow 0 \neq 0$$

II. In the original language $\mathcal{L}$, there are four types of atomic ~~sentences~~ formulas and negations of atomic formulas:

$$\alpha = \beta, \quad \alpha \leq \beta, \quad \neg\, \alpha = \beta, \quad \neg\, \alpha \leq \beta,$$

where α, β are either variables, 0, or 1.

In the expanded language, we can reduce this number to two types: $\alpha = \beta$ and $\alpha < \beta$ since

$$\alpha \le \beta \leftrightarrow \alpha < \beta \vee \alpha = \beta$$
$$\neg \alpha = \beta \leftrightarrow \alpha < \beta \vee \beta < \alpha$$
$$\neg \alpha \le \beta \leftrightarrow \beta < \alpha$$

Then a typical Θ is

$$\alpha_1 < x \wedge \ldots \wedge \alpha_\ell < x \wedge x < \beta_1 \wedge \ldots \wedge x < \beta_m \wedge x = \gamma_1 \wedge \ldots \wedge x = \gamma_n \wedge [\Psi],$$

where $\alpha_i, \beta_i, \gamma_i$ are variables distinct from x or constants, and Ψ does not contain x.

III. We perform the reduction of $\bigvee_x \Theta$ in five cases:

__Case 1.__ $\ell = m = n = 0$. $\bigvee_x \Theta \leftrightarrow \Psi$.

__Case 2.__ $n \neq 0$. Let $\Theta(\gamma_1)$ be obtained from Θ by substituting an occurrence of γ_1 for each occurrence of x. Then $\bigvee_x \Theta \leftrightarrow \Theta(\gamma_1)$

__Case 3.__ $n = 0$; $\ell, m \neq 0$. We can show by induction that

$$\bigvee_x \Theta \leftrightarrow \alpha_1 < \beta_1 \wedge \ldots \wedge \alpha_\ell < \beta_1 \wedge \alpha_1 < \beta_2 \wedge \ldots \wedge \alpha_\ell < \beta_2 \wedge \ldots \wedge \alpha_1 < \beta_m \wedge \ldots \wedge \alpha_\ell < \beta_m \wedge [\Psi]$$

__Case 4.__ $\ell = n = 0$; $m \neq 0$. $\bigvee_x \Theta \leftrightarrow 0 < \beta_1 \wedge \ldots \wedge 0 < \beta_m \wedge [\Psi]$

__Case 5.__ $m = n = 0$; $\ell \neq 0$ $\bigvee_x \Theta \leftrightarrow \alpha_1 < 1 \wedge \ldots \wedge \alpha_\ell < 1 \wedge [\Psi]$

IV. We note that

$\alpha < \alpha \leftrightarrow F$	$F \vee \Theta \leftrightarrow \Theta$	$T \vee \Theta \leftrightarrow T$
$\alpha < 0 \leftrightarrow F$	$F \wedge \Theta \leftrightarrow F$	$T \wedge \Theta \leftrightarrow \Theta$
$1 < \alpha \leftrightarrow F$	$\neg F \leftrightarrow T$	$\neg T \leftrightarrow F$
$0 < 1 \leftrightarrow T$		

and that the reduced formula X obtained by iterating III contains only the formulas $0<1$, $1<0$, $0=1$, T, F. Hence $T \vdash X$ or $T \vdash \neg X$.

V. The axioms listed in I are sufficient to establish the reductions in III and IV.

Vaughts–Łoś Test

Definition. A consistent set Γ of sentences of a p.l. $\mathcal{L}$ is $\underline{\nu\text{-categorical}}$ iff all models of Γ with cardinality ν are isomorphic.

Vaught's Theorem. Suppose Γ is a consistent set of sentences of a p.l. $\mathcal{L}$ with λ symbols such that Γ has no finite models and Γ is ν-categorical for some $\nu \geq \lambda$. Then Γ is complete.

Proof: Suppose $\neg\theta$ is not decidable from Γ. Then $\Gamma \cup \{\theta\}$ is consistent, and since Γ has no finite models, Γ, θ must have an infinite model. Hence by the Lowenheim-Skolem Theorem, Γ, θ has a model of cardinality ν; say $\mathfrak{R}$. Similarly, let $\mathfrak{S}$ be a model of $\Gamma, \neg\theta$ of cardinality ν. Then $\mathfrak{R} \not\equiv \mathfrak{S}$, so that $\mathfrak{R} \not\cong \mathfrak{S}$, which contradicts the ν-categoricity of Γ.

Example. Let Γ be the set of axioms for $Th\langle RT, <, 0, 1\rangle$. Then Γ is consistent and has no finite models. Moreover, Γ is $\aleph_0$-categorical by Cantor's Theorem, so that Γ is complete.

Cantor's Theorem states that all dense enumerable simple orderings are isomorphic. For let $\langle A, <, 0, 1\rangle$ and $\langle B, <, 0, 1\rangle$ be structures of $Th\langle RT, <, 0, 1\rangle$, and enumerate A and B by $0, 1, a_1, a_2, \ldots$; $0, 1, b_1, b_2, \ldots$ We construct an isomorphism F by

$F0 = 0 \qquad F1 = 1 \qquad Fa_1 = b_1$

$Fa_2 =$ first element of $B - \{0, 1, b_1\}$ in same relation to b_1 as a_2 is to a_1 ; say b'

if $b' \neq b_2$, $F^{-1}b_2 = 1^{st}$ element of $A - \{0, 1, a_1, a_2\}$ which works

Continue working back and forth between A and B in this manner. For more detail, see Kamke, Naive Set Theory.

Prime Model Test

Definitions.

Let $\mathcal{R}$ be a structure of a predicate language $\mathcal{L}$, and let $\mathcal{L}'$ be obtained from $\mathcal{L}$ by adjoining names for the elements of $\mathcal{R}$. Then the diagram of $\mathcal{R}$ ($\Delta_{\mathcal{R}}$) is the set of all atomic sentences and negations of atomic sentences of $\mathcal{L}'$ which hold in $\mathcal{R}$.

Let T be a non-empty consistent set of sentences of a p.l. $\mathcal{L}$. Then T is model-complete iff

I. for every $\mathcal{R}, \mathcal{S} \in \text{Mod}\ T$ such that $\mathcal{R} \leq \mathcal{S}$, also $\mathcal{R} \prec \mathcal{S}$.

or II. for every $\mathcal{R} \in \text{Mod}\ T$, $T \cup \Delta_{\mathcal{R}}$ is complete in $\mathcal{L}'$.

The two definitions of model completeness are equivalent. For suppose I holds and $T \cup \Delta_{\mathcal{R}}$ is not complete. Let Θ be undecidable from $T \cup \Delta_{\mathcal{R}}$ and hold in $\mathcal{R}$, and let $\mathcal{R}'$ be the structure of $\mathcal{L}'$ corresponding to $\mathcal{R}$. $T \cup \Delta_{\mathcal{R}}, \neg\Theta$ is consistent and has a model $\mathcal{S}'$. But $\Delta_{\mathcal{R}}$ holds in $\mathcal{S}'$ so that $\mathcal{R}' \leq \mathcal{S}'$ and by I, $\mathcal{R}' \prec \mathcal{S}'$, which is a contradiction. Conversely, let $\mathcal{R}, \mathcal{S} \in \text{Mod}\ T$, $\mathcal{R} \leq \mathcal{S}$. $T \cup \Delta_{\mathcal{R}}$ is complete by II, so that $\mathcal{S}$ also satisfies $\Delta_{\mathcal{R}}$.

Theorem. Let T be a consistent set of sentences, and suppose ϕ and ψ are sentences such that whenever $M, M' \in \text{Mod}\ T$, $M \leq M'$, and ϕ holds in M, then ψ holds in M'. Then there exists a purely existential sentence Θ for which $T \vdash \phi \to \Theta$ and $T \vdash \Theta \to \psi$.

Proof: Let ϵ be an arbitrary existential sentence for which $T \vdash \epsilon \to \psi$, and let Ω be the set of all such $\neg\epsilon$. Suppose $T \cup \Omega \cup \phi$ is consistent, and let $\mathcal{R}$ be a model. Now any structure $\mathcal{S}$ which satisfies $T \cup \Delta_{\mathcal{R}}$ is isomorphic to an extension of $\mathcal{R}$, and since ϕ holds in $\mathcal{R}$, ψ holds in $\mathcal{S}$. Hence $T \cup \Delta_{\mathcal{R}} \vdash \psi$.

In particular, for some finite subset $\{\delta_1, \dots, \delta_n\} \subseteq \Delta_{\mathcal{R}}$, $T \vdash \delta_1 \wedge \dots \wedge \delta_n \to \psi$. Let $\delta(a_1 \dots a_k) : \delta_1 \wedge \dots \wedge \delta_n$, where the $a_1 \dots a_k$ are those elements in the domain of $\mathcal{R}$ without names in $\mathcal{L}$.

$$T \vdash \neg \psi \to \neg \delta(a_1 \dots a_k)$$

$$T \vdash \neg \psi \to \bigwedge_{v_1 \dots v_k} \neg \delta(v_1 \dots v_k) \qquad \text{since } a_1 \dots a_k \text{ do not occur in } T, \psi$$

$$T \vdash \bigvee_{v_1 \dots v_k} \delta(v_1 \dots v_k) \to \psi$$

Hence $\neg \bigvee_{v_1 \dots v_k} \delta(v_1 \dots v_k) \in \Omega$, but $\bigvee_{v_1 \dots v_k} \delta(v_1 \dots v_k)$ holds in $\mathcal{R}$, which is a contradiction. Thus $T \cup \Omega \cup \phi$ is inconsistent. Consequently $T \cup \Omega \vdash \neg \phi$, and for some finite subset $\{\neg\omega_1, \dots, \neg\omega_n\} \subseteq \Omega$, $T \vdash \neg\omega_1 \wedge \dots \wedge \neg\omega_n \to \neg \phi$.

$$T \vdash \phi \to \omega_1 \vee \dots \vee \omega_n$$

$$T \vdash \omega_1 \vee \dots \vee \omega_n \to \psi \qquad \text{since } T \vdash \omega_i \to \psi \text{ for each } \omega_i$$

Furthermore, $\omega_1 \vee \dots \vee \omega_n$ may be placed in existential form by moving all quantifiers to the front.

__Corollary.__ If ϕ holds in M' whenever ϕ holds in M and $M \subseteq M'$ (ϕ __persistent under extension__), then there exists an existential sentence Θ for which $T \vdash \phi \leftrightarrow \Theta$.

__Corollary.__ (dual to above) If ϕ holds in M whenever ϕ holds in M' and $M \subseteq M'$ (ϕ __persistent under restriction__), then there exists a universal sentence Θ such that $T \vdash \phi \leftrightarrow \Theta$.

__Proof:__ If ϕ is persistent under restriction, then $\neg\phi$ is persistent under extension, and for some existential sentence Θ, $T \vdash \neg\phi \leftrightarrow \Theta$, or $T \vdash \phi \leftrightarrow \neg\Theta$. But $\neg\Theta$ is universal.

__Theorem.__ If T is model complete, then to every sentence ϕ corresponds a purely existential sentence Θ for which $T \vdash \phi \leftrightarrow \Theta$.

__Proof:__ If T is model complete, every sentence is persistent under extension.

Theorem. T is model complete iff for every formula ϕ with free variables $v_1, \ldots v_k$ there exists an existential formula ψ with no additional free variables such that $T \vdash \bigwedge_{v_1 \ldots v_k} (\phi \leftrightarrow \psi)$. (i.e., iff every definable set is existentially definable.)

Proof: Suppose T is model complete and $M \in \text{Mod}\, T$. Let $a_1 \ldots a_n$ satisfy ϕ in M. Then $a_1 \ldots a_n$ satisfy ϕ in every extension M' of M. Let $\mathcal{L}'$ be the language with names for the elements of M. Then $\phi(a_1 \ldots a_n)$ is persistent under extension with respect to T in $\mathcal{L}'$, and hence there is an existential sentence ψ in $\mathcal{L}'$ such that

$$T \vdash \phi(a_1, \ldots, a_n) \leftrightarrow \psi(a_1 \ldots a_n, b_1 \ldots b_m)$$

$$T \vdash \phi(a_1 \ldots a_n) \leftrightarrow \bigvee_{x_1 \ldots x_m} \psi(a_1 \ldots a_n, x_1 \ldots x_m)$$ since $b_1 \ldots b_m$ do not occur in T or ϕ. By generalization,

$$T \vdash \bigwedge_{v_1 \ldots v_n} [\, \phi(v_1 \ldots v_n) \leftrightarrow \bigvee_{x_1 \ldots x_m} \psi(v_1 \ldots v_n, x_1 \ldots x_m)],$$

which is the desired result.

Conversely, suppose such an existential formula ψ exists for every formula ϕ. ψ is persistent under extension, so that if $a_1 \ldots a_k$ satisfy ϕ in $M \in \text{Mod}\, T$, $a_1 \ldots a_k$ satisfy ϕ in all extension models. Hence all extensions of M are elementary and T is model complete.

Definition. A sentence ϕ is <u>primitive</u> iff it is purely existential with quantifier free part consisting of a conjunct of atomic formulas and negations of atomic formulas.

Theorem. T is model-complete iff for every $M \in \text{Mod}\, T$ and every primitive formula ϕ, $a_1 \ldots a_k$ satisfy ϕ in some $M' \supseteq M$ implies $a_1 \ldots a_k$ satisfy ϕ in M.

This theorem provides a test for model-completeness.

Proof: If the condition holds for primitive formulas, it holds for all existential formulas since

$$\bigvee_x (\phi_1 \vee \dots \vee \phi_k) \leftrightarrow \bigvee_x \phi_1 \vee \dots \vee \bigvee_x \phi_k.$$

Let ψ be any existential formula. Then $\psi(a_1 \dots a_k)$ is persistent under restriction in $\mathcal{L}'$, the language with names for elements of M. Hence there is an existential sentence θ such that

$$T \vdash \psi(a_1 \dots a_k) \leftrightarrow \neg\, \theta(a_1 \dots a_k)$$

$$T \vdash \neg \psi(a_1 \dots a_k) \leftrightarrow \theta(a_1 \dots a_k)$$

$$T \vdash \bigwedge_{v_1 \dots v_k} [\neg \psi(v_1 \dots v_k) \leftrightarrow \theta(a_1 \dots a_k)]$$

Thus all formulas are equivalent to existential formulas, and by the preceeding theorem, T is model complete.

Definition. Let T be a consistent non-empty set of sentences. A model M_0 of T is a *prime model* iff every model of T has a submodel isomorphic to M_0.

Lemma. Let M_0 be a prime model of T and let Δ_0 be its diagram. Then $T \cup \Delta_0 \vdash \phi$ iff $T \vdash \phi$.

Proof: If $T \cup \Delta_0 \vdash \phi$, then ϕ holds in all models of T, so that $T \vdash \phi$.

Theorem (Prime Model Test) If T is model-complete and has a prime model, then T is complete.

Proof: Since T is model complete, $T \cup \Delta_0$ is complete; and since M_0 is prime, T is then complete.

Some Applications of Tests for Completeness

Additive structure of fields

Let F be a finite field and consider Th < F, 0, + >. We may take as axioms the usual group axioms plus axioms asserting that the characteristic of F is p and F has p^k elements: $\bigwedge_x (\overbrace{x+x+\ldots+x}^{p \text{ times}} = 0)$, $\bigvee_{x_1 \ldots x_{p^k}} (x_1 \neq x_2 \wedge \ldots \wedge x_{p^k-1} \neq x_{p^k})$

All models for Th < F, 0, + > are isomorphic (as can be seen by identifying the k generators of the fields), and hence the theory is complete.

Suppose F is infinite of characteristic p. Then a complete set of axioms may be obtained by replacing the last one above by the set asserting the existence of infinitely many elements. The same reasoning applies; or we could use Vaught's Test.

Finally let F be infinite of characteristic 0. Axioms include the group axioms, $\bigvee_{x,y} (x \neq y)$, axioms for characteristic 0, and the set $\bigwedge_y \bigvee_x \; y = x+x$

$\bigwedge_y \bigvee_x \; y = x+x+x$, ... to insure that F has the structure of the rational field and not just of the integers.

Theory of the Integers under Addition

We propose to demonstrate by the method of elimination of quantifiers that Th < Int., 0, 1, +, < > is complete. The following axioms are due to Presburger:

A1. $x + 0 = x$

A2. $x + (y+z) = (x+y) + z$

A3. $\bigwedge_x \bigvee_y \; x + y = 0$

A4. $x + y = y + x$

} Group axioms

A5. $x<y \lor y=x \lor y<x$

A6. $\neg x<x$

A7. $x<y \land y<z \to x<z$

A8. $x<y \to x+z<y+z$

A9. $0<1$

A10. $\neg \bigvee_x (0<x \land x<1)$

A11. $\bigwedge_x \bigvee_y (x=y+y \lor x=y+y+1)$

$\bigwedge_x \bigvee_y (x=y+y+y \lor x=y+y+y+1 \lor x=y+y+y+1+1)$

$\vdots$

A11. serves as an induction scheme. Note that using A8. we can prove that the characteristic is 0: i.e., $x+x+\ldots+x=0 \to x=0$.

To simplify considerations, we introduce the following definitions:

(1) $1+1=2$, $1+1+1=3, \ldots$ (referred to as natural numbers)

(2) $0\cdot x=0$, $1\cdot x=x$, $2\cdot x=x+x, \ldots$ (multiplication by natural numbers)

(3) $x-y=z$ iff $x=y+z$

(4) $x\equiv y \mod k$ iff $\bigvee_z k\cdot z=x-y$ (k a natural number)

(5) $T \leftrightarrow 0=0$, $F \leftrightarrow 0\neq 0$

<u>Lemma</u>. If $0\le k<m$, where k and m are natural numbers, then $k\equiv 0 \mod m$ implies $k=0$.

<u>Proof</u>: If $k\equiv 0 \mod m$, $\bigvee_u k=m\cdot u$. Now if $u\le 0$, [redacted] $m\cdot u\le 0$. Likewise $1\le u$ implies $m\le m\cdot u$. Hence $u=0$.

We must now consider formulas constructed from the following atomic parts:

$\alpha=\beta$, $\alpha\neq\beta$, $\alpha<\beta$, $\neg\alpha<\beta$, $\alpha\equiv\beta \mod k$, $\alpha\not\equiv\beta \mod k$,

where α and β are terms constructed from $+$ and $k\cdot$. First we simplify the types of formulas to be considered:

(i) All negations of atomic formulas may be eliminated since

$\alpha\neq\beta \leftrightarrow \alpha<\beta \lor \beta<\alpha$

$\neg\alpha<\beta \leftrightarrow \alpha=\beta \lor \beta<\alpha$

$\neg\alpha\equiv\beta \mod k \leftrightarrow \alpha\equiv\beta+1 \mod k \lor \ldots \lor \alpha\equiv\beta+(k-1) \mod k$

(ii) Next, singling out the variable x, we can move all x's to the same side of the $=$ or $<$ sign, so that we need consider only formulas of the types

$$j\cdot x = \alpha \ ; \ k\cdot x \equiv \beta \bmod k' \ ; \ \gamma < l\cdot x \ ; \ m\cdot x < \delta \ ; \ \psi$$

where ψ is a formula not containing x.

<u>Lemma</u>. $k\cdot x \equiv \beta \bmod m \leftrightarrow tk\cdot x \equiv t\beta \bmod tm$

<u>Proof</u>: $k\cdot x \equiv \beta \bmod m \leftrightarrow k\cdot x - \beta = m\cdot u$

$\leftrightarrow tk\cdot x - t\beta = tm\cdot u$ (by preceeding lemma)

$\leftrightarrow tk\cdot x \equiv t\beta \bmod tm$

(iii) We may further take all coefficients of x to be the same since if $t \neq 0$,

$$j\cdot x = \alpha \leftrightarrow tj\cdot x = t\alpha$$
$$j\cdot x < \alpha \leftrightarrow tj\cdot x < t\alpha$$
$$k\cdot x \equiv \beta \bmod m \leftrightarrow tk\cdot x \equiv t\beta \bmod tm$$

Hence by taking n equal to the least common multiple of the coefficients of x, we reduce to formulas like

$$n\cdot x = \alpha \ ; \ n\cdot x \equiv \beta \bmod k \ ; \ \gamma < n\cdot x \ ; \ n\cdot x < \delta \ ; \ \psi$$

(iv) The coefficient of x may be eliminated by a change of variable $x' = n\cdot x$ if we stipulate $x' \equiv 0 \bmod n$. Thus we reduce to the formulas

$$x = \alpha \ ; \ x \equiv \beta \bmod k \ ; \ \gamma < x \ ; \ x < \delta \ ; \ \psi$$

(v) All congruences may be taken to be of the form $x \equiv \beta \bmod p^k$ for p prime by the following lemma.

<u>Lemma</u>. $x \equiv 0 \bmod mn \leftrightarrow x \equiv 0 \bmod m \wedge x \equiv 0 \bmod n$ for $(m,n) = 1$

<u>Proof</u>: If $(m,n) = 1$, then $\bigvee_{j,k} (km - jn) = 1$. Suppose $x = mu = nv$. Then $mn(kv - ju) = mkx - jnx = x$, so that $x \equiv 0 \bmod mn$. The converse is trivial.

(vi) We may further reduce congruences so that a given prime occurs to the same power in all its congruences. For suppose $x \equiv \alpha \mod p^k$ and $x \equiv \beta \mod p^\ell$. If $k = \ell$, we may replace the second congruence by $\alpha \equiv \beta \mod p^k$. If $k < \ell$, then

$$x \equiv \alpha \mod p^k \leftrightarrow x \equiv \alpha \mod p^\ell \vee x \equiv \alpha + p^k \mod p^\ell \vee \dots \vee x \equiv \alpha + (p^{\ell-k}-1)p^k \mod p^\ell.$$

<u>Lemma</u>. If $km - jn = 1$, then $x \equiv \alpha \mod m$ and $x \equiv \beta \mod n$ iff $x \equiv km\beta - jn\alpha \mod mn$.

<u>Proof</u>: Suppose $x \equiv \alpha \mod m$ and $x \equiv \beta \mod n$. Then $jnx \equiv jn\alpha \mod mn$ and $kmx \equiv km\beta \mod mn$, and hence $x \equiv km\beta - jn\alpha \mod mn$.

Conversely, if $x \equiv km\beta - jn\alpha \mod mn$, then $x \equiv -jn\alpha \mod m$. $x \equiv km\alpha - jn\alpha \mod m$ and thus $x \equiv \alpha \mod m$. Likewise $x \equiv \beta \mod n$.

(vii) By the preceeding lemma, all congruences may be combined into one since their moduli are relatively prime.

We now describe how to eliminate the quantifier from $\bigvee_x \phi$, where ϕ is the typical conjunct

$$x = \alpha_1 \wedge \dots \wedge x = \alpha_j \wedge [x \equiv \beta \mod m] \wedge \gamma_1 < x \wedge \dots \wedge \gamma_k < x$$
$$\wedge\, x < \delta_1 \wedge \dots \wedge x < \delta_\ell \wedge [\psi]$$

<u>Case I</u>. $j \neq 0$. Then $\bigvee_x \phi(x) \leftrightarrow \phi(\alpha_1)$.

<u>Case II</u>. $j = 0$. $k = 0$ or $\ell = 0$. $\bigvee_x \phi \leftrightarrow T \wedge [\psi]$ since congruences have arbitrarily large (or small) solutions.

<u>Case III</u>. No congruence, $j = 0$, $k \neq 0$, $\ell \neq 0$.

$$\bigvee_x \phi \leftrightarrow \gamma_1 + 1 < \delta_1 \wedge \dots \wedge \gamma_1 + 1 < \delta_\ell \wedge \dots \wedge \gamma_k + 1 < \delta_1 \wedge \dots \wedge \gamma_k + 1 < \delta_\ell \wedge [\psi]$$

<u>Case IV</u>. Congruence, $j=0$, $k\neq 0$, $\ell \neq 0$.

Then ϕ is equivalent to the disjunction of $k\times\ell$ formulas of the type

$$\gamma_1 < \gamma_i \wedge \dots \wedge \gamma_{i-1} < \gamma_i \wedge \gamma_{i+1} < \gamma_i \wedge \dots \wedge \gamma_k < \gamma_i$$
$$\wedge\ \delta_j < \delta_1 \wedge \dots \wedge \delta_j < \delta_{j-1} \wedge \delta_j < \delta_{j+1} \wedge \dots \wedge \delta_j < \delta_\ell$$
$$\wedge\ x \equiv \beta \bmod m \wedge \gamma_i < x \wedge x < \delta_j$$

where $0 < i \leq k$ and $0 < j \leq \ell$. Then the quantifier in $\bigvee_x \phi$ may be eliminated by noting that

$$x \equiv \beta \bmod m \wedge \gamma < x \wedge x < \delta$$
$$\leftrightarrow (\gamma+1 \equiv \beta \bmod m \wedge \gamma+1 < \delta)$$
$$\vee (\gamma+2 \equiv \beta \bmod m \wedge \gamma+2 < \delta) \vee \dots$$
$$\vee (\gamma+m \equiv \beta \bmod m \wedge \gamma+m < \delta)$$

This completes the proof by elimination of quantifiers that $Th\langle \mathbb{N}, 0, 1, +, < \rangle$ is complete.

Suppose we wish to consider the natural numbers under addition. We could repeat the above proof for $Th\langle Nat, 0, 1, +, < \rangle$ by replacing A3 and A9 by

A3'. $\bigwedge_{x,y} \bigvee_z (x+z=y \vee y+z=x)$

A9'. $0<1 \wedge 0=x \vee 1=x \vee 1<x$.

However an easier proof of the completeness of $Th\langle Nat, 0, 1, +, < \rangle$ is afforded by defining

$$Nat\, x \leftrightarrow x=0 \vee 0<x$$

and considering the formulas

$$\bigvee_x [\phi(x) \wedge Nat\, x] \quad , \quad \bigwedge_x [Nat\, x \to \phi(x)].$$

Then the completeness of $Th\langle \mathbb{N}, 0, 1, +, < \rangle$ yields the completeness of $Th\langle Nat, 0, 1, +, < \rangle$.

<u>Problem</u>. Investigate the problem of finding a complete set of axioms for $Th\langle Pos.\ Int., 1, \cdot \rangle$. This theory was proved to be decidable by Skolem in 1930 and Mostowski in 1952 (JSL), but as of yet no one has produced a complete set of axioms.

Feferman has shown $Th\langle Pos.\ Int., 1, \cdot, \approx \rangle$ is still decidable, where $x \approx y$ iff x and y have the same number of prime factors.

The Rationals under Multiplication

To illustrate one possible method of attacking the preceeding problem, we derive a complete set of axioms for Th<Rat, 1, ·>. The method is based on the characterization of abelian groups by Wanda Szmielew in Fundamenta Math (1954).

Definition. An abelian group A is of the first kind iff there exists a positive integer n such that $nA = 0$. Otherwise, A is of the second kind.

Definition. Elements $x_1, \ldots, x_n$ are linearly independent mod m iff for all integers $a_1, \ldots, a_n$, $\Sigma a_i x_i = 0$ implies $a_i \equiv 0 \bmod m$ for all i.

$x_1, \ldots, x_n$ are strongly linearly independent mod m iff for all integers $a_1, \ldots, a_n$, $\Sigma a_i x_i \equiv 0 \bmod m$ implies $a_i \equiv 0 \bmod m$ for all i.

Theorem. (Szmielew) Two abelian groups are arithmetically equivalent iff they are of the same kind and for every prime p and positive integer k, the maximum number of elements in each group is the same for each of the following classes:

(i) elements strongly l.i. mod p^k

(ii) elements of order p^k which are l.i. mod p^k

(iii) elements of order p^k which are strongly l.i. mod p^k.

Using this theorem, we may characterize the Th<Rat, 1, ·> by the usual group axioms plus the following axioms: First, a set asserting the group is of the second kind - $\bigvee_x x \neq 1$, $\bigvee_x x \cdot x \neq 1$, $\bigvee_x x \cdot x \cdot x \neq 1, \ldots$

Next we want axioms stating that 1 is the only element of order p^k. This will then satisfy conditions (ii) and (iii). We take
$$x \neq 1 \rightarrow x^2 \neq 1$$
$$x \neq 1 \rightarrow x^3 \neq 1,$$
$$\vdots$$

Notice that the axioms in the last paragraph are now redundant, as they may be derived from these plus $\bigvee_x x \neq 1$.

Finally, in order to satisfy (i), we want to assert the existence of arbitrarily many linearly independent mod m elements. We exhibit such an axiom for two l.i. elements mod m, omitting the generalization. We want elements x, y such that $\bigvee_z x^a y^b = z^m \rightarrow a \equiv b \equiv 0 \bmod m$, or equivalently
$$a \not\equiv 0 \vee b \not\equiv 0 \bmod m \rightarrow \bigwedge_z x^a y^b \neq z^m.$$
We may state this in a first order language by
$$\bigvee_{x,y} \bigwedge_{z_1, \ldots, z_{\frac{m(m-1)}{2}}} [x \neq z_1^m \wedge xy \neq z_2^m \wedge xy^2 \neq z_3^m \wedge \ldots \wedge x^{m-1} y^{m-1} \neq z_{\frac{m(m-1)}{2}}].$$

No such characterization is available for groups in general since general group theory is not decidable. The same applies to the theory of fields.

<u>Problem.</u> Suppose an element a is not a square in a model A of arithmetic. Is there a model $B \succ A$ of arithmetic in which a is a square? State and prove a general theorem of which this is a special case.

Real Closed Fields

We now establish the previously mentioned fact that all real closed fields are arithmetically equivalent by showing that their theory is complete. The result was first established by Tarski by the method of the elimination of quantifiers. Our demonstration is due to [redacted] A. Robinson and utilizes model-completeness.

We recall that a field is <u>formally real</u> iff -1 is not the sum of squares (notion due to Artin & Schreir - 1926). A real field has characteristic 0. A field is <u>real closed</u> iff it is real and no proper algebraic extension is real. Since this definition cannot be axiomatized as such in a first order language, we employ the following result:

<u>Definition.</u> A field R is <u>ordered</u> iff there exists a subset of elements of R called the positive elements (written $\{a>0\}$) such that for all $a \in R$,

(i) exactly one of $a=0$, $a>0$, $0>a$ holds

(ii) $a>0 \wedge b>0 \rightarrow a+b>0,\ a \cdot b>0$

Also, (iii) $a>b$ means $a-b>0$.

<u>Theorem.</u> A field R is real closed iff R is real, every polynomial of odd degree has a solution in R, and $\bigwedge_a \bigvee_x (a = x^2 \vee -a = x^2)$.

<u>Theorem.</u> Every ordered field has a uniquely determined (up to isomorphism) real algebraic extension which is real closed.

If we adjoin i as a root of $x^2=-1$ to a real closed field R, then the result is an algebraically closed field, and every polynomial may be factored as

(*) $(x-a_1)\cdots(x-a_n)[x-(b_1+ic_1)]\cdots[x-(b_m+ic_m)]$,

or in the real field itself as

$$(x-a_1)\cdots(x-a_n)[(x-b_1)^2+c_1^2]\cdots[(x-b_m)^2+c_m^2]$$

since every factor in (*) occurs with its conjugate.

Thus the ordering of a transcendental extension $R(\alpha)$ is completely determined by the ordering of α with respect to the elements of R, for every element of $R(\alpha)$ may be written as

$$a_0 \frac{P(\alpha)}{Q(\alpha)} = a_0 \frac{P(\alpha)\,Q(\alpha)}{Q(\alpha)^2},$$

where P and Q are polynomials.

Let P be the set of axioms for real closed fields. We show that P is model-complete. Let $M(x_1,\dots,x_m, u_1,\dots,u_n)$ be a conjunction of formulas of the types

$\alpha=\beta,\ \alpha\neq\beta,\ \alpha>\beta,\ \alpha\leq\beta,\ \alpha+\beta=\gamma,\ \alpha+\beta\neq\gamma,\ \alpha\cdot\beta=\gamma,\ \alpha\cdot\beta\neq\gamma,$

where α,β,γ are one of the variables $x_1,\dots,x_m, u_1,\dots,u_n$, 0, or 1. Suppose R and S are real closed fields, $R\leq S$, and for some $a_1,\dots,a_m$ in R,

$$(*) \quad \bigvee_{u_1\cdots u_n} M(a_1,\dots,a_m, u_1,\dots,u_n)$$

holds in S. We need to show that (*) holds in R.

We proceed by contradiction. Suppose M is a formula such that (*) holds in S but not in R, and such that the number n of bound variables is the minimum for which such a formula exists. Since (*) holds in S, there is a b in S such that (**) $\bigvee_{u_1\cdots u_{n-1}} M(a_1,\dots,a_m, u_1,\dots,u_{n-1}, b)$ holds in S. By assumption, it also holds in any subfield of S containing b; i.e., for any T such that $R(b)\leq T\leq S$.

Let T_0 be the real closure of $R(b)$. $T_0\leq S$ so that (**) holds in T_0, and hence in all extensions of T_0. Now a set of axioms for T_0 is

$$P \cup \Delta_R \cup T$$

where Δ_R is the diagram of R and T is the set of all sentences of the form $a<b$ or $b<a$, with a in R, which are true in S. Since (**) holds in all models satisfying these axioms,

$$P\cup\Delta_R\cup T \vdash \bigvee_{u_1\cdots u_n} M(a_1,\dots,a_m, u_1,\dots,u_n).$$

But then,

$$P \cup \Delta_R \vdash \Theta(b) \to \bigvee_{u_1 \cdots u_n} M(a_1, \ldots, a_m, u_1, \ldots, u_n),$$

where $\Theta(b)$ is the conjunction of a finite number of inequalities $a<b$ and $b<a$ from Γ. Then

$$P \cup \Delta_R \vdash \bigvee_y \Theta(y) \to \bigvee_{u_1 \cdots u_n} M(a_1, \ldots, a_m, u_1, \ldots, u_n).$$

But $\Delta_R \vdash \bigvee_y \Theta(y)$, for suppose $\Theta(b)$: $a_1 < \ldots < a_t < b < a_1' < \ldots < a_j'$. If $t=0$, take $y = a_1' - 1$; if $j=0$, take $y = a_t + 1$; otherwise take $y = \frac{1}{2}(a_t + a_1')$. Thus we have shown that

$$P \cup \Delta_R \vdash \bigvee_{u_1 \cdots u_n} M(a_1, \ldots, a_m, u_1, \ldots, u_n),$$

so that P is model-complete.

That P is complete follows from the fact that any real closed field contains a prime field isomorphic to the real algebraic field.

Now consider the set P' of axioms for a real closed field without the notion of $<$. P' is still model complete since we may define

$$x < y \leftrightarrow \bigvee_z (x = y + z^2 \wedge z \neq 0)$$

and since

$$\neg x < y \leftrightarrow x = y \vee y < x.$$

That is, since P is model-complete, every formula is equivalent to an existential formula; in P', every occurrence of $<$ may be replaced by its definition, and since both the definition and its negation are existential, the resulting formula is still existential. Hence P' is still model-complete. (Note the relation of this result to the preceeding problem.)

<u>Problem</u>. Show that the theory of algebraically closed fields is model complete. Note that this theory is not complete unless the characteristic is specified.

Since P' is model-complete, any formula is equivalent to an existential formula

$$\Phi(x_1,\dots,x_n) \leftrightarrow \bigvee_{y_1\cdots y_k} \sigma(x_1,\dots,x_n,y_1,\dots,y_k),$$

where σ is a boolean combination of equations. Noting that

$$\alpha=0 \vee \beta=0 \leftrightarrow \alpha\cdot\beta=0$$
$$\alpha=0 \wedge \beta=0 \leftrightarrow \alpha^2+\beta^2=0$$
$$\alpha\neq 0 \leftrightarrow \bigvee_{y} \alpha y=1,$$

we see that σ may be transformed into a polynomial P so that $\Phi(x_1,\dots,x_n) \leftrightarrow \bigvee_{y_1,\dots,y_k,\dots,y_\ell} P(x_1,\dots,x_n,y_1,\dots,y_k,\dots,y_\ell)$.

In an algebraically closed field we cannot do as well since there $\alpha=0 \wedge \beta=0 \leftrightarrow \bigwedge_{u,v} \alpha u=\beta v$. Hence the polynomial may be preceeded by a mixture of both types of quantifiers.

Robinson's method produces a decision procedure for real closed fields; namely, start listing all theorems of the theory until a given sentence or its negation appears. Tarski's method, however, gives more insight into the theory as it uses less logical apparatus. His result may be summarized as:

> Let P be the set of axioms for [redacted] real closed fields with symbols 0, 1, +, ·, >. Then every formula $\Phi(x_1,\dots,x_n)$ is P-equivalent to a formula Ψ with no more free variables and no bound variables.

This is a stronger result than Robinson's, for now a decision procedure will consist of "checking" a finite number of equations in the reduced formula. In such a manner, many unsolved problems in the theory of real closed fields may be attacked by using computers to perform the reduction. Still, the length of formulas and number of different cases soon becomes prohibitive for even problems of moderate complexity.

R. M. Robinson has solved one problem using model-theoretic techniques. Consider the problem of placing n points on a sphere so the minimum distance between any two is a maximum. For $n=2$, the points are the ends of a diameter; $n=3$, the vertices of an equilateral triangle; $n=4$, the vertices of a tetrahedron. The proper placement is known for $n \leq 9$ and $n=24$, the latter case having been solved by R.M. Robinson.

Another application of Tarski's method concerns the definability of sets of real numbers. If $\phi(x)$ is a formula with one free variable, then the reduced formula ψ is a boolean combination of formulas of the types $\alpha=\beta$ and $\alpha<\beta$, where α and β are polynomials in x. Hence the set defined by $\phi(x)$ is a finite union of intervals with algebraic endpoints. In particular, the set of natural numbers is not definable. (It is possible, however, to define the set of natural numbers in the rational field. The proof of this fact is difficult.)

Rings of polynomials over fields

One method of demonstrating the incompleteness of a structure with the operations $+$ and $\cdot$ is to show that the set of natural numbers may be defined in the structure. (c.f., R. M. Robinson, Transactions, 1951). We shall demonstrate this method by proving the incompleteness of rings of polynomials in one unknown over a field $\mathfrak{F} = \langle F, 0, 1, +, \cdot \rangle$ of characteristic 0. The generalization to more unknowns is trivial.

We define $x|y \leftrightarrow \bigvee_z x \cdot z = y$.

$$x \in F \leftrightarrow x|1 \vee x=0,$$

where 1 is the unit element of the ring. I.e., the field elements are the polynomials of degree 0. We claim

$$\mathrm{Nat}\, x \leftrightarrow \bigvee_{u,v} [u \notin F \wedge v \neq 0 \wedge u|v \wedge \bigwedge_{w} (w \in F \wedge u+w|v \rightarrow u+w+1|v \vee w=x)].$$

This assertion is justified as follows: Suppose x is a natural number and let $u = \alpha$, $v = \alpha \cdot (\alpha+1) \cdots (\alpha+x)$, where α is the transcendental element of the ring. Then u and v satisfy the formula in [ ]. Note that we don't have to define α; all we need to know is that it exists. Conversely, suppose such a u and v exist. Then $u|v$, $u+1|v$, $u+2|v, \ldots$, so that if x were not a natural number, v would have infinately many non-unit divisors. But this is impossible, and hence x must be a natural number.

Consistency and Definability

Consistency Lemma (A. Robinson)

Let $\mathcal{L}$ and $\mathcal{L}'$ be predicate logics with $\mathcal{L} \subseteq \mathcal{L}'$. Suppose that Γ is a set of sentences which is complete in $\mathcal{L}$, Γ_1 and Γ_2 are consistent sets of sentences of $\mathcal{L}'$ such that $\Gamma \subseteq \Gamma_1 \cup \Gamma_2$, and that the relation symbols and constants of Γ_1 and Γ_2 are in $\mathcal{L}$. Then $\Gamma_1 \cup \Gamma_2$ is consistent.

Before proceeding to the proof, we illustrate the depth of the lemma. Consider a language $\mathcal{L}$ with $0, 1, +, \cdot$, and a language $\mathcal{L}'$ with the additional unary relations Nat and Nat'. Let Γ be a complete set of axioms for real closed fields; Γ_1 the true sentences of the real field with the unary relation Nat $x \leftrightarrow x$ is a natural number; and Γ_2 the true sentences of the real algebraic numbers with the relation Nat'$x \leftrightarrow x$ is a natural number.

Since computable functions are definable, the extension of

$$\varphi_{Nat}(p,q,r,s) \leftrightarrow \text{Nat } p \wedge \text{Nat } q \wedge \text{Nat } r \wedge \text{Nat } s \wedge \frac{p}{q} < e < \frac{r}{s},$$

where $e = 2.718\ldots$, is definable. Similarly, $\varphi_{Nat'}$ is definable. Hence the Dedekind cut determining e is definable in terms of both Γ_1 and Γ_2.

Since e is in the domain of a model for Γ_1, we have

$$(*) \quad \bigvee_x \bigwedge_{p,q,r,s} \left(\varphi_{Nat}(p,q,r,s) \rightarrow \frac{p}{q} < x < \frac{r}{s} \right).$$

But in a model for Γ_2,

$$(**) \quad \neg \bigvee_x \bigwedge_{p,q,r,s} \left(\varphi_{Nat'}(p,q,r,s) \rightarrow \frac{p}{q} < x < \frac{r}{s} \right).$$

Hence for a model of $T_1 \cup T_2$ to exist, Nat and Nat' must have different interpretations in that model. Since (*) holds in this model while the negation of (**) does not, Nat' must be a larger set than Nat. I.e., Nat' must define a non-standard model of arithmetic.

In our proof we shall employ the Henkin Inconsistency Lemma (to appear, JSL). This lemma is actually a strong form of the completeness theorem (take $\Gamma = \Delta$ below to derive the completeness theorem), and indeed the proof is basically the same.

<u>Definition.</u> The <u>vocabulary</u> $W(\Gamma)$ of a set Γ of sentences consists of all relation, constant, and operation symbols occurring in Γ.

<u>Inconsistency</u> <u>Lemma</u> (Henkin)

Let Γ and Δ be sets of sentences. If $\Gamma \cup \Delta$ has no model, then there exists a sentence θ such that $W(\theta) \subseteq (W(\Gamma) \cap W(\Delta)) \cup \{T, F\}$, $\Gamma \vdash \theta$, and $\Delta \vdash \neg\theta$.

<u>Proof</u>: We shall prove the lemma for predicate logics without equality and operations. The extension to general predicate logics is the same as before.

Let ν be the cardinality of $W(\Gamma) \cup W(\Delta)$. We adjoin ν additional constants to $W(\Gamma)$ to form a language $\mathcal{L}_1$ and the same ν constants to $W(\Delta)$ to form a language $\mathcal{L}_2$. Well-order the constants by $\{c_\mu\}_{\mu<\nu}$ and the sentences which occur in $\mathcal{L}_1$ or $\mathcal{L}_2$ by $\{\varphi_\mu\}_{\mu<\nu}$.

Suppose T_i is a set of sentences, $i=1,2$. We say that T_1 and T_2 are <u>locally</u> <u>consistent</u> iff there is no sentence Θ, $W(\Theta) \subseteq W(T_1) \cup W(T_2)$, for which $T_1 \vdash \Theta$ and $T_2 \vdash \neg\Theta$.

<u>Lemma</u>. If T_1 and T_2 are locally consistent considered as sentences of $W(T_1)$ and $W(T_2)$, then they are locally consistent when considered as sentences of $\mathcal{L}_1$ and $\mathcal{L}_2$.

<u>Proof</u>: Suppose T_1 and T_2 are not locally consistent in $\mathcal{L}_1$ and $\mathcal{L}_2$. Then for some Θ in $\mathcal{L}_1 \cap \mathcal{L}_2$,

$$T_1 \vdash \Theta(c_1 \dots c_n)$$
$$T_2 \vdash \neg\Theta(c_1 \dots c_n).$$

Since $c_1 \dots c_n$ do not occur in T_1 or T_2,

$$T_1 \vdash \bigwedge_{x_1 \dots x_n} \Theta(x_1 \dots x_n)$$
$$T_2 \vdash \bigvee_{x_1 \dots x_n} \neg\Theta(x_1 \dots x_n)$$

or

$$T_2 \vdash \neg \bigwedge_{x_1 \dots x_n} \Theta(x_1 \dots x_n),$$

which contradicts the local consistency of T_1 and T_2.

To complete the proof of the lemma, we suppose that T and Δ are locally consistent and produce a model for $T \cup \Delta$. We define

$T_0 = T$

$T_{\mu+1} = T_\mu \cup \{\varphi_\mu, [\varphi(c)]\}$ if $\varphi_\mu \in \mathcal{L}_1$ and T_μ, φ_μ and Δ_μ are locally consistent. $\varphi(c)$ is added if $\varphi_\mu = \bigvee_\alpha \varphi(\alpha)$, where c is the first constant not in T_μ, Δ_μ, or $\varphi(\alpha)$

$T_{\mu+1} = T_\mu$ otherwise

$T_\lambda = \bigcup_{\mu<\lambda} T_\mu$ if λ is a limit ordinal

Similarly,

$\Delta_0 = \Delta$

$\Delta_{\mu+1} = \Delta_\mu \cup \{\Phi_\mu, [\Phi(c)]\}$ if $\Phi_\mu \in \mathcal{L}_2$ and $\Gamma_{\mu+1}$ and Δ_μ, Φ_μ are locally consistent. $\Phi(c)$ is added if $\Phi_\mu = \bigvee_\alpha \Phi(\alpha)$, where c is the first constant not in $\Gamma_{\mu+1}$, Δ_μ, or $\Phi(\alpha)$

$\Delta_{\mu+1} = \Delta_\mu$ otherwise

$\Delta_\lambda = \bigcup_{\mu<\lambda} \Delta_\mu$ if λ is a limit ordinal

Now let $\Gamma' = \Gamma_\nu$ and $\Delta' = \Delta_\nu$.

I. Γ' and Δ' are locally consistent.

By the following lemma and arguments used before, if Γ_μ and Δ_μ are locally consistent, then so are $\Gamma_{\mu+1}$ and $\Delta_{\mu+1}$.

<u>Lemma.</u> If $\Gamma, \bigvee_\alpha \Phi(\alpha)$ and Δ are locally consistent, then so are $\Gamma, \bigvee_\alpha \Phi(\alpha), \Phi(c)$ and Δ, where c is a constant which does not occur in Γ, Δ, or $\Phi(\alpha)$.

<u>Proof</u>: Suppose the lemma is false. Then there is a sentences $\Theta(c)$ for which

$$\Gamma, \bigvee_\alpha \Phi(\alpha) \vdash \Phi(c) \to \Theta(c) \quad \text{and}$$
$$\Delta \vdash \neg\Theta(c).$$

Then,

$$\Gamma, \bigvee_\alpha \Phi(\alpha) \vdash \bigwedge_\alpha (\Phi(\alpha) \to \Theta(\alpha))$$
$$\Gamma, \bigvee_\alpha \Phi(\alpha) \vdash \bigvee_\alpha \Phi(\alpha) \to \bigvee_\alpha \Theta(\alpha)$$
$$\Gamma, \bigvee_\alpha \Phi(\alpha) \vdash \bigvee_\alpha \Theta(\alpha).$$

But,

$$\Delta \vdash \bigwedge_\alpha \neg\Theta(\alpha)$$
$$\text{or } \Delta \vdash \neg\bigvee_\alpha \Theta(\alpha),$$

which is a contradiction.

II. If $\sigma \in \mathcal{L}_1$, then either $\sigma \in \Gamma'$ or $\neg\sigma \in \Gamma'$.
If $\sigma \in \mathcal{L}_2$, then either $\sigma \in \Delta'$ or $\neg\sigma \in \Delta'$.

<u>Proof</u>: If both $\sigma \notin \Gamma'$ and $\neg\sigma \notin \Gamma'$, then σ, Γ', and Δ' are locally inconsistent as are $\neg\sigma$, Γ', and Δ'. Hence

$$\Gamma', \sigma \vdash \theta_1 \quad \text{and} \quad \Delta' \vdash \neg\theta_1$$

$$\Gamma', \neg\sigma \vdash \theta_2 \quad \text{and} \quad \Delta' \vdash \neg\theta_2.$$

Furthermore,

$$\Gamma' \vdash \sigma \rightarrow \theta_1 \quad \text{and} \quad \Gamma' \vdash \neg\sigma \rightarrow \theta_2$$

Therefore

$$\Gamma' \vdash \theta_1 \vee \theta_2$$

But $\Delta' \vdash \neg(\theta_1 \vee \theta_2)$, which contradicts the local consistency of Γ' and Δ'.

III. If $\bigvee_\alpha \phi(\alpha) \in \Gamma'$, then $\phi(c) \in \Gamma'$ for some c. Similarly for Δ', both results following by construction.

We now define a valuation on the sentences of $\mathcal{L}_1 \cup \mathcal{L}_2$. For atomic sentences ϕ, let

$$v(\phi) = T \quad \text{if} \quad \phi \in \Gamma' \cup \Delta'$$

$$v(\phi) = F \quad \text{if} \quad \neg\phi \in \Gamma' \cup \Delta'$$

$$v(\phi) \quad \text{arbitrary otherwise.}$$

The valuation is extended to all sentences in the normal fashion.

Let $\mathcal{M}$ be the model having as domain the constants of $\mathcal{L}_1 \cup \mathcal{L}_2$. For $\phi \in \mathcal{L}_1$, $v(\phi) = T$ iff $\phi \in \Gamma'$, as in the proof of the completeness theorem. Hence $\mathcal{M}$ is a model for T. Similarly, for $\phi \in \mathcal{L}_2$, $v(\phi) = T$ iff $\phi \in \Delta'$, and $\mathcal{M}$ is a model for Δ. This completes the proof of the lemma.

Henkin actually stated this result in terms of the following notions of Gentzen derivability:

<u>Definition</u> $\Gamma \underset{\text{(Gentzen)}}{\models} \Delta$ iff every model of Γ satisfies some sentence of Δ.

$\Gamma \underset{\text{Gentzen}}{\vdash} \Delta$ iff there exist sentences $\delta_0, \dots, \delta_k$ in Δ such that $\Gamma \vdash \delta_0 \vee \dots \vee \delta_k$.

<u>Henkins Theorem</u>. If $\Gamma \models \Delta$, then there exists a sentence Θ such that $W(\Theta) \subseteq W(\Gamma) \cap W(\Delta)$ and for which $\Gamma \vdash \Theta$ and $\Theta \underset{\text{Gentzen}}{\vdash} \Delta$.

<u>Proof</u>: If $\Gamma \models \Delta$, then Γ and $\operatorname{Neg} \Delta$ have no common model. By the Inconsistency Lemma, there exists a sentence Θ with $W(\Theta) \subseteq W(\Gamma) \cap W(\Delta)$ such that $\Gamma \vdash \Theta$ and $\operatorname{Neg} \Delta \vdash \neg \Theta$. $\vdash \neg \delta_1 \wedge \dots \wedge \neg \delta_k \rightarrow \neg \Theta$ or $\vdash \Theta \rightarrow \delta_1 \vee \dots \vee \delta_k$. Thus $\Theta \underset{\text{Gentzen}}{\vdash} \Delta$.

The theorem is equivalent to the Inconsistency Lemma, for suppose Γ and Δ have no common model. Then $\Gamma \models \operatorname{Neg} \Delta$, and there exists a sentence Θ for which $\Gamma \vdash \Theta$ and $\Theta \underset{\text{Gentzen}}{\vdash} \operatorname{Neg} \Delta$. $\vdash \Theta \rightarrow \neg \delta_1 \vee \dots \vee \neg \delta_k$ or $\Delta \vdash \neg \Theta$.

Note also that by the Completeness Theorem, $\Gamma \models \Delta$ iff $\Gamma \underset{\text{Gentzen}}{\vdash} \Delta$. If $\Gamma \models \Delta$, then Γ and $\operatorname{Neg} \Delta$ have no common model, or $\Gamma \cup \operatorname{Neg} \Delta$ is not consistent. Hence $\Gamma \cup \operatorname{Neg} \Delta \vdash \delta_0$ and $\Gamma \vdash \neg \delta_1 \wedge \dots \wedge \neg \delta_k \rightarrow \delta_0$ or $\Gamma \vdash \delta_0 \vee \delta_1 \vee \dots \vee \delta_k$. Thus $\Gamma \underset{\text{Gentzen}}{\vdash} \Delta$. The converse is obvious.

The Consistency Lemma of A. Robinson now follows as a corollary of the Inconsistency Lemma:

<u>Consistency Lemma.</u> Suppose that Γ_1 and Γ_2 are consistent sets of sentences and that $\Gamma_1 \cap \Gamma_2$ is complete relative to $W(\Gamma_1) \cap W(\Gamma_2)$. Then $\Gamma_1 \cup \Gamma_2$ is consistent.

<u>Proof</u>: If Γ_1 and Γ_2 have no common model, then there is a sentence θ with $W(\theta) \subseteq W(\Gamma_1) \cap W(\Gamma_2)$ such that $\Gamma_1 \vdash \theta$ and $\Gamma_2 \vdash \neg\theta$. But this contradicts the hypotheses that $\Gamma_1 \cap \Gamma_2$ is complete and that both Γ_1 and Γ_2 are consistent.

As another corollary we have:

<u>Craig's Lemma.</u> If $\vdash \phi \to \psi$, then there exists a sentence θ with $W(\theta) \subseteq W(\phi) \cap W(\psi)$ such that $\vdash \phi \to \theta$ and $\vdash \theta \to \psi$.

<u>Proof</u>: Suppose $\vdash \phi \to \psi$. Then $\{\phi\}$ and $\{\neg\psi\}$ have no common model, so that there is a θ such that $\phi \vdash \theta$ and $\neg\psi \vdash \neg\theta$. I.e., $\vdash \phi \to \theta$ and $\vdash \theta \to \psi$.

Craig's Lemma may be proved also for formulas as follows: Let $x_1 \ldots x_n$ be the free variables occurring in the formula $\phi \to \psi$, and suppose $\phi \to \psi$. Choose constants $c_1 \ldots c_n$ not occurring in $\phi \to \psi$, increasing the language if necessary. By Craig's Lemma as above, there exists a sentence θ with $W(\theta) \subseteq W(\phi(c_1 \ldots c_n)) \cap W(\psi(c_1 \ldots c_n))$ such that $\vdash \phi(c_1 \ldots c_n) \to \theta$ and $\vdash \theta \to \psi(c_1 \ldots c_n)$. By generalization, $\vdash \phi \to \theta(x_1 \ldots x_n)$ and $\vdash \theta(x_1 \ldots x_n) \to \psi$.

<u>Definition.</u> Let $\mathcal{L}$ be a predicate logic with equality and relation symbols $R, R_1, \ldots$, and let Γ be a consistent set of sentences of $\mathcal{L}$. R is <u>defined implicitly</u> in terms of $R_1, \ldots$ iff for every domain A and relations $T_1, \ldots$ on A there is at most one model $\langle A, T, T_1, \ldots \rangle$ of Γ.

Implicit definability may also be defined syntactically as well as semantically, as in the following theorem. In the subsequent discussion, Δ will be the set of sentences obtained from those of Γ by replacing each occurrence of R by a new relation symbol S (not in $\mathcal{L}$), and $\mathcal{L}'$ will be the language so expanded.

<u>Theorem.</u> R is defined implicitly in terms of $R_1, \ldots$ with respect to Γ iff $\Gamma \cup \Delta \vdash \bigwedge_{x_1 \cdots x_n} (Rx_1 \ldots x_n \leftrightarrow Sx_1 \ldots x_n)$.

<u>Proof:</u> Obvious application of Completeness Theorem.

<u>Definition.</u> Let R be a relation symbol of rank n. R is <u>defined explicitly</u> by a formula ϕ with respect to Γ in terms of $R_1, \ldots$ iff $R \notin W(\phi)$, ϕ has at most the free variables $x_1, \ldots, x_n$, and $\Gamma \vdash \bigwedge_{x_1 \cdots x_n} (Rx_1 \ldots x_n \leftrightarrow \phi)$.

<u>Beth's Theorem.</u> If R is defined implicitly w.r.t. Γ in terms of $R_1, \ldots$, then there exists a formula ϕ such that R is defined explicitly by ϕ w.r.t. Γ in terms of $R_1, \ldots$.

<u>Proof</u>: By hypothesis, $T \cup \Delta \vdash Rx_1 \dots x_n \leftrightarrow Sx_1 \dots x_n$. Let γ and δ be conjunctions of sentences of T and Δ respectively such that

$$\vdash \gamma \wedge \delta \rightarrow (Rx_1 \dots x_n \leftrightarrow Sx_1 \dots x_n).$$

$$\vdash \gamma \wedge Rx_1 \dots x_n \rightarrow (\delta \rightarrow Sx_1 \dots x_n)$$

By Craig's Lemma, there exists a formula θ with free variables at most $x_1 \dots x_n$ such that

$$\vdash \gamma \wedge Rx_1 \dots x_n \rightarrow \theta$$

$$\vdash \theta \rightarrow (\delta \rightarrow Sx_1 \dots x_n)$$

and such that $W(\theta) \subseteq \{=, R_1, \dots\}$. I.e., neither R or S occur in θ. Hence,

$$T \vdash Rx_1 \dots x_n \rightarrow \theta$$

$$\Delta \vdash \theta \rightarrow Sx_1 \dots x_n,$$

and in the proof of the latter deduction we may replace all occurrences of S by occurrences of R to obtain

$$T \vdash \theta \rightarrow Rx_1 \dots x_n.$$

Thus $T \vdash \theta \leftrightarrow Rx_1 \dots x_n$.

A curious observation with regard to Beth's Theorem is that despite it's apparent strength, it has very few applications. One reason is that it is difficult to apply. For instance, in number theory, the ~~function~~ relation $Rxy \leftrightarrow y = 2^x$ is recursively definable by

$$R01 \wedge Rxy \rightarrow R(x+1, y+y).$$

Yet it is not clear that the definition is implicit due to the existence of non-standard models. (R is in fact implicitly definable since Gödel has shown all primitive recursive functions to be explicitly definable.)

The main application of Beth's Theorem occurs in proofs of non-definability, as will be demonstrated later. What the theorem really tells us is that "Padua's method" always works; i.e., if a relation is not explicity definable w.r.t. a set Γ of sentences, then it is possible to find two models for Γ differing only in the interpretation of that relation.

For example, let $\mathcal{R} = \langle$ Real numbers, $0, 1, +, \cdot, F \rangle$, where F denotes the algebraic numbers, and let $\Gamma = \mathcal{T}h\,\mathcal{R}$. Padua's method shows that F cannot be defined in terms of + and $\cdot$ w.r.t. Γ since $\bigvee_x \neg F(x)$ holds in the real closed field but not in the real algebraic field.

Definability in Arithmetic

1. + in terms of S and $\cdot$ w.r.t. $\mathcal{T}h \langle$Pos. Int., $S, +, \cdot \rangle$

$$x + y = z \leftrightarrow S(x \cdot z) \cdot S(y \cdot z) = S(z \cdot z \cdot S(x \cdot y))$$

2. + is not definable in terms of $\cdot$ alone since there is an automorphism of the integers which leaves $\cdot$ but not + fixed. (This is an example of Padua's ~~model~~ method, for the automorphism creates a new model differing from the old only in the interpretation of +). The particular automorphism is obtained by interchanging 2 and 3 in the multiplicative structure:

n	0	1	2	3	4	5	6	7	8	9	10	...
T(n)	0	1	3	2	9	5	6	7	27	4	15	...

Obviously $x \odot y = T(T^{-1}x \cdot T^{-1}y) = x \cdot y$, but $x \oplus y \neq x + y$.

3. S can be defined in terms of < (obvious), but the converse situation does not hold. Intuitively, S determines only the local behavior of <; i.e., consider the non-standard model of $\mathcal{T}h \langle$Nat, $S, <, 0 \rangle$:

$$0, 1, 2, 3, \ldots, \quad \ldots, a-1, a, a+1, \ldots, \quad \ldots b-1, b, b+1, \ldots$$

Interchanging a and b leaves S and 0 fixed, but not <. The only difficulty with this application of Padua's method is that we must know that the above is a model, and that the demonstration of this fact may be tedious to formalize.

4. + cannot be defined in terms of 0, 1, S, and <. We shall demonstrate this result not by Padua's method, but by producing a model for $T' = \mathcal{Th}\langle Nat, 0, 1, S, <\rangle$ in which there is no interpretation of +. For the model take

$$0, 1, 2, \ldots ; \ldots, a-1, a, a+1, \ldots$$

In this model there is no element a^* for which $a^* > a$, $a^* > a+1$, ... ; but if + were definable, $a+a$ would be such an element.

Alternatively, we could start with any non-standard model for + and map every non-standard number a into $a+1$, thereby preserving 0, 1, S, and <, but not +.

5. · cannot be defined in terms of 0, 1, S, <, and +. As in 4, consider the model for $\mathcal{Th}\langle Nat, 0, 1, S, <, +\rangle$

$$0, 1, 2, \ldots, \ldots, \ldots, a-1, a, a+1, \ldots, \ldots$$

with all necessary rows filled in. In this model there is no a^* for which $a^* > a$, $a^* > a+a$, ... ; but if · were definable, $a \cdot a$ would be such an element.

<u>Problems</u>

In the domain of natural numbers, give explicit definitions of · in terms of

(a) + and |

(b) + and ⊥, where $x \perp y \leftrightarrow \bigwedge_z (z|x \wedge z|y \rightarrow z=1)$.

Definability in Fields

In a field of characteristic 0 we may define 0, 1, and individual rationals. More generally we have

Theorem. If F is an algebraic field and $\alpha \in F$, then α is arithmetically definable iff α is fixed under all automorphisms of F.
(R.M. Robinson, JSL)

Proof: If the characteristic of F is $p \neq 0$, then $x \to x^p$ is an automorphism of F. The fixed elements satisfy $x^p = x$, whose only solutions are $0, 1, 2, \ldots, p-1$. These elements are trivially definable.

Suppose F has characteristic 0 and is a simple extension of the rationals, $F = R(\theta)$. Let f be the irreducible polynomial with rational coefficients such that $f(\theta) = 0$, and let $\theta_1, \ldots, \theta_k$ be the roots of $f(x) = 0$ which are in F. Automorphisms of F are characterized by $\sigma_i(\theta) = \theta_i$, $i = 1, \ldots, k$. Furthermore, $\alpha = g(\theta)$ for some polynomial g in $R[\theta]$. Then $\sigma_i(\alpha) = \sigma_i g(\theta) = g(\theta_i)$, and since α is fixed under automorphisms, we may define

$$x = \alpha \leftrightarrow \bigvee_y \left(f(y) = 0 \wedge x = g(y) \right)$$

Finally, let F be an arbitrary algebraic field of characteristic 0. Since F is countable, we may write $F = \bigcup F_n$, where

$$F_0 = R(\alpha)$$
$$F_n \subseteq F_{n+1}$$
$$F_n = R(\theta_n).$$

Let σ_n be an isomorphic mapping of F_n onto a subfield of F. Then σ_n is determined by $\sigma_n(\theta_n)$, which in turn must be a root of the irreducible polynomial for θ_n over R. Hence there exists only a finite number of such isomorphisms.

<u>Lemma</u>. Let F be an algebraic field, $\alpha \in F$. If α is fixed under all automorphisms of F, then there exists a subfield $K \le F$ of finite degree over R such that α is fixed under all isomorphisms of K onto a subfield of F.

<u>Proof</u>: If the lemma is false, then for each n there exists an isomorphism of F_n onto a subfield of F such that α is not fixed. Each isomorphism of F_{n+1} onto a subfield of F is an extension of an isomorphism of F_n onto a subfield of F, and at each stage there are only a finite number of isomorphisms. Hence by König's Lemma, there is an isomorphism σ of F onto a subfield F' of F which does not leave α fixed. But we must have $F' = F$, and this contradicts the fact that α is fixed under all automorphisms of F.

Now choose $K = R(\theta)$ where, by the lemma, α is fixed under all isomorphisms of K onto subfields of F. Let $\theta_1, \dots, \theta_k$ be the roots of $f(\theta) = 0$ which are in F, where f is the irreducible polynomial for θ over R. As before, isomorphisms of K into F are determined by $\sigma_i(\theta) = \theta_i$, and $\alpha = g(\theta) = \sigma_i g(\theta) = g(\theta_i)$. Hence

$$x = \alpha \leftrightarrow \bigvee_y (f(y) = 0 \wedge x = g(y)).$$

Note in connection with the preceeding theorem that we define $\sqrt{2}$ in $R(\sqrt[4]{2})$ by

$$x = \sqrt{2} \leftrightarrow \bigvee_{y} (y^4 = 2 \wedge x = y^2).$$

The definition

$$x = \sqrt{2} \leftrightarrow x^2 = 2$$

does not work, since $-\sqrt{2}$ also satisfies the right hand side.

Homomorphic Images of Algebras

For our final result in this section we need a strengthened version of the Inconsistency Lemma. Again the proof is similar to the former, and will only be sketched.

Definition. A formula ϕ is in negation normal form (nnf) iff each negation symbol occurring in ϕ immediately precedes a relation symbol, and the only logical symbols in ϕ are $\neg, \vee, \wedge, \bigvee, \bigwedge, =$.

Definition. An occurrence of a relation symbol in a formula ϕ in nnf is a positive occurrence iff it is not immediately preceded by a negation sign in that occurrence. Otherwise the occurrence is termed negative.

Let Θ be in nnf. Then Θ^* is obtained from Θ by turning all logical symbols (except $\neg$) upside down, and by changing all positive occurrences of relation symbols to negative ones and vice versa. We have

$$\vdash \Theta^* \leftrightarrow \neg\Theta.$$

Let Γ and Δ be sets of sentences in nnf, and define $\mathcal{S}_\Gamma$ to be the set of all sentences φ which are in nnf and such that each relation symbol occurring in φ occurs with the same sign in some sentence of Γ as in φ. Define $\mathcal{S}_\Delta$ similarly. We assume that $T, F \in \mathcal{S}_\Gamma \cap \mathcal{S}_\Delta$.

Theorem. If Γ and Δ have no common model, then there exists a sentence θ in $\mathcal{S}_\Gamma$ such that θ^* is in $\mathcal{S}_\Delta$ and

$$\Gamma \vdash \theta \quad , \qquad \Delta \vdash \theta^*.$$

Proof: First consider the case without equality, constants, or operations. Adjoin ν additional constants $\{c_\mu\}_{\mu<\nu}$, where ν is the cardinality of the symbols in $\Gamma \cup \Delta$. Let $\mathcal{S}'_\Gamma$ be the set of all sentences in the expanded language in nnf with the same signed relations as in Γ. Define $\mathcal{S}'_\Delta$ similarly. Well order $\mathcal{S}'_\Gamma \cup \mathcal{S}'_\Delta$ by $\{\varphi_\mu\}_{\mu<\nu}$.

If Σ_1, Σ_2 are sets of sentences in nnf, Σ_1 and Σ_2 are locally consistent iff there does not exist a sentence $\theta \in \mathcal{S}'_{\Sigma_1}$ such that $\theta^* \in \mathcal{S}'_{\Sigma_2}$ and $\Sigma_1 \vdash \theta$, $\Sigma_2 \vdash \theta^*$.

The sets Γ_μ, Δ_μ for $\mu \le \nu$ are defined exactly as in the proof of the Inconsistency Lemma, this time using the new notion of locally consistent. Let $\Gamma' = \Gamma_\nu$ and $\Delta' = \Delta_\nu$. As before, we have

I. If $\varphi \in \mathcal{S}'_\Gamma$ and $\Gamma \vdash \varphi$, then $\varphi \in \Gamma'$. Similarly for $\varphi \in \mathcal{S}'_\Delta$.

II. If $\bigvee_\alpha \varphi(\alpha) \in \Gamma'$, then $\varphi(c) \in \Gamma'$ for some c.

III. Γ' and Δ' are locally consistent.

IV. If $\varphi \in \mathcal{S}'_\Gamma - \Gamma'$, then Γ', φ and Δ' are not locally consistent.

We now take the set $\{c_\alpha\}_{\alpha<\nu}$ as ~~domain~~ the domain of a model $\mathfrak{M}$, and define a valuation v as follows: For atomic formulas,

$v(\phi) = T$ iff $\phi \in \Delta' \cup \Gamma'$

$v(\phi) = F$ if $\neg\phi \in \Delta' \cup \Gamma'$

$v(\phi) = F$ otherwise (assignment arbitrary).

The valuation is extended in the usual manner.

<u>Lemma</u>. $v(\phi) = T$ for all $\phi \in \Gamma' \cup \Delta'$.

<u>Proof</u>: Routinely by induction on the length of ϕ.

Hence $\mathfrak{M}$ is a model for $\Gamma \cup \Delta$, and the theorem is proved.

~~The result of the theorem may be strengthened to include operations and constants by expanding the language to include terms, and taking the set of all terms as the domain of the model. The case of equality is more involved since the axioms for = contain both positive and negative occurrences of =.~~

<u>Craig's Lemma</u>. If ϕ and ψ are in nnf and $\vdash \phi \to \psi$, then there exists a θ in nnf such that each relation in θ occurs with the same sign in both ϕ and ψ as in θ (or $\theta = T$ or F), and

$\vdash \phi \to \theta$

$\vdash \theta \to \psi$.

<u>Proof</u>: Apply the strengthened Inconsistency Lemma to $\Gamma = \{\phi\}$ and $\Delta = \{\psi^*\}$.

Notes on Henkin's Theorem

We first proved the Inconsistency Lemma and Craig's Lemma for systems with no distinction with respect to the signs of relations. Equality was introduced through equivalence classes. This method requires us to consider the relation '=' as occurring in both the sets Γ and Δ of the theorem, for '=' may have to appear in the interpolating formula even though it does not occur explicitly in both sets. E.g., consider applying Craig's Lemma to

$$\vdash (\bigvee_x Rx \wedge \bigvee_x \neg Rx) \rightarrow \bigvee_{x,y} x \neq y.$$

Operations and constants were then introduced as relations by using additional axioms involving equality.

The stronger theorem for signed relations does not apply in its strong form to languages with operations. For suppose + occurs in Γ and $\cdot$ only in Δ. In the proof of the lemma we would want to show that the model constructed is a model for Γ, or that for all $\phi \in \mathcal{L}_{\Gamma'}$ (the language constructed from all terms and positive relations in Γ'), $v(\phi) = T \Leftrightarrow \phi \in \Gamma'$. In particular, we need $\bigwedge_\alpha \phi(\alpha) \in \Gamma \Rightarrow v(\bigwedge_\alpha \phi(\alpha)) = T$. But our inductive hypothesis only allows us to conclude that $v(\phi(c)) = T$ for all terms c of the language of Γ (e.g., $v(\phi(a+b)) = T$; the value $v(\phi(c \cdot d))$ is undetermined, and hence we cannot conclude that $v(\bigwedge_\alpha \phi(\alpha)) = T$.

Thus, in applying the strong form of the inconsistency lemma, we may not place any restrictions on the occurrence of operation symbols.

<u>Definition.</u> A set Γ of sentences of a p.l. $\mathcal{L}$ is <u>increasing</u> in a set $\mathcal{S}$ of relation symbols iff for any model $\mathfrak{M}$ of Γ, whenever we replace each of the relations of $\mathcal{S}$ by larger relations to obtain a structure $\mathfrak{M}'$, then also $\mathfrak{M}' \in \mathrm{Mod}\,\Gamma$.

For each $R \in \mathcal{S}$ we associate a new symbol R' not in $\mathcal{L}$. Let

$$c(R, R') \leftrightarrow \bigwedge_{x_1 \cdots x_n} (R x_1 \cdots x_n \rightarrow R' x_1 \cdots x_n),$$

and let I be the set of all such sentences $c(R, R')$ for all $R \in \mathcal{S}$. Finally let Γ' be the set of sentences obtained by replacing R by R' throughout Γ. Then Γ is increasing in $\mathcal{S}$ iff every model of $\Gamma \cup I$ is also a model of Γ'; i.e., iff $\Gamma \cup I \vdash \Gamma'$.

<u>Theorem.</u> If Γ is a set of sentences in nnf and all relations in a set $\mathcal{S}$ occur only positively in Γ, then Γ is increasing.

<u>Proof</u>: By induction on the length of formulas $\gamma \in \Gamma$.

Let $I, \mathcal{L}$ and $\mathcal{S}$ be as before, and let $\mathcal{S}'$ be the set of all R' for $R \in \mathcal{S}$. Let Σ, Γ, and Δ be sets of sentences of $\mathcal{L}$, and define Σ', Γ', and Δ' by replacing all relations symbols of $\mathcal{S}$ by the corresponding symbols of $\mathcal{S}'$. Then we have the following interpolation theorem:

<u>Theorem.</u> If $\Sigma, \Sigma', \Gamma, I \vdash \Delta'$, then there exists a set Π of sentences π in nnf which are positive in all the relation symbols of $\mathcal{S}$ and not containing any symbols of $\mathcal{S}'$ such that

$$\Sigma, \Gamma \vdash \Pi$$
$$\Sigma, \Pi \vdash \Delta.$$

<u>Proof</u>: Suppose first that $\Delta = \{\delta\}$. Then by hypothesis there exist conjunctions σ, σ', γ, and ι_0 of sentences of Σ, Σ', Γ, and I respectively such that

$$\vdash \sigma \wedge \sigma' \wedge \gamma \wedge \iota_0 \to \delta'.$$

Or

$$\vdash \sigma \wedge \gamma \to (\iota_0 \wedge \sigma' \to \delta').$$

Now no relations in $\mathcal{S}'$ occur in $\sigma \wedge \gamma$, and those in $\mathcal{S}$ occur positively in $\iota_0 \wedge \sigma' \to \delta'$. Hence by Craig's Lemma, there exists a sentence π in nnf such that π contains no relations of $\mathcal{S}'$ and all relations of $\mathcal{S}$ occur positively in π, and for which

$$\vdash \sigma \wedge \gamma \to \pi$$
$$\vdash \pi \to (\iota_0 \wedge \sigma' \to \delta').$$

Let $\hat{\iota}$ be obtained from ι by replacing R' by R. Then

$$\vdash \pi \to (\hat{\iota}_0 \wedge \sigma \to \delta),$$

as can be seen by modifying the proof of $\pi \to (\iota_0 \wedge \sigma' \to \delta')$. But $\hat{\iota}_0$ is a theorem of logic, so that $\Sigma, \Gamma \vdash \pi$ and $\Sigma, \pi \vdash \delta$.

Finally, let Π be the set of all such π defined in this manner for all $\delta \in \Delta$. Then

$$\Sigma, \Gamma \vdash \Pi \quad \text{and} \quad \Sigma, \Pi \vdash \Delta.$$

<u>Corollary</u>. Γ is increasing iff there exists a set Π of sentences in nnf such that $\Gamma \vdash \Pi$ and $\Pi \vdash \Gamma$.

An *algebraic* system is one in which there are operations and equality, but no relations. Homomorphic images are obtained by mappings similar to residue classes in number theory. Regarding these systems, we have the following theorem due to R. C. Lyndon (*Bulletin*, 1959).

Theorem. Suppose Φ and Ψ are sentences containing no relations other than $=$ such that whenever Φ holds in an algebraic system $\mathfrak{A}$, then Φ holds in any homomorphic image of $\mathfrak{A}$. Then there exists a positive sentence π such that

$$\vdash_{=} \Phi \rightarrow \pi \qquad \text{and} \qquad \vdash_{=} \pi \rightarrow \Psi.$$

Proof: Let $\gamma(\equiv)$ be the conjunction of the conditions expressing the facts that $\equiv$ is an equivalence relation preserving the operations of $\mathfrak{A}$. E.g., if $\mathfrak{A}$ is a system of number theory,

$$\begin{aligned}\gamma(\equiv) \leftrightarrow\ & \bigwedge_x (x \equiv x) \wedge \bigwedge_{x,y} (x \equiv y \rightarrow y \equiv x) \\ & \wedge \bigwedge_{x,y,z} (x \equiv y \wedge y \equiv z \rightarrow x \equiv z) \\ & \wedge \bigwedge_{x,x',y,y'} (x \equiv x' \wedge y \equiv y' \rightarrow x+y \equiv x'+y' \wedge x \cdot y \equiv x' \cdot y')\end{aligned}$$

Then the hypothesis of the theorem may be expressed as

$$\vdash \Phi(\equiv) \wedge \gamma(\equiv) \wedge \gamma(\equiv\!\!\!\equiv) \wedge \iota(\equiv, \equiv\!\!\!\equiv) \rightarrow \Psi(\equiv\!\!\!\equiv),$$

where ι is as before and $\Phi(\equiv)$, $\Psi(\equiv\!\!\!\equiv)$ denote the sentences obtained from Φ and Ψ by making the indicated substitutions for $=$. Rewriting,

$$\vdash \Phi(\equiv) \wedge \gamma(\equiv) \wedge \iota(\equiv, \equiv\!\!\!\equiv) \rightarrow [\gamma(\equiv\!\!\!\equiv) \rightarrow \Psi(\equiv\!\!\!\equiv)].$$

By Craig's Lemma there exists a sentence $\pi(\equiv\!\!\!\equiv)$ containing only the relation $\equiv\!\!\!\equiv$ positively for which

$$\vdash \Phi(\equiv) \wedge \gamma(\equiv) \wedge \iota(\equiv, \equiv\!\!\!\equiv) \rightarrow \pi(\equiv\!\!\!\equiv)$$

$$\vdash \pi(\equiv\!\!\!\equiv) \rightarrow [\gamma(\equiv\!\!\!\equiv) \rightarrow \Psi(\equiv\!\!\!\equiv)].$$

But $\vdash \iota(=, =)$, so that

$$\vdash \Phi(=) \wedge \gamma(=) \rightarrow \pi(=)$$

$$\vdash \pi(=) \rightarrow [\gamma(=) \rightarrow \Psi(=)], \quad \text{or}$$

$$\vdash_{=} \Phi \rightarrow \pi$$

$$\vdash_{=} \pi \rightarrow \Psi.$$

Higher Order Predicate Logics

Finite Axiomatization

We assume as given

(1) a formal language $\mathcal{L}$ (with grammar)

(2) a notion Cn of consequence in $\mathcal{L}$; i.e., a function which correlates with every set of sentences of $\mathcal{L}$ another such set

(3) a mathematical structure.

The problem of finite axiomatizability of the theory of the given structure is the problem of determining whether or not there is a finite set Φ of sentences such that $Cn(\Phi) = \Gamma$, where Γ is the set of all true sentences in the given structure.

Examples: $\mathcal{L}$ may be a first order logic, a set of existential sentences, etc.; Cn may denote derivability, validity, etc.

The RWS Language

We consider a restricted weak second order language for fields with

Logical symbols: $\bigwedge, \bigvee, \wedge, \vee, \neg, =, \in$

Relations and constants: $0, 1, +, \cdot$

Variables: $x, y, z, \ldots$ ranging over elements of the structure

$X, Y, Z, \ldots$ ranging over finite sets of elements of the structure

("Restricted" refers to allowing only set variables and not relational variables; "weak" pertains to the finite restriction.)

Fields finitely axiomatizable in the RWS theory are the fields of rationals, algebraic numbers, real algebraic numbers, and complex numbers. The real field is not finitely axiomatizable. Indeed, Mostowski has shown that no recursive, r.e., arithmetic, or even hyperarithmetic set of axioms exists. At present we demonstrate only the positive results.

In an arbitrary field we may define

$$\mathrm{Nat}\, x \leftrightarrow \bigwedge_T \{[0 \in T \wedge \bigwedge_y (y \in T \rightarrow y+1 \in T \vee y = x)] \rightarrow x \in T\}$$

$$\mathrm{Int}\, x \leftrightarrow \mathrm{Nat}\, x \vee \mathrm{Nat}\, {-x}$$

With these definitions we may axiomatize the RWS theory of the rational field by adding the following axioms to the field axioms:

(1) Characteristic 0 : $\neg \bigvee_T \bigwedge_x (\mathrm{Nat}\, x \rightarrow x \in T)$

(2) All elements rational:

$$\bigwedge_x \bigvee_{y,z} [\mathrm{Nat}\, y \wedge \mathrm{Int}\, z \wedge x \cdot (1+y) = z].$$

Note that this result implies that there can be no satisfactory deductive apparatus for the RWS theory since the true first order sentences of number theory are not recursively enumerable, but are contained in the consequences of the axioms.

Restricting our attention to fields of characteristic 0, we define

$$\mathrm{Alg}\, x \leftrightarrow \bigvee_T \bigvee_y [\mathrm{Nat}\, y \wedge y \neq 0 \wedge y \in T \wedge \bigwedge_z (z \in T \rightarrow \bigvee_w (\mathrm{Int}\, w \wedge x \cdot z + w \in T))]$$

I.e., x is algebraic iff there is a finite set of polynomials in x with integer coefficients with the closure property noted. For this property to hold, either some polynomial must have the value 0, or two polynomials must have the same value.

To characterize algebraic fields we still need a notion of finite sequences (still char. 0):

$$\mathrm{Seq}(U, V, m, n) \leftrightarrow \mathrm{Nat}\, m \wedge \mathrm{Nat}\, n \wedge n \neq 0 \wedge \bigwedge_k [0 < k \leq n \rightarrow \bigvee_u (u \in U \wedge u - km \in V)]$$

$$\mathrm{Seq}(U, V, m, n) \wedge 0 < k \leq n \rightarrow$$
$$k^{th} \text{ term of } (U, V, m, n) = x \leftrightarrow \bigvee_u (x = u - km \wedge u \in U \wedge x \in V),$$

where $\quad x \leq y \leftrightarrow \mathrm{Nat}\, x \wedge \mathrm{Nat}\, y \wedge \bigvee_z (\mathrm{Nat}\, z \wedge x + z = y).$

The justification of this definition is as follows: given a sequence $a_1, \ldots, a_n$, let $V = \{a_1, \ldots, a_n\}$. Choose m a positive integer such that $m > \max_{i,j} |a_i - a_j|$, and let $U = \{a_k + km : 0 < k \leq n\}$. The uniqueness condition follows since if $a_j + jm - km = a_\ell$, then $|a_j - a_\ell| = m|k - j|$, which can hold only if $j = k = \ell$ by the choice of m.

<u>Problems</u> Give a finite set of axioms for the RWS theory of

(1) the field of algebraic numbers
(2) the field of real algebraic numbers
(3) finite extension fields of the rationals.

Note that by the above definitions notations may be simplified by introducing small Greek ~~varia~~ letters as sequences variables and interpreting

$\bigwedge_\alpha$ as $\bigwedge_{U,V,m,n} [\mathrm{Seq}(U, V, m, n) \rightarrow \ldots]$

$\bigvee_\alpha$ as $\bigvee_{U,V,m,n} [\mathrm{Seq}(U, V, m, n) \wedge \ldots]$

$x = \alpha_k \leftrightarrow x = k^{th} \text{ term of } (U, V, m, n).$

Translation back into the formalism is straightforward, even if somewhat tedious, and considerable clarity is gained by the abbreviated notation.

Tarski's WS System

References:

Scott, Tarski, *Notices* (1958)
Büchi, *Logic, Methodology, and Philosophy* (Stanford)
Zeitschrift
(with particular reference to decision problems for WS theories of arithmetic; finite automata)
Mostowski, *Essays on Foundations* (ed. Bar-Hillel)

Logical symbols: $\neg, \wedge, \bigvee, =, I, ^\frown$
Variables: $v_0, v_1, \ldots$
$V_0, V_1, \ldots$
Relation symbols: any number, with correlated ranks

Atomic sequence terms: Iv_j, V_k
Sequence terms: If α and β are sequence terms, then so is $\alpha^\frown\beta$.
Atomic formulas: $v_i = v_j$
$\Pi v_{k_1} \ldots v_{k_n}$, where Π is an n-ary relation
$\alpha = \beta$, where α, β are sequence terms
Formulas: as usual

As seen, the WS language is a weak second order language with sequence variables. We proceed to the definition of satisfaction, using the following metalinguistic abbreviations:

Let A be a non-empty set. Then $A^{(\omega)}$ is the set of all sequences $a_0, a_1, \ldots$ with $a_i \in A$ such that for some k, $a_n = a_k$ for all $n \geq k$. A^* is the set of all finite sequences. If $x \in A^{(\omega)}$ and Nat k, then $x(^k/a)$ is the sequence obtained from x by substituting a in the k^{th} place.

For convenience of notation, we consider structures with one ternary relation. The generalization is obvious.

<u>Definition</u>. (x, X) satisfies a formula φ of $\mathcal{L}$ in the structure $\mathfrak{A} = \langle A, R \rangle$, where A is a non-empty set, if $x \in A^{(\omega)}$, $X \in (A^*)^{(\omega)}$, and one of the following holds:

1. φ is of the form $v_m = v_n$ and $x_m = x_n$
2. φ is of the form $\rho v_m v_n v_p$ and $R x_m x_n x_p$
3. φ is of the form $\alpha = \beta$, where α and β are sequence terms, and the corresponding sequences are the same. I.e., the sequence corresponding to α is obtained by replacing each occurrence of $\mathbb{V}_m$ by X_m and each occurrence of $I v_m$ by $\langle x_m \rangle$.
4. $\varphi = \neg \psi$ and (x, X) does not satisfy ψ
5. $\varphi = \psi \wedge \chi$ and (x, X) satisfies ψ and χ
6. $\varphi = \bigvee v_k \psi$ and for some $a \in A$, $(x(^k/a), X)$ satisfies ψ
7. $\varphi = \bigvee \mathbb{V}_k \psi$ and for some $\alpha \in A^*$, $(x, X(^k/\alpha))$ satisfies ψ.

A sentence σ is <u>true</u> in $\mathfrak{A} = \langle A, R \rangle$ iff every pair (x, X) with $x \in A^{(\omega)}$ and $X \in (A^*)^{(\omega)}$ satisfies σ in $\mathfrak{A}$. (Note that we could have as well said "iff some pair" since σ is a sentence.)

Let $\mathcal{R} = \langle A, R \rangle$ and $\mathcal{S} = \langle B, S \rangle$ be two structures. "$\mathcal{R} \leq \mathcal{S}$" is defined as before. $\mathcal{R}$ and $\mathcal{S}$ are <u>WS-equivalent</u> iff every WS sentence true in $\mathcal{R}$ is true in $\mathcal{S}$ (and conversely). $\mathcal{S}$ is a <u>WS-extension</u> of $\mathcal{R}$ iff $\mathcal{R} \leq \mathcal{S}$ and for every formula ϕ and pair (x, X) with $x \in A^{(\omega)}$ and $X \in (A^*)^{(\omega)}$, if (x, X) satisfies ϕ in $\mathcal{R}$ it also satisfies ϕ in $\mathcal{S}$ (and conversely). As before we may prove the following test for WS-extensions:

<u>Theorem</u>. Let $\mathcal{R} = \langle A, R \rangle$ and $\mathcal{S} = \langle B, S \rangle$ be structures of $\mathcal{L}$. Then $\mathcal{S}$ is a WS-extension of $\mathcal{R}$ iff

(1) $\mathcal{R} \leq \mathcal{S}$

(2) for every formula ϕ and every pair (x, X) with $x \in A^{(\omega)}$ and $X \in (A^*)^{(\omega)}$, if (x, X) satisfies a formula $\vee v_k \phi$ in $\mathcal{S}$, then there exists an $a \in A$ such that $(x({}^k/a), X)$ satisfies ϕ in $\mathcal{S}$.

<u>Proof</u>: Necessity is obvious. Sufficiency is shown by a double induction on the number of 2^{nd} order quantifiers and on the length of formulas containing a given number of ~~for~~ these quantifiers.

I. Since $\mathcal{R} \leq \mathcal{S}$, if (x, X) satisfies ϕ in $\mathcal{S}$ and ϕ is one of the forms 1-3, then (x, X) satisfies ϕ in $\mathcal{R}$, and conversely.

II. If $\phi = \neg\psi$ and ψ is not satisfied by (x, X) in $\mathcal{S}$, then by the inductive hypothesis, ψ is not satisfied by (x, X) in $\mathcal{R}$, and hence ϕ is satisfied. Conversely,...

III. If $\phi = \psi \wedge \chi$, then ...

IV. If $\phi = \vee v_k \psi$ and (x, X) satisfies ϕ in $\mathcal{S}$, then by hypothesis, there is an $a \in A$ such that $(x({}^k/a), X)$ satisfies ψ in $\mathcal{S}$. Hence by the inductive hypothesis, $(x({}^k/a), X)$ satisfies ψ in $\mathcal{R}$, and hence (x, X) satisfies ϕ in $\mathcal{R}$. Converse is easier.

V. If $\phi = \bigvee \mathcal{V}_k \psi$ and (x, X) satisfies ϕ in $\mathcal{S}$, then there is a $\beta \in \mathcal{B}$ such that $(x, X(^k/_\beta))$ satisfies ψ in $\mathcal{S}$. Suppose $\beta = \langle b_1, \ldots, b_m \rangle$ and let $v_{N+1}, \ldots, v_{N+m}$ be variables not occurring in ϕ. Let ϕ' be obtained from ϕ by replacing the second order quantifier "$\bigvee \mathcal{V}_k$" by the sequence of first order quantifiers "$\bigvee v_{N+1} \ldots \bigvee v_{N+m}$" and by replacing $\mathcal{V}_k$ wherever it occurs in ψ by $Iv_{N+1}{}^\frown Iv_{N+2}{}^\frown \ldots {}^\frown Iv_{N+m}$. ϕ' is satisfied in $\mathcal{S}$ by (x, X). By the inductive hypothesis, ϕ' is satisfied by (x, X) in $\mathcal{R}$, and hence so is ϕ. The converse is trivial.

Even though we no longer have a completeness theorem, the Downwards Lowenheim - Skolem - Tarski Theorem still holds and is proved in the same manner.

<u>Downwards LST Theorem</u>

Let $\mathcal{S} = \langle \mathcal{B}, S \rangle$ be a structure of cardinality β of the language $\mathcal{L}$ (with a denumerable number of relation symbols). Let C be a subset of $\mathcal{B}$ of cardinality γ, and let α be an infinite cardinal for which $\gamma \leq \alpha \leq \beta$. Then there is a structure $\mathcal{R} = \langle A, R \rangle$ of cardinality α such that $C \subset A$ and $\mathcal{S}$ is a WS-extension of $\mathcal{R}$.

<u>Proof</u>: Well order the elements of $\mathcal{B}$ by $\{b_\lambda\}_{\lambda < \beta}$. Let A_0 be a set of elements of $\mathcal{B}$ containing C and of cardinality α. Let A_{n+1} be the set of elements a of $\mathcal{B}$ such that for some pair (x, X) with $x \in A_n^{(\omega)}$, $X \in (A_n^*)^{(\omega)}$ there is a k and a ϕ for which a is the first

element in the ordering of $\mathcal{B}$ such that $(x(^k/a), X)$ satisfies ϕ in $\mathcal{S}$.

$A_n \subseteq A_{n+1}$ (take $\phi = v_j = v_k$). Let $A = \bigcup A_n$, $R = S \upharpoonright A$. card A = card A_0 since no step increases the cardinality. Suppose $x \in A^{(\omega)}$, $X \in (A^*)^{(\omega)}$, and (x, X) satisfies $\bigvee v_k \phi$ in $\mathcal{S}$. We need to show that there is an element $a \in A$ such that $(x(^k/a), X)$ satisfies ϕ in $\mathcal{S}$. Choose n such that $x \in (A_n)^{(\omega)}$ and $X \in (A_n^*)^{(\omega)}$. Since (x, X) satisfies $\bigvee v_k \phi$ in $\mathcal{S}$, there is a $b \in \mathcal{B}$ such that $(x(^k/b), X)$ satisfies ϕ in $\mathcal{S}$. But one such b is in A_{n+1} and hence in A. Thus $\mathcal{S}$ is a WS-extension of $\mathcal{R}$.

The theorem also holds for the RWS language since it is a weaker language than the WS language. I.e., we can represent the notion of a set by that of being a term in a sequence, as follows: Let X represent a finite sequence of the domain. Then

$$x \text{ is a term of } X \iff \bigvee_{T,T'} T^\frown I_x{}^\frown T' = X.$$

(Note that T, T' may represent empty sequences).

<u>Problems</u> Does the Downwards LST Theorem hold for restricted (strong) second order logics?

Show that the Compactness theorem does not hold in the RWS logic.

Axiomatization of the Complex Numbers

We shall give RWS axioms for the theory of the complex numbers based on the following result of Scott and Tarski (Notices, 1958).

Let $\mathcal{A}$ and $\mathcal{B}$ be algebraically closed fields of the same characteristic. Then $\mathcal{A}$ and $\mathcal{B}$ are WS-equivalent iff they have the same finite degree of transcendence or else each has an infinite degree of transcendence over its prime field.

Using notation developed before, let γ stand for the sequence (u, v, m, n). We define

$|\gamma| = n$

$s = \Sigma\gamma \leftrightarrow \bigvee_{\delta} [|\delta| = |\gamma| \wedge \delta_1 = \gamma_1 \wedge \delta_{|\gamma|} = s \wedge \bigwedge_{k} (1 < k < |\gamma| \wedge \text{Nat } k \rightarrow \delta_k = \delta_{k-1} + \gamma_k)]$

$p = \Pi\gamma \leftrightarrow$ (similar definition for product)

$\text{Int } \gamma \leftrightarrow \bigwedge_{k} (0 < k < |\gamma| \wedge \text{Nat } k \rightarrow \text{Int } \gamma_k)$

$\text{Dis } \gamma \leftrightarrow \bigwedge_{j,k} (0 < j, k \leq |\gamma| \wedge \text{Nat } j \wedge \text{Nat } k \wedge \gamma_k = \gamma_j \rightarrow k = j)$

Elements $u_1, \ldots, u_k$ are <u>algebraically independent</u> over the rational field iff whenever $P(u_1, \ldots u_k) = 0$, where P is a polynomial with integer coefficients, then all coefficients of P are zero. We proceed to define the notion of a sequence of alg. ind. elements.

$x \text{ Pow } y \leftrightarrow \bigvee_{\gamma} [\gamma_1 = 1 \wedge x = \gamma_{|\gamma|} \wedge \bigwedge_{k} (1 < k \leq |\gamma| \wedge \text{Nat } k \rightarrow \gamma_k = \gamma_{k-1} \cdot y)]$

$$\beta \text{ Pow } \gamma \leftrightarrow |\beta| = |\gamma| \wedge \bigwedge_k (0 < k < |\gamma| \wedge \text{Nat } k \rightarrow \beta_k \text{ Pow } \gamma_k)]$$

$$\text{Ind } \alpha \leftrightarrow \bigwedge_{\beta,\gamma} (\beta \text{ Pow } \alpha \wedge \gamma \text{ Pow } \alpha \wedge \Pi\beta = \Pi\gamma \rightarrow \beta = \gamma)$$

$$\wedge \bigwedge_{\lambda,\mu,\nu} \{ |\lambda| = |\mu| = |\nu| \wedge \text{Dis } \lambda \wedge \text{Int } \mu \wedge \Sigma\nu = 0$$
$$\wedge \bigwedge_k [0 < k \leq |\lambda| \rightarrow \bigvee_\beta (\beta \text{ Pow } \alpha \wedge \lambda_k = \Pi\beta) \wedge \nu_k = \lambda_k \cdot \mu_k]$$
$$\rightarrow \bigwedge_k (0 < k \leq |\mu| \rightarrow \mu_k = 0) \}$$

I.e., the difference of two monomials in the elements of α is zero only if the monomials are identical; and for any polynomial ν whose terms are integral (μ) multiples of distinct monomials (λ), $\Sigma\nu = 0$ only if all coefficients are zero.

Hence we may axiomatize the complex numbers by

(i) the standard field axioms
(ii) characteristic 0
(iii) field algebraically closed
} as in problems
(iv) infinite degree of transcendence

$$\bigwedge_\alpha [\text{Ind } \alpha \rightarrow \bigvee_\beta (|\beta| > |\alpha| \wedge \text{Ind } \beta)]$$

Axiomatization of the Real Numbers

We may axiomatize the theory of the real numbers in a RSO logic by Dedekind's Theorem; i.e., take as axioms those for ordered fields plus

$$\bigwedge_{S,T} \{ [\bigwedge_x (x \in S \vee x \in T) \wedge \neg \bigvee_x (x \in S \wedge x \in T) \wedge \bigvee_{x,y} (x \in S \wedge y \in T)$$
$$\wedge \bigwedge_{u,v} (u \in S \wedge v \in T \rightarrow u < v)] \rightarrow \bigvee_t \bigwedge_{u,v} (u \in S \wedge v \in T \rightarrow u \leq t \leq v) \}$$

The same result also holds in a language where set variables are restricted to range over denumerable sets. We change the above axiom so that S and T become sets of rationals:

$$\ldots \bigwedge_x (x \in S \vee x \in T \leftrightarrow \mathrm{Rat}\, x) \ldots$$

In this case we must also require that the field be archimedean:

$$\bigwedge_x \bigvee_{y,z} (\mathrm{Rat}\, y \wedge \mathrm{Rat}\, z \wedge y \leq x \leq z).$$

Note that the possibility of giving RSO axioms for the real numbers shows that the Downwards LST does not hold in this system, for the reals have no denumerable isomorphic subfield.

As mentioned before, the theory of the reals is not axiomatizable in a RWS theory. We might expect a characterization similar to that of the complex numbers - archimedean real closed fields of infinite degree of transcendence over the rationals. However two such fields are not necessarily WS-equivalent. The difference is that, whereas in the complex field all transcendental elements may be considered equivalent (via isomorphisms), in the real field particular transcendental numbers may be defined. Hence we would at least have to require that every definable number be in the field (of course such a set of axioms is no longer recursive). Question: Is such a set of axioms sufficient to characterize the reals?

We illustrate two methods of defining particular reals: continued fractions and binary expansions. Let x be an irrational real number ≥ 1 whose unique continued fraction expansion is

$$\cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cdots}}}$$

Then we may define (in a RWS theory)

$$y = x_n \leftrightarrow \bigvee_{\gamma,\delta} \{ 0 \le \delta_1 < 1 \wedge x - \gamma_1 = \delta_1 \wedge y = \gamma_{|\gamma|} \wedge |\gamma| = |\delta|$$
$$\wedge \bigwedge_k [\text{Nat } k \wedge 1 < k \le |\gamma| \rightarrow \text{Nat } \gamma_k \wedge \gamma_k \neq 0$$
$$\wedge 1 = \delta_{k-1}(\gamma_k + \delta_k) \wedge 0 < \delta_k < 1] \}.$$

As an example we could define e by $\{2,1,2,1,1,4,1,1,6,\ldots\}$

$$x = e \leftrightarrow x_1 = 2 \wedge x_2 = 1 \wedge \bigwedge_n (\text{Nat } n \wedge n \neq 0 \rightarrow$$
$$x_{3n} = 2n \wedge x_{3n+1} = x_{3n+2} = 1).$$

Alternatively, suppose $x = .\hat{x}_1 \hat{x}_2 \ldots$ Then

$$y = \hat{x}_n \leftrightarrow \bigvee_{\alpha,\beta,\gamma} \{ |\alpha| = |\beta| = |\gamma| \wedge \beta_1 = \tfrac{1}{2} \wedge y = \alpha_{|\gamma|}$$
$$\wedge \bigwedge_k [0 < k \le |\gamma| \wedge \text{Nat } k \rightarrow (k = 1 \vee \beta_k = \tfrac{1}{2}\beta_{k-1})$$
$$\wedge (\alpha_k = 0 \vee \alpha_k = 1) \wedge \gamma_k = \alpha_k \beta_k] \wedge \Sigma\gamma < x < \Sigma\gamma + \beta_n \}$$

Particular real numbers x are then defined by sets S_x : $n \in S_x \leftrightarrow \hat{x}_n = 1$.

It is easily seen that by either of the above two devices the theory of the real numbers may be treated as a part of second order number theory.

RWS Theory of the Natural Numbers

We note various results concerning the RWS Theory of the natural numbers:

a) $\cdot$ may be defined in terms of $0, 1, +$ by

defining $\quad x \backslash y \leftrightarrow \bigvee_T [0 \in T \wedge \bigwedge_u (u \in T \rightarrow u+x \in T \vee u = y)$,

and then defining $\cdot$ as in a previous homework problem.

b) $+$ cannot be defined in terms of $0, 1, S$ since Büchi has shown the theory of $0, 1, S$ to be decidable, and by (a) if $+$ were definable, then $\cdot$ would be also, and the theory would be undecidable. The problem of defining $+$ in terms of $0, 1, S$ is still open for the RSO theory.

c) The RWS theory of the natural numbers is no stronger than the first order theory since we may represent finite sets in this theory, as follows. Let p be a prime and $x \neq 0$; the pair (x, p) shall represent a set

$$u \in (x, p) \leftrightarrow \bigvee_q (\pi q \wedge q \backslash x \wedge Rem(\tfrac{q}{p}) = u).$$

Since $0 \leq Rem(\frac{q}{p}) < p$, any such set is finite. Conversely, given a finite set $a_1, \ldots, a_n$, choose p to be any prime greater than $\max |a_i|$. For each a_i, we find a prime q_i such that $a_i = Rem(\frac{q}{p})$: if $a_i = 0$, take $q_i = p$; if $a_i \neq 0$, then $(a_i, p) = 1$, and hence by Dirichlet's Theorem, there is a q such that $q_i \equiv a_i \mod p$. Finally, set $x = \prod_{i=1}^{n} q_i$. Then $u \in (x, p)$ iff $u = a_i$ for some i.

d) As a final example of definability, we define + in terms of S and double (2·). In order to do this, we make use of a <u>pairing function</u> which maps ordered pairs univalently into the natural numbers. I.e.,

$$J(x,y) = J(u,v) \leftrightarrow x = u \wedge y = v.$$

The particular function we shall define will be

$$J(x,y) = 2^x(2y+3).$$

In our definition, we shall also employ the following notions

$$z \in P_n \leftrightarrow \bigvee_y z = J(n,y)$$
$$z \in Q_n \leftrightarrow \bigvee_x z = J(x,n)$$
$$z \in R_n \leftrightarrow \bigvee_{x,y} [z = J(x,y) \wedge x+y = n]$$
$$S(u,v) \leftrightarrow \bigvee_{x,y} [u = J(x,y) \wedge v = J(x+1,y)]$$
$$T(u,v) \leftrightarrow \bigvee_{x,y} [u = J(x,y) \wedge v = J(x,y+1)].$$

We define these notions as follows:

$$u < v \leftrightarrow \bigvee_T [u \in T \wedge \bigwedge_x (x+1 \in T \rightarrow x \in T) \wedge v \notin T]$$

$$z \in Q_n \leftrightarrow \bigvee_T [2n+3 \in T \wedge \bigwedge_u (u \in T \rightarrow 2u \in T \vee u = z)]$$

$$S(u,v) \leftrightarrow \bigvee_n [u \in Q_n \wedge v = 2u]$$

$$T(u,v) \leftrightarrow \bigvee_n [u \in Q_n \wedge v \in Q_{n+1} \wedge u < v < 2u]$$

I.e., for some n, $u = 2^x(2n+3)$, $v = 2^y(2n+5)$, and $2^x(2n+3) < 2^y(2n+5) < 2^{x+1}(2n+3)$. Since $1 < 1 + \frac{2}{2n+3} < 2$, we must have $x = y$, and hence $T(u,v)$.

$$z \in R_n \leftrightarrow \bigwedge_A \{2n+3 \in A \wedge \bigwedge_{u,v,w} [S(u,v) \wedge T(u,w) \wedge w \in A \rightarrow v \in A] \rightarrow z \in A\}$$

I.e., $(0,n) \in A$ and $(x,y) \in A \rightarrow (x+1, y-1) \in A$

$$z \in P_n \leftrightarrow \bigvee_A \{ \bigvee_v (u \in Q_0 \wedge v \in R_n \wedge v \in A) \wedge \bigwedge_{u,v} (u \in A \wedge T(u,v) \rightarrow v \in A \vee v = z \}$$

I.e., $J(n,0) \in A$ and $J(n,x) \in A \rightarrow J(n, x+1) \in A$. Finally the pairing function may be defined by

$$z = J(x,y) \leftrightarrow z \in P_x \wedge z \in Q_y.$$

Our original object, though, was to define + in terms of S and double, and this is accomplished by

$$a+b=c \leftrightarrow \bigvee_z (z \in P_a \wedge z \in Q_b \wedge z \in R_c)$$

(See R.M, Robinson, Proceedings, c1957)

Non-restricted theories

Let WS_2 be a language which allows relations in addition to sets. Then + may be defined in WS_2 by

$$a+b=c \leftrightarrow \bigvee_M \{ (0,a) \in M \wedge \bigwedge_{x,y} [(x,y) \in M \rightarrow (Sx, Sy) \in M \vee (x=b \wedge y=c)] \}.$$

Axioms for WS

1. $\bigwedge_{u} \bigvee_{X} I_u = X$

2. $\bigvee_{Z} X^\frown Y = Z$

3. $(X^\frown Y)^\frown Z = X^\frown(Y^\frown Z)$

4. $X^\frown Y = X^\frown Z \rightarrow Y = Z$

5. $X^\frown I_u = Y^\frown I_v \rightarrow u = v$

6. $\bigwedge_{u} \Phi(I_u) \wedge \bigwedge_{X,u} (\Phi(X) \rightarrow \Phi(X^\frown I_u)) \rightarrow \bigwedge_{X} \Phi(X)$

Note that 6. is an induction principle for sequences. The WS theory may be transformed into a first order theory by introducing a predicate

$\sigma(x) \leftrightarrow x$ is a sequence.

The above axioms do not allow for an empty sequence. To obtain one we introduce a new symbol $\emptyset$ and stipulate

$$\bigwedge_{X} \emptyset^\frown X = X$$

Tautologies

We shall give a proof only of T4, thus demonstrating that T4 is a theorem. Thereafter, we shall use metatheorems to establish that T5 – T26 are also theorems. After the first few times, we shall not always refer to every use of M1 and M3. These metatheorems are:

M1 Any axiom is a theorem.

M2 If $\vdash \phi \to \psi$ and $\vdash \phi$, then $\vdash \psi$.

M3 If $\vdash \phi$, then $\vdash \phi\binom{\alpha}{\psi}$.

M4 If $\vdash \phi \to \psi$ and $\vdash \psi \to \theta$, then $\vdash \phi \to \theta$

proof of M4:

$$\vdash (\phi \to \psi) \to ((\psi \to \theta) \to (\phi \to \theta))$$

by M1 on A1 (below) and 3 applications of M3.

Now assume $\vdash \phi \to \psi$ and $\vdash \psi \to \theta$ and apply M2 twice.

Our axioms are A1 – A3 below.

A1 $(p \to q) \to ((q \to r) \to (p \to r))$

A2 $(\neg p \to p) \to p$

A3 $p \to (\neg p \to q)$

T4 $p \to p$

1. $(\neg p \to p) \to p$ A2
2. $p \to (\neg p \to p)$ A3
3. $p \to p$ M4

1. $(p \to q) \to ((q \to r) \to (p \to r))$ A1
2. $(p \to q) \to ((q \to p) \to (p \to p))$ sub in 1
3. $(p \to (\neg p \to p)) \to (((\neg p \to p) \to p) \to (p \to p))$ sub in 2

4. $p \to (\neg p \to q)$ A 3

5. $p \to (\neg p \to p)$ sub in 4

6. $((\neg p \to p) \to p) \to (p \to p)$ det 5 from 3

7. $(\neg p \to p) \to p$ A 2

8. $p \to p$ det 7 from 6

T5 $((\neg p \to q) \to (\neg q \to q)) \to (p \to (\neg q \to q))$

1. $\vdash (p \to (\neg p \to q)) \to (((\neg p \to q) \to (\neg q \to q)) \to (p \to (\neg q \to q)))$

M_1 on A_1, M_3 twice

2. $\vdash p \to (\neg p \to q)$ M_1 on A_3

3. $\vdash ((\neg p \to q) \to (\neg q \to q)) \to (p \to (\neg q \to q))$ M_2 on 1, 2

T6 $(\neg q \to \neg p) \to (p \to (\neg q \to q))$

1. $\vdash (\neg q \to \neg p) \to ((\neg p \to q) \to (\neg q \to q))$ M1 on A1, M3 3 times

2. $\vdash (\neg q \to \neg p) \to (p \to (\neg q \to q))$ M4 on 1, T5

T7 $(\neg q \to \neg p) \to (((\neg q \to q) \to q) \to (p \to q))$

1. $\vdash (p \to (\neg q \to q)) \to (((\neg q \to q) \to q) \to (p \to q))$ A1

2. $\vdash (\neg q \to \neg p) \to (((\neg q \to q) \to q) \to (p \to q))$ M4 on T6, 1

T8 $q \to (((\neg q \to q) \to q) \to (p \to q))$

1. $\vdash q \to (\neg q \to \neg p)$ A3

2. $\vdash q \to (((\neg q \to q) \to q) \to (p \to q))$ M4 on 1, T7

T9 $p \to ((\neg q \to q) \to q)$

1. $\vdash ((\neg q \to q) \to q) \to$

$(((\neg((\neg q \to q) \to q) \to ((\neg q \to q) \to q)) \to ((\neg q \to q) \to q)) \to$

$(p \to ((\neg q \to q) \to q)))$ M3 on T8

2. $\vdash ((\neg((\neg q \to q) \to q) \to ((\neg q \to q) \to q)) \to ((\neg q \to q) \to q)) \to$
$(p \to ((\neg q \to q) \to q))$ M2 on 1, A2

3. $\vdash (\neg((\neg q \to q) \to q) \to ((\neg q \to q) \to q)) \to ((\neg q \to q) \to q)$
M3 on A2

4. $\vdash p \to ((\neg q \to q) \to q)$ M2 on 2, 3

T10 $(((\neg q \to q) \to q) \to (p \to q)) \to (\neg(p \to q) \to (p \to q))$

1. $\vdash (\neg(p \to q) \to ((\neg q \to q) \to q)) \to$
$((((\neg q \to q) \to q) \to (p \to q)) \to (\neg(p \to q) \to (p \to q)))$
A1

2. $\vdash \neg(p \to q) \to ((\neg q \to q) \to q)$ T9

3. $\vdash (((\neg q \to q) \to q) \to (p \to q)) \to (\neg(p \to q) \to (p \to q))$
M2 on 1, 2

T11 $(((\neg q \to q) \to q) \to (p \to q)) \to (p \to q)$

1. $\vdash (\neg(p \to q) \to (p \to q)) \to (p \to q)$ A2

2. $\vdash (((\neg q \to q) \to q) \to (p \to q)) \to (p \to q$ M4 on T10, 1

T12 $q \to (p \to q)$

1. $\vdash q \to (p \to q)$ M4 on T8, T11

T13 $(\neg q \to \neg p) \to (p \to q)$

1. $\vdash (\neg q \to \neg p) \to (p \to q)$ M4 on T7, T11

T14 $\neg p \to (p \to q)$

1. $\vdash \neg p \to (\neg q \to \neg p)$ T12
2. $\vdash \neg p \to (p \to q)$ M4 on 1, T13

T15 $\neg\neg p \to p$

1. $\vdash \neg\neg p \to (\neg p \to p)$ T14
2. $\vdash \neg\neg p \to p$ M4 on 1, A2

T16 $p \to \neg\neg p$

1. $\vdash (\neg\neg\neg p \to \neg p) \to (p \to \neg\neg p)$ T13
2. $\vdash (\neg\neg\neg p \to \neg p)$ T15
3. $\vdash p \to \neg\neg p$ M2 on 1, 2

T17 $(p \to \neg p) \to \neg p$

1. $\vdash (\neg\neg p \to p) \to ((p \to \neg p) \to (\neg\neg p \to \neg p))$ A1
2. $\vdash (p \to \neg p) \to (\neg\neg p \to \neg p)$ M2 on 1, T15
3. $\vdash (\neg\neg p \to \neg p) \to \neg p$ A2
4. $\vdash (p \to \neg p) \to \neg p$ M4 on 2, 3

T18 $((p \to q) \to p) \to p$

1. $\vdash (\neg p \to (p \to q)) \to (((p \to q) \to p) \to (\neg p \to p))$ A1
2. $\vdash ((p \to q) \to p) \to (\neg p \to p)$ M2 on 1, T14
3. $\vdash ((p \to q) \to p) \to p$ M4 on 2, A2

T19 $(p \to (p \to q)) \to (p \to q)$

1. $\vdash (p \to (p \to q)) \to (((p \to q) \to q) \to (p \to q))$ A1
2. $\vdash (((p \to q) \to q) \to (p \to q)) \to (p \to q)$ T18
3. $\vdash (p \to (p \to q)) \to (p \to q)$ M4 on 1, 2

T20 $p \to ((p \to q) \to q)$

1. $\vdash p \to ((p \to q) \to p)$ T12
2. $\vdash ((p \to q) \to p) \to ((p \to q) \to ((p \to q) \to q)$ A1
3. $\vdash p \to ((p \to q) \to ((p \to q) \to q)$
4. $\vdash ((p \to q) \to ((p \to q) \to q) \to ((p \to q) \to q)$ T19
5. $\vdash p \to ((p \to q) \to q)$ M4 on 3, 4

T21 $(q \to r) \to ((p \to q) \to (p \to r))$

1. $\vdash ((p \to q) \to ((q \to r) \to (p \to r))) \to$
   $((((q \to r) \to (p \to r)) \to (p \to r)) \to ((p \to q) \to (p \to r)))$ A1
2. $\vdash ((q \to r) \to (((q \to r) \to (p \to r)) \to (p \to r)) \to$
   $(((((q \to r) \to (p \to r)) \to (p \to r)) \to ((p \to q) \to (p \to r))) \to$
   $((q \to r) \to ((p \to q) \to (p \to r)))))$ A1
3. $\vdash (q \to r) \to (((q \to r) \to (p \to r)) \to (p \to r))$ T20
4. $\vdash ((((q \to r) \to (p \to r)) \to (p \to r)) \to ((p \to q) \to (p \to r))) \to$
   $((q \to r) \to ((p \to q) \to (p \to r)))$ M2 on 2, 3
5. $\vdash ((p \to q) \to ((q \to r) \to (p \to r))) \to ((q \to r) \to ((p \to q) \to (p \to r)))$
   M4 on 1, 4
6. $\vdash (q \to r) \to ((p \to q) \to (p \to r))$ M2 on 5, A1

T22 $(p \to (q \to r)) \to (q \to (p \to r))$

1. $\vdash (p \to (q \to r)) \to (((q \to r) \to r) \to (p \to r))$ A1
2. $\vdash (q \to ((q \to r) \to r)) \to$
   [illegible] $\to (q \to (p \to r)))$ A1

3. $\vdash q \to ((q \to r) \to r)$ T 20

4. $\vdash (((q \to r) \to r) \to (p \to r)) \to (q \to (p \to r))$ M2 on 2, 3

5. $\vdash (p \to (q \to r)) \to (q \to (p \to r))$ M4 on 1, 4

[Since this does not use T 21, an easier demonstration of T 21 could be given using T 22.]

T 23 $(p \to q) \to (\neg q \to \neg p)$

1. $\vdash (q \to \neg\neg q) \to ((p \to q) \to (p \to \neg\neg q))$ T 21
2. $\vdash (p \to q) \to (p \to \neg\neg q)$ M2 on 1, T16
3. $\vdash (\neg\neg p \to p) \to ((p \to \neg\neg q) \to (\neg\neg p \to \neg\neg q))$ A 1
4. $\vdash (p \to \neg\neg q) \to (\neg\neg p \to \neg\neg q)$ M 2 on 3, T15
5. $\vdash (p \to q) \to (\neg\neg p \to \neg\neg q)$ M4 on 2, 4
6. $\vdash (\neg\neg p \to \neg\neg q) \to (\neg q \to \neg p)$ T 13
7. $\vdash (p \to q) \to (\neg q \to \neg p)$ M4 on 5, 6

T 24 $p \to (\neg q \to \neg(p \to q))$

1. $\vdash ((p \to q) \to q) \to (\neg q \to (\neg p \to q))$ T23
2. $\vdash p \to (\neg q \to \neg p \to q)$ M4 on T 20, 1

T 25 $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$

1. $\vdash (q \to (p \to r)) \to ((p \to q) \to (p \to (p \to r)))$ T 19
2. $\vdash ((p \to (p \to r)) \to (p \to r)) \to$
   $(((p \to q) \to (p \to (p \to r))) \to ((p \to q) \to (p \to r)))$
   T 21

3. $\vdash (p \to (p \to r)) \to (p \to r)$ T19

4. $\vdash ((p \to q) \to (p \to (p \to r))) \to ((p \to q) \to (p \to r))$
M2 on 2, 3

5. $\vdash (q \to (p \to r)) \to ((p \to q) \to (p \to r))$ M4 on 1, 4

6. $\vdash (p \to (q \to r)) \to ((p \to q) \to (p \to r))$ M4 on T22, 5

T26 $(p \to q) \to ((p \to (q \to r)) \to (p \to r))$

1. $\vdash ((p \to (q \to r)) \to ((p \to q) \to (p \to r))) \to$
$((p \to q) \to ((p \to (q \to r)) \to (p \to r)))$ T22

2. $\vdash (p \to q) \to ((p \to (q \to r)) \to (p \to r))$ M2 on 1, T25

Arithmeticization of Logic

Results of Gödel have shown the sets of sentences, formulas, theorems, etc. of a first order predicate logic to be arithmetically definable, while Tarski has shown that the set of true sentences is not. In order to derive results such as these, we must develop a mechanism which enables us to talk about such sets; i.e., we must encode formulas, etc., by natural numbers (in a manner not unlike the numerical code for English sentences obtained by substituting numbers for letters).

Various classifications of sets will also be defined; namely,

HA - hyperarithmetic sets
A - arithmetically definable
RE - recursively enumerable
R - (general) recursive or computable
PR - primitive recursive
D - diophantine sets

It will be shown that $HA \supset A \supset RE \supset R \supset PR$ and that $D \subseteq RE$. More about the relation of D to the other sets is not known.

Herbrand Definability

We shall first consider a method of defining functions from Nat to Nat due to Jacques Herbrand (1908-1931). The functions defined in this manner will eventually turn out to be the hyperarithmetic ones.

Basically the method is to define new functions by functional equations involving composition from a given function. Clearly the identity or zero function give nothing new under composition; however the successor function, $Sx = x+1$, is sufficient.

For example, the identity function I is defined by

$$SI = S.$$

(Note that $IS = S$ leaves $I0$ undefined). We may also define the double function, $Dx = 2x$, and the zero function, $0x = 0$, by

$$D0 = 0$$

$$DS = SSD.$$

These equations determine D and 0 uniquely; for let $D(0) = x$. Then $D(1) = 2 + x, \ldots, D(y) = 2y + x > y$ unless $x = y = 0$. But D has a fixed point by $D0 = 0$, so that $x = 0$, and hence $0y = 0$ and $Dx = 2x$.

Along these lines we make the following definition:

<u>Definition</u> A function F_0 is <u>Herbrand definable</u> iff there is a finite system Σ_0 of functional equations in $F_1, \ldots, F_k, F, S$ such that F_0 is the unique function F for which there are functions $F_1, \ldots, F_k$ which satisfy Σ_0.

(Note that $F_1, \ldots, F_k$ do not have to be uniquely determined or even Herbrand definable themselves; they must merely exist.)

E.g., Predecessor: $PS = I$, $P0 = 0$
$Tx = 2^x$: $T0 = S0$, $TS = DT$

To obtain the functions x^2 or $x+y$, we need to have a method of encoding functions of two variables in our system. This is accomplished by pairing functions:

<u>Definition</u>. Two functions K and L are (associated) <u>pairing functions</u> iff $\bigwedge_{x,y} \bigvee_{z} (Kz = x \wedge Lz = y)$.

Such functions exist, for let $J(x,y)$ be a 1-1 mapping of ordered pairs of natural numbers onto the natural numbers. Then we may list the pairs (x_0, y_0), (x_1, y_1), ... according to $J(x_n, y_n) = n$, and we have $Kn = x_n$, $Ln = y_n$. One such function J is the Cantor function

$$J(x,y) = \frac{(x+y)^2 + 3x + y}{2}$$

which lists pairs in the order

$(0,0)$, $(0,1)$, $(1,0)$, $(0,2)$, $(1,1)$, $(2,0)$, $(0,3)$, $(1,2)$, ...

Functions may also be paired. Given F + G, we can write the function H which pairs F and G ($H = J(F, G)$) by $KH = F$, $LH = G$. E.g., $(K+L)J(F,G) = F+G$. Note that the meaning of $F(A,B)$ is $F(A,B)x = F(Ax, Bx)$, and that an equation $H = J(F,G)$ cannot appear in a Herbrand definition, but must be replaced by $KH = F$ and $LH = G$.

At first we shall use the following easily defined pairing functions

$$KD = I \qquad KSD = K$$
$$LD = 0 \qquad LSD = SL.$$

I.e., $K(2x) = x$ and $L(2x) = 0$, so that K and L are uniquely determined on the even numbers. Also $K(2x+1) = Kx$ and $L(2x+1) = 1 + Lx$, so that $2x$ corresponds to $(x,0)$, $4x+1$ to $(x,1)$, $8x+3$ to $(x,2)$, etc. K and L are thus determined on the odd numbers by the number of times the operations of taking the predecessor and halving must be applied to obtain an even number. The mapping J is given by

$$\begin{aligned} J(x,y) &= (SD)^y Dx \\ &= (PDS)^{y-1} SDDx && \text{since } SD = PDS \\ &= PD^{y-1} SSDDx && \text{since } PDSPDS = PD^2S, \text{ etc.} \\ &= PD^y SDx && \text{since } SSD = DS \\ &= 2^y(2x+1) - 1 \end{aligned}$$

Remembering that $J(F, G) = H \Leftrightarrow KH = F \wedge LH = G$, we note $J(I, O) = O$ and $J(K, SL) = SO$.

We may now define particular functions of two arguments:

(i) Addition: $AO = I$, $ASO = SA$.

I.e., $AJ(I, O) = I$ and $AJ(K, SL) = SA$. Note that A is defined as a function of one argument so that $AJ(F, G) = (K+L)J(F,G) = F + G$.

(ii) Multiplication: $MO = O$; $MSO = AJ(M, K)$, or more precisely, $MSO = AW$, $KW = M$, $LW = K$.

(iii) Square Function: $Q = MJ(I, I)$

(iv) Factorial: $FO = SO$, $FS = MJ(F, S)$.

Functional equations may also express certain properties of a given function. E.g., for what functions F does there exist a function G for which $FG = I$? Clearly F must assume all values; that this condition is sufficient is seen by defining Gx = least y such that $Fy = x$. Conversely, those functions G for which there exists an F satisfying $FG = I$ are precisely the univalent ones. Combining the two conditions $(FG = GF = I)$ insures that $F = G^{-1}$ is a permutation.

As we are interested in defining sets of numbers, we may correlate such sets and definable functions in two ways: by characteristic functions and the ranges of functions. We shall employ the second of these methods:

<u>Definition</u> A set $\mathcal{S} \subseteq Nat$ is Herbrand definable iff there is a system Σ of functional equations in F, S, and certain auxiliary functions such that $\mathcal{S}$ is the range of F for each F which satisfies Σ.

E.g., the set $\mathcal{S}$ of natural numbers which are the sum of two squares is defined as the range of $F = AJ(QK, QL)$.

Corresponding to the above definition, we may characterize all functions G which have the same range as F by $FX = G$ and $GY = F$, since $FX = G$ implies $\mathcal{R}F$ = range $F \subseteq \mathcal{R}G$, etc.

If $\mathcal{R}F$ is infinite and has an infinite complement, then we may define a function G in terms of F, S, and auxiliary functions so that $\mathcal{R}G$ = complement $\mathcal{R}F$:

$HH' = H'H = I$ — H is a permutation

$\left.\begin{array}{l} FX = HD \\ HDY = F \end{array}\right\}$ — F and HD have the same range

$\left.\begin{array}{l} GU = HSD \\ HSDV = G \end{array}\right\}$ — G has range equal to the complement of $\mathcal{R}F$

I.e., we define a permutation H to map the partition of the integers determined by the odd and even integers into a partition determined by $\mathcal{R}F$ and its complement.

For functions of more than two variables, we could define extended pairings:

$$J_0(x_0) = x_0, \quad J_{n+1}(x_0, \ldots, x_{n+1}) = J(x_0, J_n(x_1, \ldots, x_n))$$

Then if $J_n(x_0, \ldots, x_n) = w$,

$$x_0 = Kw, \quad x_1 = KLw, \ldots, \quad x_i = KL^i w, \ldots, \quad x_n = L^n w.$$

Also relations could be defined by

$$Rxy \text{ iff } J(x, y) \in \mathcal{S}.$$

Thus, for example,

$$x \mid y \leftrightarrow J(x, y) \in \mathcal{R}J(K, M).$$

Next we define certain logical functions:

(i) Equality

$$EJ(x,y) = \begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x\neq y. \end{cases}$$

We define E by means of a permutation G mapping the even integers into indices of pairs (x,x), and then defining E on RG and its complement:

$$GG' = G'G = I$$
$$GD = J(I,I)$$
$$EGD = SO$$
$$EGSD = O$$

(ii) Inequality

$$\bar{E}J(x,y) = \begin{cases} 1 & \text{if } x\neq y \\ 0 & \text{if } x=y \end{cases}$$

Using G as above, we set

$$\bar{E}GD = O$$
$$\bar{E}GSD = SO.$$

(iii) And

$$UJ(x,y) = \begin{cases} 1 & \text{if } x>0 \text{ and } y>0 \\ 0 & \text{otherwise} \end{cases}$$

Definition: $UJ(K,L) = \bar{E}J(K\cdot L, 0)$

(iv) Or

$$VJ(x,y) = \begin{cases} 1 & \text{if } x>0 \text{ or } y>0 \\ 0 & \text{otherwise} \end{cases}$$

Definition:

$$VJ(0,0) = 0$$
$$VJ(SK,L) = VJ(K,SL) = SO$$

(Note: For the above functions, 1 corresponds to T, 0 to F.)

For the arithmeticization of logic we shall use the Cantor pairing function,* which possesses the properties

$$Kx \le x \qquad Kx = x \text{ iff } x = 0$$
$$Lx \le x \qquad Lx = x \text{ iff } x = 0 \text{ or } x = 1.$$

Let $\mathcal{L}$ be a predicate logic with logical symbols $\neg, \wedge, \vee, \bigwedge, \bigvee, =$; variables $v_0, v_1, \ldots$; and binary operations $+, \cdot$. We Gödel number the formulas of $\mathcal{L}$ as follows:

$$\begin{array}{lcl} \Phi_{8t} & : & v_{Kt} = v_{Lt} \\ \Phi_{8t+1} & : & v_{Kt} + v_{KLt} = v_{LLt} \\ \Phi_{8t+2} & : & v_{Kt} \cdot v_{KLt} = v_{LLt} \\ \Phi_{8t+3} & : & \neg \Phi_t \\ \Phi_{8t+4} & : & \Phi_{Kt} \vee \Phi_{Lt} \\ \Phi_{8t+5} & : & \Phi_{Kt} \wedge \Phi_{Lt} \\ \Phi_{8t+6} & : & \bigvee_{v_{Kt}} \Phi_{Lt} \\ \Phi_{8t+7} & : & \bigwedge_{v_{Kt}} \Phi_{Lt} \end{array}$$

In order to define satisfaction of formulas, we will need a function F such that

$$FJ(n,k) = \begin{cases} 1 & \text{if } v_k \text{ is free in } \Phi_n \\ 0 & \text{otherwise.} \end{cases}$$

We define F in each of the eight residue classes as follows: v_k occurs free in Φ_{8t} iff $k = Kt$ or $k = Lt$. Hence

$$FJ(D^3K, L) = VJ(EJ(L, KK), \; EJ(L, LK))$$

Similarly,

$$\begin{aligned} FJ(SD^3K, L) &= VJ(EJ(L,KK), \; VJ(EJ(L,KLK), EJ(L,LLK))) \\ FJ(S^2D^3K, L) &= FJ(SD^3K, L) \\ FJ(S^3D^3K, L) &= FJ(K, L) = F \\ FJ(S^4D^3K, L) &= VJ(FJ(KK, L), \; FJ(LK, L)) \\ FJ(S^5D^3K, L) &= FJ(S^4D^3K, L) \\ FJ(S^6D^3K, L) &= UJ(FJ(LK, L), \; \bar{E}J(KK, L)) \\ FJ(S^7D^3K, L) &= FJ(S^6D^3K, L) \end{aligned}$$

That F is uniquely determined may be shown by induction on t.

* See p. 111, Problem 4.

We may now define the set of sentences by means of a permutation C which maps the even integers into Gödel numbers of sentences:

$$CC' = C'C = I$$
$$FJ(CDK, L) = 0$$
$$FJ(CSD, Z) = SO$$

I.e., for any $n \in RCD$, there is no k for which v_k occurs free in Φ_n, and there is a function Z giving the index of a variable occurring free in any formula Φ_n with $n \notin RCD$. Hence

$$\Phi_n \text{ is a sentence iff } n \in RCD.$$

In order to define satisfaction, we need to represent infinite sequences which are ultimately 0. We say that x represents the sequence

$$x_0 = Kx,\ x_1 = KLx, \ldots,\ x_n = KL^n x, \ldots$$

The sequence is ultimately 0 since $Lx \leq x$ and $K0 = K1 = 0$. Conversely, given any sequence, we can construct x. E.g., 1, 2, 5, 0, 0,... is represented by $J(1, J(2, J(5, 0)))$.

Similarly there is a correspondence between functions and infinite sequences of functions given by $F_n = FJ(n, x)$. In this manner we may define a function giving the n^{th} term of a sequence $x_n = TJ(n, x)$ by

$$TJ(0, I) = K$$
$$TJ(SK, L) = TJ(K, LL).$$

I.e., T is defined inductively on n by $TJ(n+1, x) = TJ(n, Lx)$ since the sequence Lx is merely x without its first term.

We shall need three further functions:

(i) $HJ(t, J(x,y)) = \begin{cases} 1 & \text{if } x_n = y_n \text{ for all } n \neq t \\ 0 & \text{otherwise} \end{cases}$

(ii) $H_1 J(t, x) = y$, where $y_t = Sx_t$ and $y_n = x_n$ for $n \neq t$

(iii) $H_2 J(t, x) = y$, where $y_t = Px_t$ and $y_n = x_n$ for $n \neq t$

For (i), $HJ(0, J(x,y)) = 1$ iff all terms but the first of x and y are equal; i.e., iff $Lx = Ly$.
To define $HJ(x+1, J(x,y))$, we renumber terms

$$x_0 \ , \quad (Lx)_0 = x_1 \ , \quad (Lx)_1 = x_2 \ , \ \ldots$$
$$y_0 \ , \quad (Ly)_0 = y_1 \ , \quad (Ly)_1 = y_2 \ , \ \ldots$$

and require $HJ(x+1, J(x,y)) = 1$ iff $HJ(x, J(Lx, Ly)) = 1$ and $Kx = x_0 = y_0 = Ky$. Thus the formal definition is

$$HJ(0, I) = EJ(LK, LL)$$
$$HJ(SK, J(KL, LL)) = UJ(HJ(K, J(LKL, LLL), EJ(KKL, KLL)).$$

For (ii) and (iii), the definitions follow easily using (i):

(ii) $TJ(K, H_1 L) = STJ(K, L) = ST$
$\quad HJ(K, J(H_1, L)) = SO$

(iii) $TJ(K, H_2 L) = PT$
$\quad HJ(K, J(H_2, L)) = SO$

Finally we are able to define the satisfaction function

$$WJ(x, x) = \begin{cases} 1 & \text{if the seq. } x = \langle x_0, x_1, \ldots \rangle \text{ satisfies } \varphi_x \\ 0 & \text{otherwise.} \end{cases}$$

W is defined in each of eight cases. The first six are straightforward; e.g.,

$$WJ(8x, x) = \begin{cases} 1 & \text{if } x_{Kx} = x_{Lx} \\ 0 & \text{otherwise} \end{cases}$$

For these cases, we have

$$WJ(D^3K, L) = EJ(TJ(KK, L), TJ(LK, L))$$
$$WJ(SD^3K, L) = EJ((K+L)J(TJ(KK, L), TJ(KLK, L)), TJ(LLK, L))$$
$$WJ(S^2D^3K, L) = \text{same with } K \cdot L \text{ for } K+L$$
$$WJ(S^3D^3K, L) = EJ(0, W)$$
$$WJ(S^4D^3K, L) = VJ(WJ(KK, L), WJ(LK, L))$$
$$WJ(S^5D^3K, L) = UJ(WJ(KK, L), WJ(LK, L))$$

Next we want $WJ(8\ell+6, x) = \begin{cases} 1 & \text{if } \bigvee_{v_{k\ell}} \varphi_{L\ell} \text{ is satisfied by } x \\ 0 & \text{otherwise} \end{cases}$.

In order to provide a definition in this case, we define a permutation A such that $J(\ell, x) \in \mathcal{R}\,AD$ iff x satisfies $\bigvee_{v_{k\ell}} \varphi_{L\ell}$. This condition is assured (a) by the existence of a function B such that $J(\ell, x) \in \mathcal{R}\,AD$ implies $BJ(\ell, x)$ is a sequence differing from x only in the $k\ell^{th}$ term and which satisfies $\varphi_{L\ell}$, and (b) if $J(\ell, x) \in \mathcal{R}\,ASD$, then $\varphi_{L\ell}$ is not satisfied by x or by any sequence differing from x only in the $k\ell^{th}$ term. Thus,

$$AA' = A'A = I$$
$$WJ(S^6 D^3 K, L)AD = SO$$
$$WJ(S^6 D^3 K, L)ASD = O$$
$$\text{(a)}\quad WJ(LK, B)AD = SO$$
$$HJ(KK, J(B, L))AD = SO$$
$$\text{(b)}\quad WJ(LK, L)ASD = O$$
$$J(K, H_1 J(KK, L))ASD = ASDC$$
$$J(K, H_2 J(KK, L))ASD = ASDF$$

Similarly for $WJ(8\ell+7, x) = \begin{cases} 1 & \text{if } x \text{ satisfies } \bigwedge_{v_{k\ell}} \varphi_{L\ell} \\ 0 & \text{otherwise} \end{cases}$,
we take

$$GG' = G'G = I$$
$$WJ(S^7 D^3 K, L)GD = SO$$
$$WJ(S^7 D^3 K, L)GSD = O$$

$$\left.\begin{array}{l} WJ(LK, L)GD = SO \\ J(K, H_1 J(KK, L))GD = GDX \\ J(K, H_2 J(KK, L))GD = GDY \end{array}\right\} \begin{array}{l} J(\ell, x) \in \mathcal{R}\,GD \Rightarrow x \\ \text{satisfies } \varphi_{L\ell}, \text{ as do all} \\ \text{seq. differing only in } k\ell^{th} \text{ term} \end{array}$$

$$\left.\begin{array}{l} WJ(LK, M)GSD = O \\ HJ(KK, J(M, L))GSD = O \end{array}\right\} \begin{array}{l} J(\ell, x) \in \mathcal{R}\,GSD \Rightarrow \text{seq. } MJ(\ell, x) \\ \text{does not satisfy } \varphi_{L\ell}, \text{ but} \\ \text{differs from } x \text{ only in } k\ell^{th} \text{ term} \end{array}$$

This completes the definition of W.

Lemma. W is not arithmetically definable.

Proof: Suppose W were arithmetically definable. Then there would be a formula Φ_n with free variables v_0, v_1 such that

$$W(v_0) = v_1 \leftrightarrow \Phi_n(v_0, v_1).$$

Let $\mathcal{S} = \{x : WJ(x, J(x,0)) \neq 1\}$; i.e., the set of all x such that the sequence $\langle x, 0, 0, \ldots \rangle$ does not satisfy Φ_x. Since the Cantor pairing function J is arith. definable, $\mathcal{S}$ is also arith. definable:

$$(*) \quad x \in \mathcal{S} \leftrightarrow WJ(x, J(x,0)) \neq 1 \leftrightarrow \neg\Phi_n(J(x, J(x,0)), 1)$$

Hence there exists a k such that Φ_k has v_0 as its only free variable and $(**)\, x \in \mathcal{S} \leftrightarrow \Phi_k(x)$.

But then
$$\begin{aligned} k \in \mathcal{S} &\rightarrow WJ(k, J(k,0)) = 1 && \text{by } (**) \\ &\rightarrow k \notin \mathcal{S} && \text{by } (*) \\ k \notin \mathcal{S} &\rightarrow WJ(k, J(k,0)) \neq 1 && \text{by } (**) \\ &\rightarrow k \in \mathcal{S} && \text{by } (*) \end{aligned}$$

Thus we have arrived at the contradiction $k \in \mathcal{S} \leftrightarrow k \notin \mathcal{S}$, and hence our assumption that W is arith. definable must be false.

Note that in the proof of the lemma, we used the following definition of arithmetically definable functions: G is <u>arithmetically definable</u> (<u>A</u>) iff there exists a formula Φ_n with free variables v_0, v_1 such that $Gx = y \leftrightarrow J(x, J(y,0))$ satisfies Φ_n; i.e.,

$$Gx = y \leftrightarrow WJ(n, J(x, J(y,0))) = 1.$$

With this definition, we may immediately establish the following theorem:

<u>Theorem</u> $AD \subset HD$; i.e., the class of arithmetically definable functions (sets) is properly included in the class of Herbrand definable functions (sets).

<u>Proof</u>: If G is arithmetically definable, then $Gx = y \leftrightarrow WJ(n, J(x, J(y, 0))) = 1$ for some n. A Herbrand definition of G is

$$WJ(S^n 0,\ J(I,\ J(G, 0))) = S0.$$

Hence $AD \subseteq HD$, and by the lemma, $W \in HD \sim AD$, so that $AD \subset HD$.

As an application of the fact that W is Herbrand definable, we show that the set of Gödel numbers of true sentences is Herbrand definable. Recalling that the set of Gödel numbers of sentences is equal to $\mathcal{R}\, CD$ for the C defined before, we wish $WJ(CDn, 0) = 1$ iff Φ_{CDn} is true. As usual, we define

$$AA' = A'A = I$$
$$WJ(CD, 0)\, AD = S0$$
$$WJ(CD, 0)\, ASD = 0$$

and $\mathcal{R}\, CDAD$ is the set of true sentences.

<u>Hyperarithmetic Functions</u>

The class of Herbrand definable functions is more commonly referred to as the class of hyperarithmetic functions. We shall now establish the equivalence of the two classes, after first defining "hyperarithmetic".

We increase our language $\mathcal{L}$ to a language $\mathcal{L}'$ by adjoining a symbol F to represent a unary function. Formulas are Gödel numbered as before:

$$\Phi_{q\ell} \quad : \quad v_{K\ell} = v_{L\ell}$$
$$\Phi_{q\ell+1} \quad : \quad Fv_{K\ell} = v_{L\ell}$$
$$\Phi_{q\ell+2} \quad : \quad v_{K\ell} + v_{KL\ell} = v_{LL\ell}$$
$$\vdots$$

etc.

<u>Definition</u>. A predicate or relation is <u>arithmetic in F</u> iff it is definable by a formula of $\mathcal{L}'$.

E.g., $\mathcal{Q}(x, y, F) \Leftrightarrow Fy = x \wedge \bigwedge_z (Fz = x \rightarrow \bigvee_v y+v = z)$.

The satisfaction function W_F is defined with F as a parameter:
$$W_F J(n, x) = \begin{cases} 1 & \text{if } x \text{ satisfies } \Phi_n(F) \\ 0 & \text{otherwise.} \end{cases}$$

Its formal definition mimics that of W: letting $N0 = 0$, $NS = S^9 N$, we add
$$W_F J(SNK, L) = EJ(FTJ(KK, L), TJ(LK, L))$$
to the same definitions for the other eight cases. Thus, for each function F, we get a uniquely determined function W_F.

<u>Definition</u>. A set $\mathcal{S}$ of natural numbers is <u>hyperarithmetical</u> (HA) iff there are predicates $\mathcal{Q}(x, F)$ and $\mathcal{B}(x, F)$ arithmetical in F such that
$x \in \mathcal{S}$ iff there exists an $F \ni \mathcal{Q}(x, F)$
$x \notin \mathcal{S}$ iff there exists an $F \ni \mathcal{B}(x, F)$.

I.e., $\mathcal{S}$ is HA iff it is definable in both one function quantifier forms. (HA $= \Sigma^1_1 \cap \Pi^1_1$ defined later).

<u>Definition</u>. A function F is <u>hyperarithmetical</u> iff its graph $\mathcal{F} = \{J(x, Fx)\}$ is a hyperarithmetical set.

<u>Theorem</u>. A function F (or a non-empty set $\mathcal{S}$) is Herband definable iff it is hyperarithmetical.

Proof: Suppose $\mathcal{S}$ is a given HA set, and let $\mathcal{A}(x, F)$ and $\mathcal{B}(x, F)$ be its defining predicates. Then for each x we can choose a function F_x such that

$$(*) \quad \mathcal{A}(x, F_x) \vee \mathcal{B}(x, F_x)$$

is true. Now let F be the function that encodes the sequence $\{F_0, F_1, \dots\}$: $FJ(x,y) = F_x y$. Then

$$F_x y = z \leftrightarrow \bigvee_w (Fw = z \wedge Kw = x \wedge Lw = y)$$
$$\leftrightarrow \bigvee_w (Fw = z \wedge (x+y)^2 + 3x + y = 2w)$$

(using the Cantor pairing function). Hence $(*)$ is equivalent to an arithmetical predicate $\mathcal{C}(x, F)$. Similarly, $\mathcal{A}(x, F_x)$ is equivalent to an arithmetical predicate $\mathcal{A}'(x, F)$, and

$$\bigvee_F [\bigwedge_x \mathcal{C}(x, F) \wedge \bigwedge_x (x \in \mathcal{S} \leftrightarrow \mathcal{A}'(x, F))].$$

Since $\mathcal{A}$ and $\mathcal{C}$ are arithmetical, there are k, ℓ such that

$$\mathcal{C}(x, F) \leftrightarrow W_F J(k, J(x, 0)) = 1$$
$$\mathcal{A}'(x, F) \leftrightarrow W_F J(\ell, J(x, 0)) = 1.$$

Then we may define the characteristic function R of the set $\mathcal{S}$ by

$$W_F J(S^k 0, J(I, 0)) = S0$$
$$R = W_F J(S^\ell 0, J(I, 0)).$$

Now to show that $\mathcal{S}$ is HD, we construct a function whose range is $\{x : R(x) = 1\}$. If $\mathcal{S}$ is the set of all natural numbers, then $\mathcal{S}$ is trivially HD. If not, we define a permutation G which maps the even integers onto the set of pairs whose first element is in $\mathcal{S}$:

$$GG' = G'G = I$$
$$RKGD = S0$$
$$RKGSD = 0.$$

Then $\mathcal{S} = \mathcal{R}\, KGD$.

If F is a hyperarithmetical function, then its graph $\hat{F}$ is HA and consequently HD from the above. Hence $\hat{F} = \mathcal{R} Z$, where Z satisfies a system Σ of functional equations. For a Herbrand definition of F, take Σ plus $FKZ = LZ$.

Conversely, suppose $\mathcal{S}$ is Herbrand definable. Then there exists a system $\Sigma(S, R, U_1, \ldots, U_k)$ of functional equations such that any R satisfying Σ has range $\mathcal{S}$. Considering K and L as given functions, we can rewrite Σ as $\Theta(S, K, L, Z)$ by letting $KZ = R$, $KL^k Z = U_k$. Then

$$x \in \mathcal{S} \leftrightarrow \bigvee_Z [\Theta(S, K, L, Z) \wedge x \in RKZ],$$

or to transform the right side

$$x \in \mathcal{S} \leftrightarrow \bigvee_Z [\bigwedge_t \Theta(S, K, L, Z)t \wedge \bigvee_y = KZ_y]$$

(where $\bigwedge_t \Theta(S, K, L, Z)t$ means the conjunction of equations of Θ holds for all t). The right side is now seen to be equivalent to an arithmetical predicate since

$$ABx = y \leftrightarrow \bigvee_z (Az = y \wedge Bx = z)$$
$$Kx = y \leftrightarrow \bigvee_z (2x = (y+z)^2 + 3y + z)$$
$$Lx = y \leftrightarrow \bigvee_z (2x = (z+y)^2 + 3z + y).$$

Furthermore,

$$x \notin \mathcal{S} \leftrightarrow \bigvee_Z [\bigwedge_t \Theta(S, K, L, Z) \wedge x \notin RKZ],$$

where the right side is similarly equivalent to an arithmetical predicate. Hence $\mathcal{S}$ is hyperarithmetical.

If F is a Herbrand definable function, then its graph $\hat{F} = R\, J(I, F)$ is also HD. By the above, $\hat{F}$ is HA, and thus so is F.

References:

Grzegorczyk, Mostowski, et. al., <u>JSL</u> (1958)

Kleene, <u>Bulletin</u> (1955)

Problems

1. Give a Herbrand definition of the n^{th} prime function; i.e., $F0 = 2$, $F1 = 3$, $F2 = 5, \ldots$

2. Show that if M and N can be obtained by composition from I, K, and L, then $J(M,N)$ can be obtained by composition from $J(LK, KL)$ and $J(L, I)$.

In 3 and 4, do not use the pairing functions previously defined:

3. Write a system Σ of functional equations in F, G, S, and auxiliary functions which defines the class of all pairing functions; i.e., for particular functions F and G, there are auxiliary functions which satisfy Σ iff F and G are associated pairing functions.

4. Give a Herbrand definition of the Cantor pairing functions; i.e., those corresponding to the mapping
$$J(x,y) = \tfrac{1}{2}[(x+y)^2 + 3x + y]$$

5. Give a Herbrand definition of a function H which lists all polynomials with natural number coefficients; i.e., $HJ(n,x)$ is a polynomial in the terms of x for each n, and every such polynomial occurs for some n.

6. Show that there is a system
$$\Sigma(S, F, G, U_1, \ldots, U_k)$$
of functional equations such that

(i) Σ has a unique solution for $G, U_1, \ldots, U_k$ for every F with an infinite range and no solution otherwise, and

(ii) whenever $F, G, U_1, \ldots, U_k$ satisfy Σ, then $RG = RF$ and G is univalent.

7. Show that there is a system

$$\Gamma(S, F, G, U_1, \ldots, U_k)$$

of functional equations such that for every F whose range is not the set of all natural numbers there is a unique solution for $G, U_1, \ldots, U_k$, and if RF is the set of all natural numbers there is no solution; furthermore, whenever $F, G, U_1, \ldots, U_k$ satisfy Γ, then RF and RG are complementary sets.

Recursive Functions

For the present we will not give a precise definition of recursive functions, but will think of them as being functions which are in some sense effectively computable. Hence, if we attempted to specialize the Herbrand definitions we might be lead to the following equivalent characterizations of recursive functions:

Characterization I. A function F_0 is recursive iff there is a finite system Σ of functional equations in $0, S, F, U_1, \ldots, U_k$ such that

(i) Σ has a unique solution, and

(ii) For every natural number n, the equation

$$FS^n0 = S^{F_0 n}0$$

is derivable from Σ and equations of the form $\alpha = \alpha$ by replacing equals with equals.

Characterization II. A function F_0 is recursive iff there is a finite system Σ of functional equations in $0, S, F, U_1, \ldots, U_k$ such that the equation $FS^k0 = S^\ell 0$ is derivable from Σ and equations of the form $\alpha = \alpha$ by replacing equals with equals iff $\ell = F_0 k$.

Definition. A set is recursively enumerable (r.e.) iff it is empty or the range of a rec. function.

Intuitively a r.e. set is one which may be enumerated or listed. Accordingly the following characterization holds since we may list all equations derivable from a system Σ in an effective manner.

<u>Characterization.</u> A set $\mathcal{S}$ is r.e. iff there is a finite system Σ of functional equations in $0, S, F, u_1, \ldots, u_k$ such that $n \in \mathcal{S}$ iff some equation of the form $F\alpha = S^n 0$ is derivable from Σ and equations of the form $\beta = \beta$ by replacing equals with equals.

<u>Definition.</u> A set $\mathcal{S}$ is <u>recursive</u> iff its characteristic function is recursive.

<u>Characterization.</u> A set is recursive iff both it and its complement are r.e.

<u>Definition.</u> A set is <u>diophantine</u> iff it is the set of natural numbers which satisfy a formula of the form

$$\bigvee_{u_1,\ldots,u_k} P(x, u_1, \ldots, u_k) = Q(x, u_1, \ldots, u_k),$$

where P and Q are polynomials with natural number coefficients.

Obviously $D \subseteq RE$ since the values of P and Q may be listed for all $(k+1)$-tuples. It is an open question (related to Hilbert's 10^{th} problem) whether $RE \subseteq D$ or not.

<u>Theorem</u> (Davis) A set $\mathcal{S}$ is r.e. iff there is a polynomial P with integer coefficients such that

$$x \in \mathcal{S} \leftrightarrow \bigvee_{y} \bigwedge_{z \le y} \bigvee_{u_1 \ldots u_k} P(x, y, z, u_1, \ldots, u_k) = 0.$$

R.M. Robinson has shown that it is possible to take $k = 4$ in the above theorem. At any rate, the theorem shows that $RE \subseteq AD$.

Primitive Recursive Functions

The primitive recursive functions are those which may be defined from certain initial functions by substitution or recursion, as follows:

Initial functions:

Identity function: $I_{nk}(x_1, \ldots, x_n) = x_k$, $1 \le k \le n$

Zero function: $O_n(x_1, \ldots, x_n) = 0$, $0 \le n$

Successor function: $Sx = x+1$

Substitution Rule

If $A_1, \ldots, A_m$ are functions of n variables, B a function of m variables, and if $A_1, \ldots, A_m, B$ have already been defined, then a function F of n variables may be defined by

$$F(x_1, \ldots, x_n) = B(A_1(x_1, \ldots, x_n), \ldots, A_m(x_1, \ldots, x_n)).$$

Recursion Rule

If A is a function of n variables, B a function of $n+2$ variables, and if A, B have already been defined, then a function F of $n+1$ variables may be defined by

$$F(x_1, \ldots, x_n, 0) = A(x_1, \ldots, x_n)$$

$$F(x_1, \ldots, x_n, Sy) = B(x_1, \ldots, x_n, y, F(x_1, \ldots, x_n, y)).$$

Examples

(i) $u+0 = I_{11}(u)$ — Addition

$u+Sy = SI_{33}(u, y, u+y)$

(ii) $u \cdot 0 = O_1(u)$ — Multiplication

$u \cdot Sy = I_{33}(u, y, u\cdot y) + I_{32}(u, y, u \cdot y)$

(iii) $u^0 = SO_1(u)$ — Exponentiation

$u^{Sy} = I_{33}(u, y, u^y) \cdot I_{32}(u, y, u^y)$

(iv) $P0 = O_0$ — Predecessor

$PSx = I_{21}(x, Px)$

(v) $u \dot{-} 0 = I_{11}(u)$ — Subtraction

$u \dot{-} Sx = PI_{33}(u, x, u \dot{-} x)$

(vi) Let $Fx = [\sqrt{x}]$. Then

$$F0 = 0$$
$$FSx = Fx + 0^{(SFx)^2 \dot{-} Sx}$$

I.e., $FSx = Fx + 1$ if Sx is a square, and $FSx = Fx$ otherwise.

(vii) $|x-y| = (x \dot{-} y) + (y \dot{-} x)$

(viii) Let $R(x,y)$ = remainder of $x \div y$. We define

$$R(0,y) = 0$$
$$R(Sx,y) = SR(x,y) \cdot 0^{0^{|SR(x,y)-y|}}.$$

This definition implies that

$$R(x,0) = x.$$

(ix)
$$[\tfrac{0}{y}] = 0$$
$$[\tfrac{Sx}{y}] = [\tfrac{x}{y}] + 0^{R(Sx,y)}$$

Note that

$$b = a \cdot [\tfrac{b}{a}] + R(b,a).$$

(x) Let $Gx = \sum_{t<x} Ft$. If F is PR, then so is G since

$$G0 = 0$$
$$GSx = Gx + Fx.$$

(xi) Similarly for $Gx = \prod_{t<x} Ft$,

$$G0 = 1$$
$$GSx = Gx \cdot Fx$$

<u>Problems</u>

8. Show that the functions K and L corresponding to (a) $J(x,y) = \frac{1}{2}[(x+y)^2 + 3x + y]$, and (b) $J(x,y) = 2^y(2x+1)$ are primitive recursive.

9. Show that the characteristic function of the set of primes is primitive recursive.

Other classes of functions may be defined in a similar manner. Kalmar defined the <u>elementary functions</u> as the class of functions obtained from the initial functions, $[\frac{x}{y}]$, $\sum_{t<x}$, and $\prod_{t<x}$ by composition. All elementary functions are obviously primitive recursive, yet all r.e. sets may be

obtained as ranges of elementary functions.

R. M. Robinson (Bulletin, 1947) has shown that the recursion rule may be simplified by assuming some primitive recursive J, K, L as initial functions (and eliminating these later if desired). We perform this simplification in steps. First the parameters $u_1, \ldots, u_k$ may be paired. E.g., for the case $k=2$, assume that A and B have been obtained using only one parameter recursion, and

$$F(u, v, 0) = A(u, v)$$
$$F(u, v, Sx) = B(u, v, x, F(u, v, x)).$$

Then we may define a function $F'(u,x) = F(Ku, Lu, x)$ by letting

$$A'u = A(Ku, Lu)$$
$$B'(u, x, y) = B(Ku, Lu, x, y)$$
$$F'(u, 0) = A'u$$
$$F'(u, Sx) = B'(u, x, F'(u, x)).$$

F' is thereby defined using only one parameter recursion, and F may be recovered by

$$F(u, v, x) = F'(J(u, v), x).$$

Next the parameter may be eliminated altogether from the function B. For suppose A and B have been defined using this restricted form of recursion and

$$F(u, 0) = Au$$
$$F(u, Sx) = B(u, x, F(u, x)).$$

Then we define a function $F'(u, x) = J(u, F(u, x))$ by letting

$$A'u = J(u, Au)$$
$$B'(x, y) = J(Ky, x, Ly)$$
$$F'(u, 0) = A'u$$
$$F'(u, Sx) = B'(x, F'(u, x)).$$

B' has no parameter u, and F may be recovered by

$$F(u, x) = LF'(u, x).$$

Finally we may eliminate the dependence of B upon x. For suppose A and B have been defined using this form of recursion, and that

$$F(u,0) = Au$$
$$F(u,Sx) = B(x, F(u,x)).$$

Then we may define a function $F'(u,x) = J(x, F(u,x))$ by letting

$$A'u = J(0, Au)$$
$$B'y = J(SKy, B(Ky, Ly))$$
$$F'(u,0) = A'u$$
$$F'(u,Sx) = B'(F'(u,x)).$$

Hence B' does not depend on x, and F may be recovered by $F(u,x) = LF'(u,x)$. Consequently we have shown that by assuming J, K, L as initial functions, the recursion rule may be replaced by one of the form

$$F(u,0) = Au$$
$$F(u,Sx) = BF(u,x).$$

Whether the same is still true without assuming J, K, and L as initial functions is an open question, since it is not known whether the predecessor function P can be defined by this limited form of recursion.

That the primitive recursive functions are arithmetically definable was shown by Gödel in 1931. The key to his result is the representation of finite sequences in first order number theory. This representation in turn is based on the following lemma:

<u>Lemma</u>. If $0 \le a_k < m_k$ for $0 \le k \le n$ and each pair of moduli m_k are relatively prime, then for $m = m_0 m_1 \cdots m_k$ and any c, the conditions

$$R(x, m_0) = a_0$$
$$\vdots \quad \vdots \quad \vdots$$
$$R(x, m_k) = a_k$$

have a unique solution for x in $c \le x < c+m$.

<u>Proof</u>: $R(x, m_k) = R(y, m_k)$ implies $m_k \mid x-y$. Thus if x and y are solutions, $m \mid x-y$, and $c \le x, y < c+m$ implies $x-y=0$. That the conditions possess a solution follows from the fact that given $m_0, \dots, m_k$, every x in $c \le x < c+m$ determines a set $a_0, \dots, a_k$ of remainders. But there are only $m = m_0 \cdots m_k$ such sets, so that each one must correspond to a particular x.

Next we ask when $m_0, \dots, m_n$ will be relatively prime if $m_k = 1 + (k+1)d$.
Assume $p \mid m_k$ and $p \mid m_\ell$. Then $p \mid m_k - m_\ell = (k-\ell)d$. We cannot have $p \mid d$, for then also $p \mid 1$. Now choose d so that $k-\ell \mid d$. Since $0 < |k-\ell| \le n$, it suffices to take $n! \mid d$. Then $p \nmid k-\ell$, and hence m_k and m_ℓ are relatively prime. Thus to represent a sequence $a_0, \dots, a_n$, we may choose a, d (with $n! \mid d$) such that $R(a, 1+(k+1)d) = a_k$ for $0 \le k \le n$.

<u>Theorem</u>. $PR \subseteq AD$.

<u>Proof</u>: The initial functions are trivially arithmetically definable by

$$y = I_{nk}(x_1, \dots, x_n) \leftrightarrow y = x_k$$
$$y = O(x_1, \dots, x_n) \leftrightarrow y = 0$$
$$y = Sx \leftrightarrow y = x+1.$$

For the substitution rule,

$$y = B(A_1(x_1 \dots x_n), \dots, A_m(x_1 \dots x_n))$$
$$\leftrightarrow \bigvee_{u_1 \dots u_m} \{ u_1 = A_1(x_1 \dots x_n) \wedge \dots \wedge u_m = A_m(x_1 \dots x_n) \wedge y = B(u_1 \dots u_m) \}.$$

The pairing functions J, K, L are arithmetically definable as before

$$z = J(x,y) \leftrightarrow 2z = (x+y)^2 + 3x + y$$
$$x = Ku \leftrightarrow \bigvee_y u = J(x,y)$$
$$y = Lu \leftrightarrow \bigvee_x u = J(x,y).$$

Hence we need show only that a function F defined by the restricted recursion rule

$$F(u,0) = Au$$
$$F(u,Sx) = BF(u,x)$$

is arithmetically definable. This is done by asserting the existence of functional values $F(u,0), \ldots, F(u,x)$ with the required properties:

$$y = F(u,x) \leftrightarrow \bigvee_{a,d} \{ R(a, 1+d) = Au \wedge R(a, 1+(x+1)d) = y \wedge \bigwedge_{z} [z < x \rightarrow R(a, 1+(2+z)d) = BR(a, (1+z)d+1)]\}.$$

Finally, $<$ and R are arithmetically definable:

$$z < x \leftrightarrow \bigvee_{w} (w \neq 0 \wedge z+w = x)$$
$$R(x,y) = z \leftrightarrow \bigvee_{q} (x = y \cdot q + z \wedge 0 \leq z < y).$$

Primitive Recursive Sets and Relations

Definition. A relation $\Phi(x_1, \ldots, x_n)$ is primitive recursive iff there is a primitive recursive function $F(x_1, \ldots, x_n)$ such that

$$\Phi(x_1, \ldots, x_n) \leftrightarrow F(x_1, \ldots, x_n) = 0.$$

Examples

$$x = y \leftrightarrow |x-y| = 0$$
$$x > y \leftrightarrow 0^{x \dot{-} y} = 0$$

The class of PR relations is closed under the boolean operations since if $\Phi \underline{x} \leftrightarrow F\underline{x} = 0$ and $\Psi \underline{x} \leftrightarrow G\underline{x} = 0$ (where $\underline{x}$ denotes $x_0, \ldots, x_n$), then

$$\neg \Phi \underline{x} \leftrightarrow 0^{F\underline{x}} = 0$$
$$(\Phi \vee \Psi)\underline{x} \leftrightarrow F\underline{x} \cdot G\underline{x} = 0$$
$$(\Phi \wedge \Psi)\underline{x} \leftrightarrow F\underline{x} + G\underline{x} = 0.$$

Problem. 10. Find a polynomial $P(x, y, u_1, \ldots, u_k)$ with integer coefficients such that

$$y = 2^x \leftrightarrow Q_1 u_1 \ldots Q_k u_k \; P = 0,$$

where the Q_i are suitable quantifiers.

The class of PR relations is also closed under bounded quantification: let $\Phi(\underline{x}, y) \leftrightarrow F(\underline{x}, y) = 0$ be a PR relation. Then

$$\bigvee_y (y < z \wedge \Phi(\underline{x}, y)) \leftrightarrow \prod_{y<z} F(\underline{x}, y) = 0$$

$$\bigwedge_y (y < z \rightarrow \Phi(\underline{x}, y)) \leftrightarrow \sum_{y<z} F(\underline{x}, y) = 0$$

The class of PR relations is also closed under the bounded μ operator: $\mu y \{ \Phi(\underline{x}, y) \}$ = the least y such that $\Phi(\underline{x}, y)$. I.e., if $\Phi(\underline{x}, y)$ is PR, then [redacted]

$$G(\underline{x}, z) = \mu y \{ y = z \vee \Phi(\underline{x}, y) \}$$

is a PR function. For suppose

$$F(\underline{x}, y) = \begin{cases} 1 & \text{if } \neg \Phi(\underline{x}, y) \\ 0 & \text{if } \Phi(\underline{x}, y). \end{cases}$$

Then

$$\prod_{y \le k} F(\underline{x}, y) = \begin{cases} 0 & \text{if } \bigvee_{y \le k} \Phi(\underline{x}, y) \\ 1 & \text{otherwise} \end{cases}$$

$$G(\underline{x}, z) = \sum_{k<z} \prod_{y \le k} F(\underline{x}, y).$$

We now define various PR relations and functions for future use

(i) the Cantor pairing functions are defined by noting

$$J(0, 0) = 0$$
$$J(0, y+1) = J(y, 0) + 1$$
$$J(x+1, y-1) = J(x, y) + 1. \quad \text{if } y \neq 0$$

Then

$$L0 = 0 \qquad K0 = 0$$
$$LSx = PLx + [\sqrt{DSx}]\, 0^{Lx} \qquad KSx = 0^{0^{Lx}} SKx$$

(ii) the pairing function $J(x,y) = 2^y(2x+1) - 1$ by letting

$$Fx = \sum_{z<x} (0^{R(x,2^z)} \dot{-} 1)$$

and

$$Lu = FSu$$
$$Ku = \left[\frac{Su}{2^{LSu}}\right]$$

(iii) $\nu(x) = \begin{cases} 0 & \text{if } x = 0 \\ \text{number of divisors of } x & \text{if } x > 0 \end{cases}$

by

$$\nu(x) = \sum_{n=1}^{x} 0^{R(x,n)}$$

(iv) prime $x \leftrightarrow \nu(x) = 2$

(v) $\pi(x) =$ number of primes less than or equal to x

$= \sum_{u \leq x} 0^{|\nu(x) - 2|}$

(vi) Fu = least prime greater than u

$= \mu y \{ y = u! + 1 \vee (y > u \wedge \text{prime } y) \}$

(vii) $p_0 = 2, \quad p_{Sx} = F p_x$

(viii) $\min(x,y) = \mu z \{ z = x \vee z = y \}$

$\max(x,y) = x + y \dot{-} \min(x,y)$

(ix) $LCM(x,y) = \mu z \{ z = xy \vee (z \neq 0 \wedge x \mid z \wedge y \mid z) \}$

(x) $\exp_n(x) = \mu s \{ s = x \vee p_n^{s+1} \nmid x \}$

For $x > 0$, we have

$$x = \prod_{n<x} p_n^{\exp_n(x)}$$

(xi) $\operatorname{sgn} z = 0^{0^z}$

(xii) Euler ϕ-function: $\phi(x)$ = number of integers $< x$ and prime to x. Recall that if

$$x = \prod_{n=1}^{m} q_n^{\ell_n}$$

then

$$\phi(x) = \prod_{n=1}^{m} q_n^{\ell_n - 1}(q_n - 1)$$

$$= \prod_{n<x} p_n^{\exp_n x \dot{-} 1} (p_n - 1)^{\operatorname{sgn} \exp_n x}$$

Finally, we may also define functions by "course of values" recursion; i.e., a recursion scheme in which $F(x+1)$ may depend on arbitrary $F(y)$ with $y \leq x$. Given F, let

$$\tilde{F}(x) = 2^{F0} 3^{F1} \cdots p_x^{Fx}.$$

More precisely,

$$\tilde{F}0 = 2^{F0}$$

$$\tilde{F}Sx = \tilde{F}x \cdot p_{Sx}^{FSx}.$$

Then

$$Fx = \exp_x \tilde{F}x.$$

E.g., $H0 = 1$, $HSx = GH[\frac{x}{2}]$ is defined by

$$\tilde{H}0 = 2$$

$$\tilde{H}Sx = \tilde{H}x \cdot p_{Sx}^{G \exp_{[\frac{x}{2}]} \tilde{H}x}.$$

<u>Problem 11.</u> Do there exist PR functions A and B such that every primitive recursive function F is given by $F = AGB$ for some primitive recursive permutation G?

<u>Theorem</u>. Every PR function of one variable may be obtained from $0, I, K, L$ by constructing new functions F from previously obtained functions A and B by the following rules

(i) $F = AB$

(ii) $F = J(A, B)$

(iii) $\left.\begin{array}{l} FJ(I,0) = A \\ FJ(K, SL) = BF \end{array}\right\}$ or $\begin{array}{l} FD = A \\ FSD = BF. \end{array}$

Furthermore, if K and L are primitive recursive, then only such functions are obtained.

<u>Proof</u>: We show that if $F(x_1, \dots, x_n)$ is PR, then $F(K, KL, \dots, KL^{n-2}, L^{n-1})$ is in the class so generated. For the initial functions,

$$O_n(K, KL, \dots, L^{n-1}) = 0$$

$$S(K) = SK$$

$$I_{nk}(K, KL, \dots, L^{n-1}) = \begin{cases} KL^{n-1} & \text{if } k \neq n \neq 1 \\ L^{n-1} & \text{if } k = n \neq 1 \\ k & \text{if } n = 1 \end{cases}$$

For composition $F(\underline{x}) = B(A_1(\underline{x}), \dots, A_m(\underline{x}))$, we take

$$F(K, \dots, L^{n-1}) = B(K, \dots, L^{m-1})\, J(A_1(K, \dots, L^{n-1}), J(\dots, A_m(K, \dots, L^{n-1}) \dots))$$

For recursion, if $F(u, 0) = Au$

$$F(u, Sx) = BF(u, x),$$

we let $F' = F(K, L)$

$$F'J(I, 0) = (F(I, 0) =)\ A$$

$$F'J(K, SL) = (F(K, SL) =)\ BF'$$

Using this theorem, we may now show that $PR \subseteq R$ by showing that every PR function of one variable is computable according to Characterization I.

<u>Theorem.</u> Every PR function of one variable is recursive.

<u>Proof:</u> We shall construct a system Σ of functional equations from which the values of all PR functions of one variable may be computed. First the initial functions are computable:

$$\begin{array}{llll} OO = O & S = S & IO = O & DO = O \\ OS = O & & IS = S & DS = SSD \end{array}$$

Also, $KD = I \quad LD = 0$, $KSD = K \quad LSD = SL$ } pairing fct. $2^y(2x+1) - 1$.

E.g., D is computable since $DS^n O = S^{2n} O$; K is computable in terms of earlier values since $x < SDx$.

If F is defined by one of the two schemes

$$F = AB \quad \text{or} \quad \begin{array}{l} FJ(I,0) = FD = A \\ FJ(K,SL) = FSD = BF, \end{array}$$

then the values of F are computable if the values of A and B are. The difficulty lies in showing that $F = J(A,B)$ is computable. To this end we introduce an operation $*$ such that

$$F^* = J(K, FL)$$
$$F = LF^*J(I,I).$$

We will show that the $*$ of all PR functions is computable, and thus that F is computable (upon showing $J(I,I)$ to be computable).

Note that $(AB)^* = J(K, ABL) = J(K, AL)\, J(K, BL) = A^* B^*$, so that $(AB)^*$ is computable if A^*, B^* are. If F is defined by recursion, then

$$\begin{array}{lll} FD = A & \Rightarrow & F^* D^* = A^* \\ FSD = BF & & F^* S^* D^* = B^* F^*. \end{array}$$

F^* will be computable from A^* and B^* in terms of earlier values provided that

(i) $S^* D^*$ is increasing

(ii) D^* and $S^* D^*$ have complementary ranges.

For (i), we note $0^* = J(K,0) = DK$ is computable. $S^* = J(K, SL) = D$ is also computable and increasing. Then $D^*0^* = D^*DK = 0^* = DK$ or $D^*D = D$. Also $D^*S^* = D^*SD = S^*S^*D^*$, so that $D^*SD = S^*S^*D^*$ is computable and increasing (show by induction). Hence S^*D^* is increasing.

For (ii), observe that if A, B have complementary ranges, then so do $J(K, AL)$ and $J(K, BL)$.

It remains to be shown that $J(A,B)^*$ is computable. Now

$$\begin{aligned} J(A,B)^* &= J(K, J(AL, BL)) \\ &= J(K^3, J(L, LK))\, J(J(I, BL), AL) \\ &= J(K^3, J(L, LK))\, J(I, ALK)\, J(I, BL) \\ &= J(K^3, J(L, LK))\, A^*\, J(I, LK)\, B^*\, J(I, L) \end{aligned}$$

Hence it suffices to show that

$$J(K^3, J(L, LK)),\quad J(I,LK),\quad J(I,L),\quad J(I,I),\ K^*, L^*$$

are computable. First

$$K^*D^* = I^* = J(K,L) = I \qquad L^*D^* = 0^*$$
$$K^*S^*D^* = K^* \qquad L^*S^*D^* = S^*L^*$$

show that K^* and L^* are computable. For the others, we write

$$\begin{aligned} J(A,B) &= J(AK, BL)\, J(I,I) \\ &= J(AL, K)\, J(BL, K)\, J(I,I) \\ &= J(L,K)\, A^*\, J(L,K)\, B^*\, J(I,I) \end{aligned}$$

This again reduces the task to showing the computability of $J(L, LK)^*$, $J(I, LK)$, $J(I, L)$, $J(I,I)$, $J(L,K)$.

$J(L,LK)^* = J(K,LL)^*\, J(L,K)^* = L^{**}\, J(L,K)^*$, and L^{**} may be shown to be computable as before. Hence we can replace $J(L,LK)^*$ by $J(L,K)^*$ in the above list.

The remainder of the proof will be sketched, as the details are similar to those already carried out.

$J(SK, SL)\,J(I, 0) = J(S, S0) = S^* J(I,0)\, S = S^* DS$

$J(SK, SL)\,J(K, SL) = J(SK, SSL) = S^* J(SK, SL)$

Hence $J(SK, SL)$ is computable. $J(SK, SL)^*$ is also computable by $*$-ing both sides above.

$J(SK, L)\, D = J(S, 0) = DS$

$J(SK, L)\, SD = J(SK, SL)$

Hence $J(SK, L)$ and $J(SK, L)^*$ are computable.

Let $U0 = 0$

$US = SDU$. U is computable, and $Uy = 2^y - 1$.

$J(L, K)\, D = J(0, I) = U$

$J(L, K)\, SD = J(SL, K) = J(SK, L)\, J(L, K)$

Hence $J(L, K)$ and $J(L, K)^*$ are computable and may be removed from the list.

~~[illegible]~~

$J(I, I)\, 0 = J(0, 0) = 0$

$J(I, I)\, S = J(SK, SL)\, J(I, I)$.

Hence $J(I, I)$ is computable.

Finally $J(I, LK)$ and $J(I, L)$ are computable by $J(A, B) = J(L,K)A^* J(L,K) B^* J(I, I)$ since $L^* K^*$ and L^* are computable.

This completes the proof of the theorem since we have shown that the $*$ of every PR function is computable and hence that every PR function itself is computable.

Recursive Functions

With the aid of primitive recursive functions we are now able to make more explicit our characterizations of recursive functions and to prove the equivalence of these characterizations.

According to Char. II, F_0 is computable from Σ iff for all m, n, the equation $FS^m0 = S^n0$ is derivable from Σ iff $n = F_0 m$. Thus the key to computability is the notion of a "derivation" of a functional value. This notion may be formalized in a manner similar to the formalization of a notion of proof, as follows:

Consider a language with finite sequences, and let Σ be a system of functional equations in $0, S, F, U_1, \ldots, U_k$ which possesses a unique solution. We shall define the notion that a sequence of equations $E(0), E(1), \ldots, E(x)$ is a derivation from Σ of a value of F_0. Let the function letters $0, S, F, U_1, \ldots, U_k$ be numbered by $0, 1, 2, \ldots, k+2$, and let $E(\ell)$ be represented by $\alpha(\ell) \equiv \beta(\ell)$, where α and β are sequences of numbers $\leq k+2$, and where $\equiv$ is regarded as a relation on sequences. Then, informally, $E(0), \ldots, E(x)$ is a derivation from Σ of a value of F_0 iff

$$\bigwedge_{\ell \leq x} \Big\{ E(\ell) \in \Sigma \;\vee\; \alpha(\ell) = \beta(\ell) \;\vee\; \bigvee_{s<\ell} E(\ell) = \breve{E}(s)$$

$$\vee \bigvee_{r,s \leq \ell} \; \bigvee_{\gamma,\delta \leq \alpha(r)} [\alpha(r) = \gamma^\frown\alpha(s)^\frown\delta \wedge \alpha(\ell) = \gamma^\frown\beta(s)^\frown\delta \wedge \beta(\ell) = \beta(r)] \Big\}$$

$$\wedge \; \alpha(x)_0 = 2 \wedge \bigwedge_{0<y<|\alpha(x_0)|-1} [\alpha(x)_y = 1] \wedge \alpha(x)_{|\alpha(x)|-1} = 0$$

$$\wedge \bigwedge_{y<|\beta(x)|-1} \beta(x)_y = 1 \quad \wedge \quad \beta(x)_{|\beta(x)|-1} = 0$$

I.e., iff for all $\ell \le k$, $E(\ell)$ is an equation in Σ, an identity where $\alpha(\ell)$ and $\beta(\ell)$ are the same sequence, the inversion of an earlier equation (from $\alpha=\beta$ to $\beta=\alpha$), or the result of a substitution in earlier equations; and $E(k)$ is of the form $\{2,1,\dots,1,0\} = \{1,\dots,1,0\}$.

In order to provide a more formal definition and to show that the notion so defined is primitive recursive, we make the following p.r. definitions:

(i) $\#(a_0,\dots,a_{n-1}) = 2^{1+a_0} 3^{1+a_1} \cdots p_{n-1}^{1+a_{n-1}}$

$\#$ of empty sequence $(n=0)$ is 1

(ii) $a_\ell = \text{P}\exp_\ell a$

(iii) $Ma = \mu k \{k = a \vee p_k \nmid a\}$

(iv) $Ta = a_{pMa}$

(v) $a \frown b = a \prod_{k<Mb} p_{Ma+k}^{\exp_k b}$

In case a is a sequence number, (ii)-(v) assert that a_ℓ is the ℓ^{th} term of a, Ma the length of a, Ta the last term of a, and $a\frown b$ the concatenation of a and b. The following relations are also p.r.

(vi) e is the number of a sequence

$$Seq(e) \leftrightarrow e = \prod_{k<Me} p_k^{\exp_k e}$$

(vii) e is the number of a proper sequence all of whose terms are $\le r$

$$Seq'(e) \leftrightarrow Seq(e) \wedge e \neq 1 \wedge \bigwedge_{\ell<Me} e_\ell \le r$$

Now we number the variables occurring in Σ by $v_0 = 0$, $v_1 = S$, $v_2 = F$, $v_3, \dots, v_r$. Equations are numbered by

$$\#(v_{a_0} \cdots v_{a_{n-1}} = v_{b_0} \cdots v_{b_{m-1}}) = J(a,b),$$

where $a = \#(a_0,\dots,a_{n-1})$ and $b = \#(b_0,\dots,b_{m-1})$.

Then we may define a p.r. relation Deriv(e) $\leftrightarrow$ e is the number of a derivation from Σ of a value of F_0 by

$$\begin{aligned} \mathrm{Deriv}(e) \leftrightarrow \ & \mathrm{Seq}(e) \wedge \bigwedge_{\ell < Me} \{ \mathrm{Seq}'(Ke_\ell) \wedge \mathrm{Seq}'(Le_\ell) \\ & \wedge [\, e_\ell \in \Sigma \vee Ke_\ell = Le_\ell \vee \bigvee_{s<\ell} e_\ell = J(L,K)e_s \\ & \vee \bigvee_{u,v,<\ell} \bigvee_{c,d \le Ke_v} (Ke_u = c^\frown (ke_v)^\frown d \wedge Le_\ell = Le_u \\ & \qquad \wedge Ke_\ell = c^\frown (Ke_v)^\frown d)\,]\} \\ & \wedge \exp_0 KTe = 2 \wedge \bigwedge_{0<k<PMKTe} \exp_{p_k} KTe = 1 \wedge TKTe = 0 \\ & \wedge \bigwedge_{k<PMLTe} \exp_{p_k} LTe = 1 \wedge TLTe = 0, \end{aligned}$$

where $e_\ell \in \Sigma$ is an abbreviation for the conjunction of terms $e_\ell = f$ for all sequence numbers f of equations in Σ.

Since Deriv(e) is primitive recursive, there exists a primitive recursive function G such that

$$Ge = \begin{cases} 1 & \text{if Deriv}(e) \\ 0 & \text{otherwise} \end{cases}$$

and a function (p.r.) H such that

$$x \in RH \leftrightarrow Gx = 1.$$

Now if e is in fact a derivation of a value of F_0, Te is of the form $FS^m0 = S^n0$. Hence $F_0\, PPMKTH = PMLTH$, and we have shown that every function recursive by Char. II satisfies $F_0 A = B$ for some p.r. A and B. This leads to a third characterization of recursive functions:

Characterization III. A function F is recursive iff there exist p.r. functions A and B with $\bigwedge_x \bigvee_y Ay = x$ and $\bigwedge_{x,y} (Ax = Ay \rightarrow Bx = By)$ such that $FA = B$.

As for the equivalence of the three characterizations, $rec_I \subseteq rec_{II}$ since if Σ has a unique solution, $FS^k0 = S^\ell 0$ is obviously derivable iff $\ell = F_0 k$. $rec_{II} \subseteq rec_{III}$ since, as shown, the relation Deriv (e) is p.r. provided Σ satisfies the conditions of II. Finally, $rec_{III} \subseteq rec_I$ as follows: A and B, being p.r., are rec_I by the preceeding theorem. Let Σ_1 $define_I$ A and Σ_2 $define_I$ B. Then $\Sigma_1, \Sigma_2, FA = B$ $define_I$ B by the conditions imposed on A and B.

Theorem. Every recursive function is arithmetically definable.

Proof: Let $FA = B$ by Char. III. A and B are arithmetically definable as shown, and $Fx = y \leftrightarrow \bigvee_z (Az = x \wedge Bz = y)$.

Problem 12. Let F be the function of one variable such that $FJ(n, x) = F_n x$, where

$$F_0 = 0 \qquad F_{3e+4} = F_{Ke} F_{Le}$$
$$F_1 = S \qquad F_{3e+5} = J(F_{Ke}, F_{Le})$$
$$F_2 = K \qquad \begin{cases} F_{3e+6}\, J(I, 0) = F_{Ke} \\ F_{3e+6}\, J(K, SL) = F_{Le}\, F_{3e+6}. \end{cases}$$
$$F_3 = L$$

Show that F is recursive but not primitive recursive.

<u>Theorem</u>. If a set $\mathcal{S}$ is recursively enumerable and non-empty, then it is the range of a p.r. function.

<u>Proof</u>: By definition, $\mathcal{S}$ is the range of some recursive F. Let A, B be p.r. such that $FA = B$. Then $\mathcal{S} = RF = RB$.

<u>Theorem</u>. $\mathcal{S}$ is recursive iff $\mathcal{S}$ and $\bar{\mathcal{S}}$ are r.e.

<u>Proof</u>: Let $\mathcal{S}$ be recursive with characteristic function G. If $\mathcal{S} = \emptyset$, $\mathcal{S}$ is trivially r.e. Otherwise let $a \in \mathcal{S}$ and set

$$Hu = u \cdot Gu + 0^{Gu} \cdot a.$$

Then $\mathcal{S} = RH$, so that $\mathcal{S}$ is r.e. $\bar{\mathcal{S}}$ is likewise r.e. since it is recursive with characteristic function 0^{G}.

Conversely, let $\mathcal{S} = RA$ and $\bar{\mathcal{S}} = RB$, where A, B are rec. Then $GA = S0$ and $GB = 0$ determine a recursive characteristic function G for $\mathcal{S}$.

Recalling our characterization of r.e. sets, we may define a p.r. predicate asserting the derivability of an element of a r.e. set in a manner similar to the definition of Deriv (e). Let Σ_q be the system of equations consisting of the sequence of equations with number q, provided q is the number of a sequence of equations. We set

$$\mathcal{S}_q = \{k : F\alpha = S^k 0 \text{ is derivable from } \Sigma_q \text{ for some } \alpha\},$$

in case q is a sequence number,

$$\mathcal{S}_0 = \{0\}$$

$$\mathcal{S}_q = \emptyset \quad \text{otherwise.}$$

The parameter r now depends upon q, so that we redefine Seq′ by

$$Seq'(q, e) \leftrightarrow Seq(e) \wedge e \neq 1 \wedge Seq(q) \wedge$$
$$\wedge \bigwedge_{\ell \leq Me} \bigvee_{s < Mq} \left(\bigvee_{u < MKq_s} e_\ell = (Kq_s)_u \vee \bigvee_{u < MLq_s} e_\ell = (Lq_s)_u \right)$$

Now we can define the p.r. relation that e is the number of a derivation from Σ_q of a member of $\mathcal{S}_q$ by

$$\mathrm{Deriv}(q,e) \leftrightarrow \mathrm{Seq}(q) \wedge \mathrm{Seq}(e) \wedge \bigwedge_{\ell < \eta e} \{ \mathrm{Seq}'(q, Ke_\ell) \wedge \mathrm{Seq}'(q, Le_\ell) \wedge \dots \} \wedge \exp_0 KTe = 2 \wedge \bigwedge_{k < PMLTe} \exp_k Te = 1 \wedge TLTe = 0,$$

where the remainder of the term in $\{\dots\}$ is as before. Let H be the p.r. function of two variables such that

$$H(e,q) = \begin{cases} 1 & \text{if } \mathrm{Deriv}(q,e) \\ 0 & \text{otherwise,} \end{cases}$$

and let $U = J(H(K,L)\cdot L,\ H(K,L)\cdot PMLTK)$.
Then if e is a derivation of $x \in \mathcal{S}_q$,

$$UJ(e,q) = J(q,x),$$

and if e is not a derivation from Σ_q,

$$UJ(e,q) = J(0,0).$$

Hence $J(q,x) \in RU$ iff $x \in \mathcal{S}_q$, or equivalently,
$x \in \mathcal{S}_q \leftrightarrow \bigvee_{\ell} U\ell = J(q,x)$.

The function U allows us to construct a p.r. function with range $\mathcal{S}_q$ in case q is the number of a non-empty set. For if $a \in \mathcal{S}_q$,

$$0^{|KUz - q|}\cdot LUz + 0^{0^{|KUz-q|}}\cdot a$$

has range $\mathcal{S}_q$.

We are now able to demonstrate that $RE \subset R$; i.e., that there is a r.e. set which is not recursive. Let $\mathcal{U} = \{q : q \in \mathcal{S}_q\}$. Then $\mathcal{U} = R\ 0^{|UK - J(L,L)|}\cdot L$, so that $\mathcal{U}$ is r.e. But $\bar{\mathcal{U}} = \{q : q \notin \mathcal{S}_q\}$ cannot be r.e., for if $\bar{\mathcal{U}} = \mathcal{S}_k$,

$$k \in \mathcal{S}_k \leftrightarrow k \notin \mathcal{S}_k$$

which is a contradiction.

The set $\mathfrak{U}$ also serves to demonstrate that arithmetic is not decidable, since there exists a formula $\varnothing$ such that $x \in \mathfrak{U} \leftrightarrow \varnothing(x)$, and hence if there were a decision procedure for arithmetic, $\mathfrak{U}$ would be recursive.

Word Problem for Semi-groups

Axel Thue (1914) proposed the problem of determining a decision procedure for the derivability of functional equations from a given set of equations. The problem was shown to be recursively unsolvable in 1947 independently by Post (using Türing machines) and Markov (using Post normal form). The result is easily obtained from our formalization of recursive functions:

Let F be a recursive function such that $\mathcal{R}F$ is not recursive, and let Σ be a system of functional equations defining$_I$ F. Let $\Sigma' = \Sigma \cup \{GF = 0\}$, where G is a function symbol not occurring in Σ. Then the equation $GS^k = 0$ can be derived from Σ' iff $k \in \mathcal{R}F$. Hence if the word problem were recursively solvable, $\mathcal{R}F$ would be recursive, contrary to our assumption.

The generalization of the word problem to groups (where cancellation is allowed as a method of derivation: $\bigwedge_B \bigvee_{B'} (BB' = B'B = I)$) has been shown to be recursively unsolvable by Novikoff.

Another related problem concerns the existence of a decision procedure for determining when a given system of equations has a solution. Again the answer is negative, for if

$$\Sigma' = \Sigma \cup \{ GF = 0, \ GS^k0 = S0 \},$$

then Σ' has a solution iff $k \notin \mathcal{R}F$. Hence a decision procedure would imply that $\mathcal{R}F$ is recursive.

<u>Characterization</u> <u>IV</u>. A function F is recursive iff there exist primitive recursive functions A, B such that $\bigwedge_x \bigvee_y Ay = x$ and $Fx = B\mu y\{Ay = x\}$.

<u>Proof</u>: Obviously $\text{rec}_{III} \subseteq \text{rec}_{IV}$. The converse is established by using an ι rule: $\iota x\{\Phi(x)\}$ is the unique x such that $\Phi(x)$ holds. Now if $Gx = \mu y\{Ay = x\}$, then

$$Gx = \iota y\{Ay = x \wedge \sum_{z<y} 0^{|Az-x|} = 0\}$$

$$= \iota y\{|Ay - x| + \sum_{z<y} 0^{|Az-x|} = 0\}$$

$$= \iota y\{A_1(x,y) = 0\}.$$

Let C be the p.r. function $Cz = \text{sgn}\, A_1(Kz, Lz)$. Then $Gx = L\iota z\{Cz = 0 \wedge Kz = x\}$. We define

$$M(2z) = \begin{cases} 2Kz & \text{if } Cz = 0 \\ 2\sum_{u\le z} Cu + 2z - 1 & \text{if } Cz \neq 0 \end{cases}$$

$$M(2z+1) = 2\sum_{u\le z} Cu + 2z + 1.$$

M is a p.r. permutation since $\bigwedge_x \dot{\bigvee_y} A_1(x,y) = 0$, which insures that the even numbers are covered, while the odd numbers are covered in order by the counting functions $2\sum_{u\le z} Cu + 2z \pm 1$. Now if $Hx = [\frac{x}{2}]$, then

$$Gx = LHM^{-1}Dx$$

since M codes the pairs (x,y) for which $A_1(x,y) = 0$ into the even integers. G is recursive since L, H, M, D are p.r., and M^{-1} may be computed from $M^{-1}M = I$. Hence

$$Fx = BGx$$

is also recursive.

As a corollary to the preceeding proof, we have still another characterization:

<u>Characterization V</u>. F is recursive iff there exist p. r. A, B, C such that B is a permutation and $F = AB^{-1}C$.

Note that while the inverse of a recursive permutation is recursive, the inverse of a p.r. permutation is not necessarily p. r.

<u>Question</u>: Is the group of recursive functions generated by all p.r. permutations identical to the group of recursive permutations?

<u>Separability</u>

<u>Definition</u>. Two sets A and B are <u>recursively separable</u> iff there exists a recursive set C such that $A \subseteq C$ and $B \cap C = \phi$.

<u>Problem 13</u>. Show that there exist r.e. sets A, B which are not recursive but are recursively separable.

<u>Theorem</u>. There exist r.e. sets A, B which are not recursively separable.

<u>Proof</u>: Let F be the function of Problem 12 such that $F_n x = FJ(n, x)$ is an enumeration of all p.r. functions. We define a rec. enumeration of all univalent p.r. functions as follows:

$$GJ(n,x) = \begin{cases} J(n, FJ(n,x)) & \text{if } \neg \bigvee_{u<v\leq x} FJ(n,u) = FJ(n,v) \\ J(n, \max_{u<x} LGJ(n,u)+1) & \text{otherwise} \end{cases}$$

G is univalent and recursive, and the functions LG_n are precisely the p.r. univalent functions.

<u>Lemma</u>. If $\mathcal{A}, \mathcal{B}$ are disjoint r.e. sets, then there exists an n such that

$$x \in \mathcal{A} \leftrightarrow J(n, 2x) \in RG_nD$$
$$x \in \mathcal{B} \leftrightarrow J(n, 2x) \in RG_nSD.$$

<u>Proof</u>: Let $\mathcal{A} = RA$, $\mathcal{B} = RB$. If $\mathcal{A}$ and $\mathcal{B}$ are non-empty, we define a univalent p.r. fct M by

$$MDx = \begin{cases} DAx & \text{if } \bigwedge_{u<x} Au \neq Ax \\ SDDx & \text{otherwise} \end{cases}$$

$$MSDx = \begin{cases} DBx & \text{if } \bigwedge_{u<x} Bu \neq Bx \\ S^3D^2x & \text{otherwise.} \end{cases}$$

Then $M = LG_n$ for some n. The obvious modifications are made if $\mathcal{A}$ or $\mathcal{B}$ is empty.

Now let $\mathcal{S} = RGJ(K, DL)$, $\mathcal{T} = RGJ(K, SDL)$. Since G is p.r. univalent, $\mathcal{S}$ and $\mathcal{T}$ are disjoint r.e. sets. Suppose there exists a recursive $\mathcal{U}$ with $\mathcal{S} \subset \mathcal{U}$ and $\mathcal{T} \cap \mathcal{U} = \emptyset$. Define $x \in \mathcal{U}_n \leftrightarrow J(n, 2x) \in \mathcal{U}$. The $\mathcal{U}_n$ list all rec. sets: $\mathcal{U}_n$ is recursive since $\mathcal{U}$ is, and by the above lemma, if $\mathcal{A}$ is recursive, there exists an n such that

$$x \in \mathcal{A} \leftrightarrow J(n, 2x) \in RG_nD \rightarrow J(n, 2x) \in \mathcal{S}$$
$$x \notin \mathcal{A} \leftrightarrow J(n, 2x) \in RG_nSD \rightarrow J(n, 2x) \in \mathcal{T}.$$

A contradiction is reached by the usual diagonal argument. Set $\mathcal{V} = \{n : n \notin \mathcal{U}_n\}$. $\mathcal{V}$ is recursive, and if $\mathcal{V} = \mathcal{U}_n$, then $n \in \mathcal{V} \leftrightarrow n \notin \mathcal{V}$. Hence $\mathcal{S}$ and $\mathcal{T}$ must not be recursively separable.

The notion of recursive separability is of importance in questions of decidability. In any reasonable theory, the set of theorems is r.e., as is the set of invalid sentences. If these two sets can be shown to be non-recursively separable, then it follows that the theory is undecidable (since the set of theorems is not recursive) and furthermore that no extension of the axioms will give a decidable theory.

In the preceeding theorem, we showed that the class of recursive sets is not itself recursive. However it is r.e., as will follow from the next two lemmas:

<u>Lemma</u>. Every non-empty recursive set is the range of a non-decreasing recursive function, and conversely, the range of every non-decreasing rec. fct. is a recursive set.

<u>Proof</u>: Let $\mathcal{S}$ be a non-empty recursive set with $x \in \mathcal{S} \leftrightarrow Fx = 1$. Define

$$G0 = \mu y \{ Fy = 1 \}$$

$$GSx = \begin{cases} Sx & \text{if } FSx = 1 \\ Gx & \text{otherwise.} \end{cases}$$

Then G is a non-decreasing recursive function with $\mathcal{S} = \mathcal{R}G$.

Conversely, if F is non-decreasing and $\mathcal{R}F$ is finite, then $\mathcal{R}F$ is obviously recursive. If $\mathcal{R}F$ is infinite, then

$$Gy = 0^{|y - F\mu x\{Fx \geq y\}|}$$

is a recursive characteristic function for $\mathcal{R}F$.

We cannot list all non-decreasing recursive functions (give diagonal argument), but we can list all non-decreasing p.r. functions by

$$G_n x = GJ(n,x) = \max_{u \le x} F_n u.$$

Hence by the following lemma, the class of recursive sets is the class of sets RG_n:

<u>Lemma</u> To every recursive function F corresponds a p.r. function G such that RF = RG and G assumes its values in the same order as F.

<u>Proof</u>: Let $Hx = J(x, Fx)$ and let M be p.r. with the same range as H. Then MK is p.r. and assumes each value of H infinitely often. Let

$$N0 = J(0, F0)$$

$$NSu = \begin{cases} Nu & \text{if } KMKu \neq SKNu \\ MKu & \text{otherwise.} \end{cases}$$

N lists the pairs $J(x, Fx)$ in order, so that $G = LN$ is the required function.

<u>Problem 14</u>. Show that every infinite r.e. set is the range of a recursive univalent function, but is not necessarily the range of a p.r. univalent function.

<u>Problem 15</u>. Find an arithmetically definable function H such that H_n runs through exactly the recursive functions of one variable.

Summary

We have now established the inclusions $HA \overset{(i)}{\supset} AD \overset{(ii)}{\supset} GR \overset{(iii)}{\supset} PR$ for functions. The proper inclusions were demonstrated by

(i) the satisfaction function W

(ii) the function H of Problem 15

(iii) the function F of Problem 12.

For sets, we have $HA \supset AD \supset RE \supset GR \supset PR$. Each proper inclusion may be demonstrated by means of a universal set

$$J(n,x) \in \mathcal{S} \leftrightarrow x \in \mathcal{S}_n$$

where $\mathcal{S}$ is definable on one level and $\mathcal{S}_n$ runs through all sets of the next lower level. $\mathcal{S}$ cannot belong to this lower level since then a diagonal argument would give a contradiction. E.g., $GR \subset RE$ since the class of recursive sets is r.e., but not recursive. $PR \subset GR$ since $0^{F_n(n)}$ is a recursive characteristic function, but not p.r. The set $\mathcal{U} = \{q : q \notin \mathcal{S}_q\}$ is AD but not RE, and the set of numbers of true sentences is HA but not AD.

<u>Problem</u> 16. Show that there is a recursive permutation F which is not equal to $AB^{-1}C$ for any p.r. permutations A, B, C.

Can this be generalized to answer the question raised previously about the group generated by the p.r. permutations?

<u>Hint</u>: List all triples of p.r. fcts by $A_n = F_{Kn}$, $B_n = F_{KLn}$, $C_n = F_{LLn}$, and define a rec. permutation G such that $Gn \neq A_n B_n^{-1} C_n(n)$ in case A_n, B_n, C_n are permutations by

$$Gn = \begin{cases} A_n \mu q\{(\bigwedge_{w<n} Gw \neq A_n q \wedge B_n q \neq C_n n) \vee q = n+2\} \\ \qquad \text{provided } \bigwedge_{w_1<w_2<n+2} (A_n w_1 \neq A_n w_2 \wedge B_n w_1 \neq B_n w_2) \\ \mu x\{\bigwedge_{w<n} Gw \neq x\} \quad \text{otherwise} \end{cases}$$

Davis Normal Form

Theorem. A relation R is r.e. iff there is a polynomial P with integer coefficients such that $R\underline{x} \leftrightarrow \bigvee_y \bigwedge_{z \le y} \bigvee_{u_1 \dots u_k} P(\underline{x}, y, z, u_1, \dots, u_k) = 0.$

Lemma. Every p.r. function is definable (arithmetically) by a predicate of the form $Q_1 \dots Q_n \Phi$, where Φ is diophantine and $Q_1 \dots Q_n$ are either existential or bounded universal quantifiers.

Proof: Recall that every p.r. function of one variable is definable from $0, S, K, L$ by the operations

$$F = AB \qquad \begin{cases} FJ(I,0) = A \\ FJ(K, SL) = BF. \end{cases}$$
$$F = J(A,B)$$

Define $T_n x = R(Kx, 1 + (n+1)Lx)$. $T_n x = y$ is a diophantine relation since

$$T_n x = y \leftrightarrow \bigvee_u \{Kx = [1 + (n+1)Lx]u + y \ \wedge \ y \le (n+1)Lx\}$$

$$\leftrightarrow \bigvee_{u,v,w,z} \{ w = [1 + (n+1)z]u + y \ \wedge \ y + v = (n+1)z \ \wedge \ (w+z)^2 + 3w + z = 2x\}$$

$0, S, K, L$ are all definable by diophantine predicates.

$$ABx = y \leftrightarrow \bigvee_u (Bx = u \ \wedge \ Au = y)$$
$$J(A,B)x = y \leftrightarrow \bigvee_{u,v} (Ax = u \ \wedge \ Bx = v \ \wedge \ (u+v)^2 + 3u + v = 2y),$$

both of which are of the required form if A and B are definable by suitable predicates. Finally,

$$FJ(x,y) = z \leftrightarrow \bigvee_u \{T_0 u = Ax \ \wedge \ \bigwedge_{v \le y} (T_{Sv} u = BT_v u) \ \wedge \ z = T_y u\}$$

which again is of the proper form after all quantifiers have been moved to the front.

Recursively enumerable sets are expressible by a predicate of the form $\bigvee_y \Phi$, where $\Phi = Q_1 \dots Q_n \Phi'$ as in the lemma: if $\mathcal{S}$ is empty, $x \in \mathcal{S} \leftrightarrow \bigvee_y 1 = 0$; if $\mathcal{S} = RF$ for some p.r. F, then $x \in \mathcal{S} \leftrightarrow \bigvee_y Fy = x$. Now by induction on the number of quantifiers in $\Phi = \bigvee_y Q_1 \dots Q_n \Phi'$, we show that Φ is equivalent to a predicate of the form required: i.e., $\Phi \leftrightarrow \bigvee_y \bigwedge_{z \le y} \Phi''$, where Φ'' is diophantine.

Φ' is diophantine by definition. Let r, s be variables not occurring in Φ. Then $\Phi \leftrightarrow \bigvee_y Q_1 \dots Q_n \bigvee_r \bigwedge_{s \le r} \Phi'$. The proof is completed by showing that each of the quantifiers $\bigvee_y$, $Q_1, \dots, Q_n$ can be "absorbed."

(i) Let $C(\underline{x}, u, y, z)$ be diophantine. Then

$$\bigvee_z \bigvee_y \bigwedge_{u \le y} C(\underline{x}, u, y, z) \leftrightarrow \bigvee_w \bigwedge_{u \le Kw} C(\underline{x}, u, Kw, Lw)$$

$$\leftrightarrow \bigvee_w \bigwedge_{u \le w} \{ C(\underline{x}, u, Kw, Lw) \vee u > Kw \}.$$

Since the expression in $\{ \}$ is diophantine, the quantifier $\bigvee_z$ has been absorbed.

(ii) For bounded universal quantifiers, we need an intermediate result. Let $C(\underline{x}, u, v, y, z)$ be diophantine.

$$\bigvee_y \bigwedge_{v \le z} \bigwedge_{u \le y} C(\underline{x}, u, v, y, z) \leftrightarrow \bigvee_w \bigwedge_{\ell \le w} \{ [C(\underline{x}, K\ell, L\ell, Kw, Lw) \vee K\ell > Kw \vee L\ell > Lw] \wedge Lw = z \}$$

Now

$$\bigwedge_{u \le z} \bigvee_y \bigwedge_{v \le y} C(\underline{x}, u, v, y, z) \leftrightarrow \bigvee_w \bigwedge_{u \le z} \bigwedge_{v \le w} \{ C(\underline{x}, u, v, T_u w, z) \vee v > T_u w \}$$

I.e., the quantifiers $\bigwedge_{u \le z} \bigvee_y$ are interchanged by having w be the number of a sequence of the appropriate y's for each $u \le z$. By these two equivalences, the quantifier $\bigwedge_{u \le z}$ may be absorbed.

This completes the proof of the theorem.

A stronger version of the Davis normal form holds in which all but the first quantifier are bounded:

$$\bigvee_{y} \bigwedge_{z \le y} \bigvee_{u_1 \dots u_k} \{ P(\underline{x}, y, z, u_1, \dots, u_k) = 0$$

$$\leftrightarrow \bigvee_{w} \bigwedge_{z \le w} \bigvee_{u_1 \dots u_k \le w} \{ P(\underline{x}, kw, z, u_1, \dots, u_k) = 0 \ \vee \ z > kw \}$$

$$\leftrightarrow \bigvee_{w} \bigwedge_{z \le w} \bigvee_{u_1 \dots u_k \le w} \bigvee_{q, y, v \le w} \{ (y+v)^2 + 3y + v = 2w \ \wedge \ [P(\underline{x}, y, z, u_1, \dots, u_k) = 0 \vee z = y+1+q] \}.$$

Hence any r.e. relation is arithmetically definable by a predicate of the form

$$\bigvee_{w} \bigwedge_{z \le w} \bigvee_{u_1 \dots u_k \le w} P(\underline{x}, w, z, u_1, \dots, u_k) = 0.$$

As for the number of auxiliary variables $u_1 \dots u_k$ required, it is known that four are sufficient, but that one is not.

Turing Machines

The first expositions on the theory of functions computable by Turing machines were by Turing in the Proc. of the London Math. Society (1936-37) and Post, JSL (1936).

We shall consider a Turing machine which operates on a tape infinitely long to the right.

Each square of the tape is either printed (a) or blank (b). The machine scans one square of the tape at a time, and its action depends upon its internal state plus the symbol scanned. Four actions are possible: print (P), erase (E), move left (L), move right (R). (Note that R means the machine moves right, or, equivalently, the tape moves left.)

A machine with k active states 0, 1, ..., k-1 and one terminal state ∞ will be called a machine of rank k. The machine is started in state 0 with a given input tape, and its actions are then determined by a table of instructions: E.g., consider the machine $\mathfrak{A}$ of rank 1

$\mathfrak{A}$	a	b
0	R0	P∞

If $\mathfrak{A}$ scans a printed square, it moves right and stays in state 0; if it scans a blank square, it prints and enters its terminal state.

The action of a machine may be described by listing the tape configuration following each atomic act. The symbols on the tape (or relevant portion of the tape) are listed; e.g., aababbb..., or more concisely, a^2bab^∞. The scanned square and internal state are indicated by a symbol q_i to the right of the scanned square; e.g., $a^2babq_0b^\infty$. The action of the machine $\mathcal{A}$ may be described by

$$\mathcal{A}: \; bq_0 \to aq_\infty$$

$$aq_0a^mb \to a^{m+2}q_\infty$$

I.e., $\mathcal{A}$ prints the first blank square to the right.

In the description of a machine by listing configurations, the subscripts $0, \infty$ will often be omitted, it being understood that the q to the left of the $\to$ sign is q_0, and the q to the right q_∞. (The machines being introduced in this exposition will eventually be used to show that all recursive functions are computable on Turing machines).

<u>Exercise</u> List the successive tape configurations for the machine

$\mathcal{B}$	a	b
0	L0	L1
1	R2	R4
2	R3	R3
3	R3	L∞
4	P5	P5
5	R5	L6
6	E6	L0

starting with input tape $abbaaq_0b$. Show that $\mathcal{B}$ "closes the gap" preceeding a scanned block of printed squares:

$$\mathcal{B}: \; ab^{m+1}a^{n+1}qb \to aba^{n+1}qb^{m+1}$$

Two Turing machines may be "composed" to form a new machine via the following procedure: if $\mathcal{X}$ is a machine of rank r and $\mathcal{Y}$ of rank s, then the table for the machine $\mathcal{X}\mathcal{Y}$ is obtained by changing ∞ to r in the table for $\mathcal{X}$ and adding r to the number of each state in the table for $\mathcal{Y}$. E.g., let

$$\mathcal{C}: \; aqb^2 \to abaq$$

$\mathcal{C}$	a	b
0	R0	R1
1	-	P∞

$\mathcal{D}: ab^{m+1}a^n q \to aqb^{m+1}a^n$

$\mathcal{D}$	a	b
0	L0	L1
1	P∞	L1

Then $\mathcal{C}\mathcal{D}: aqb^2 \to aqba$

$\mathcal{C}\mathcal{D}$	a	b
0	R0	R1
1	–	P2
2	L2	L3
3	P∞	L3

As a particular case of composition, we may define powers of one machine: $\mathcal{A}^2 = \mathcal{A}\mathcal{A}$, e.g., prints the first two blank squares to the right. The "infinite" power is denoted by [ ]. E.g.,

[$\mathcal{A}$]	a	b
0	R0	P0.

[$\mathcal{A}$] is of little interest since the machine does not stop, but the infinite power will prove useful in connection with two terminal machines, to be defined later. To form the table for [X], change ∞ to 0 in the table for X.

A two terminal machine has two terminal states: ∞ and ∞'. E.g.,

$\mathcal{E}: baq \to baq_\infty$

$aaq \to aaq_{\infty'}$

$\mathcal{E}$	a	b
0	L1	–
1	R∞'	R∞

Two terminal machines may also be composed. If X is a two-terminal machine of rank r and Y, Z are one terminal machines of ranks s, t, then YX is a two terminal machine and $X\{{Y \atop Z}\}$ is the two terminal machine whose table is given by changing ∞ to r in the table for X, ~~adding~~ ∞' to r+s, adding r to the states in the table for Y, and adding r+s to the states in the table for Z. E.g.,

$\mathcal{E}\{\mathcal{C}^{\mathcal{A}}$: $baqb \to baaq$
$aaqb^2 \to aabaq$

	a	b
0	L1	-
1	R3	R2
2	R2	P∞
3	R3	R4
4	-	P∞

The [ ] notation may now be used in situations like

$$[X\{^{Y]}_{Z},$$

whose table is formed from the table for $X\{^Y_Z$ by changing ∞ in the table for Y to 0.

We need three more basic machines:

$\mathcal{F}$: $aaq \to aqb$
$baq \to bqb$

$\mathcal{F}$	a	b
0	E0	L∞

$\mathcal{G}$: $aqb^m a^{n+1} b \to ab^m a^{n+1} qb$

$\mathcal{G}$	a	b
0	R1	R1
1	R2	R1
2	R2	L∞

$\mathcal{H}$: $aqb^{m+1}a \to a^{m+1}qba$

$\mathcal{H}$	a	b
0	R1	-
1	L2	P0
2	E2	L∞

In summary, the basic machines act as follows:

$\mathcal{A}$: prints the first blank to the right
$\mathcal{B}$: moves printed block left to close gap
$\mathcal{C}$: starts new block of one square to the right
$\mathcal{D}$: moves to the end of preceeding printed block
$\mathcal{E}$: discriminates between ba and aa
$\mathcal{F}$: erases and moves left
$\mathcal{G}$: moves right and continues to end of next block
$\mathcal{H}$: fills in gap to the right

In order to have a Turing machine compute a function, we encode the n-tuple $(k_1, \dots, k_n)$ on tape by

$$b a^{k_1+1} b \dots b a^{k_n+1} q b^\infty.$$

Then $F(x_1, \dots, x_n)$ is <u>computable</u> by a machine $\mathfrak{M}_F$ iff $\mathfrak{M}_F$ has the action

$$(x_1, \dots, x_n) \to (F(x_1, \dots, x_n))$$

for all n-tuples of natural numbers.

We now define two "book-keeping" machines. The machine $\mathfrak{U}_m$ has the action

$$(k_1, \dots, k_m) \to (k_1, \dots, k_m, k_1)$$

and is defined by

$$\mathfrak{U}_m = \mathfrak{C} [\mathfrak{D}^m \mathfrak{E} \left\{ \begin{matrix} \mathfrak{H} \mathfrak{G}^m \\ \mathfrak{R} \mathfrak{G}^m \mathfrak{A} \end{matrix} \right.].$$

$\mathfrak{U}_m$ acts as follows: $\mathfrak{C}$ takes the tape $(k_1, \dots, k_m)$ into $(k_1, \dots, k_m, 0)$. $\mathfrak{D}^m$ causes the machine to scan the last digit of k_1. If k_1 is not 0, then $\mathfrak{R}$ subtracts 1 from k_1, $\mathfrak{G}^m$ moves the machine to the end of the tape, and $\mathfrak{A}$ adds 1 to 0 giving $(k_1 - 1, \dots, k_m, 1)$ with an extra blank between $k_1 - 1$ and k_2. This cycle is repeated, each time erasing a symbol from the block k_1 and adding one to the last block. When k_1 is finally reduced to zero, $\mathfrak{H}$ restores k_1 and $\mathfrak{G}^m$ moves the machine to the end of the tape giving $(k_1, \dots, k_m, k_1)$.

Next we define "erasing" machines $\mathfrak{J}_i$.

$\mathfrak{J}_1 : (k_0, k_1) \to (k_0)$

$$\mathfrak{J}_1 = [\mathfrak{E} \left\{ \begin{matrix} \mathfrak{R} \mathfrak{D} \\ \mathfrak{R} \end{matrix} \right.]$$

$$m \geq 2, \quad \mathfrak{J}_m : (k_0, k_1, \dots, k_m) \to (k_0, k_2, \dots, k_m)$$
$$(k_1, \dots, k_m) \to (k_2, \dots, k_m)$$

A first try at defining $\mathfrak{J}_m$ might be $\mathfrak{D}^{m-1} [\mathfrak{E} \left\{ \begin{matrix} \mathfrak{R} \\ \mathfrak{R} \end{matrix} \right.] (\mathfrak{G} \mathfrak{B})^{m-1}$ which goes back and erases the mth block from the end and then closes the gap left. However if there are only m blocks on the tape, trying to close the first gap will cause the tape to fall out of the machine. Hence we use the definition

$$\mathfrak{J}_m: \ \mathfrak{D}^{m-1}\,[\,\mathfrak{E}\begin{cases}\mathfrak{G}\mathfrak{B}\mathfrak{D}\mathfrak{A}\mathfrak{G}\mathfrak{R}^{2}(\mathfrak{G}\mathfrak{B})^{m-2}\\ \mathfrak{R}\,].\end{cases}$$

$\mathfrak{J}_m$ acts by erasing all but one symbol from the m^{th} block from the end and then performing

$$\begin{aligned} ba q b^m a^n b &\xrightarrow{\mathfrak{G}} bab^m a^n q b \xrightarrow{\mathfrak{B}} baba^n q b^m \\ &\xrightarrow{\mathfrak{D}} baqba^n b^m \xrightarrow{\mathfrak{A}} baaqa^n b^m \\ &\xrightarrow{\mathfrak{G}} ba^{n+2} q b^m \xrightarrow{\mathfrak{R}^2} ba^n q b^{m+2} \end{aligned}$$

and then closing all later gaps.

A machine $\mathfrak{P}$ to add may be defined by

$$\mathfrak{P}: \ (x,y) \rightarrow (x+y)$$
$$\mathfrak{P} = \mathfrak{D}\mathfrak{A}\mathfrak{G}\mathfrak{R}^{2}$$

I.e., $\mathfrak{P}$ overprints the blank between x and y and erases two squares from the end of the tape: $ba^{x+1}ba^{y+1}b \rightarrow ba^{x+1}aa^{y+1}b = ba^{x+y+3}b \rightarrow ba^{x+y+1}b.$

The "inverse" of addition $- \dot{-} -$ is computable by the machine

$$Q: \ (x,y) \rightarrow \begin{cases} (x-y,\,0) & \text{if } x \geq y \\ (0,\,y-x) & \text{if } y \geq x \end{cases}$$

$$Q = [\,\mathfrak{E}\begin{cases} \\ \mathfrak{R}\mathfrak{D}\mathfrak{E}\begin{cases}\mathfrak{G}\mathfrak{A} \\ \mathfrak{R}\mathfrak{G}\mathfrak{B}\,]\end{cases}\end{cases}$$

Q erases one symbol alternately from x and y until one of the two numbers is zero.

Combining $\mathfrak{P}$ and Q, the absolute value of the difference of two numbers may be computed by

$$Q\mathfrak{P}: \ (x,y) \rightarrow (|x-y|).$$

<u>Theorem</u>. All recursive functions are computable.

<u>Proof</u>: By characterization V, it suffices to show that all p.r. fcts. of one variable are computable and that the inverses of computable permutations are computable. Also from an earlier result, it suffices to show that O, S, K, L are computable, and that if A, B are computable, then so is F defined by

$$F = AB$$
$$F = J(A, B)$$
$$\text{or} \quad \begin{cases} FJ(I, O) = A \\ FJ(K, SL) = BF, \end{cases}$$

and if B is onto, then $B^{-1}x = \mu y\{By = x\}$ is computable.

Now $\mathfrak{M}_O : (x) \to (0)$ is the machine $[\mathcal{E}\{\mathcal{D}_1]$. $\mathfrak{M}_S$ is simply the machine $\mathcal{A} : (x) \to (x+1)$.

To compute the Cantor pairing functions, we define the k^{th} triangular number

$$T_k = \sum_{j=1}^{k} j = \frac{k(k+1)}{2} = T_{k-1} + k$$

and note that

$$J(x, y) = T_{x+y} + x.$$

Kz is thus the excess over a triangular number and is computed by

$$\mathfrak{M}_K : \mathcal{C}[\mathcal{A}\,\mathcal{L}_2^2\,\mathcal{Q}\,\mathcal{E}\begin{cases}\mathcal{D}_1\,\mathcal{L}_2\,\mathcal{D}_3^2\,] \\ \mathcal{D}_1^3\end{cases}$$

I.e., $(x) \xrightarrow{\mathcal{C}} (x, 0) = (x - T_0, 0)$ and

$$\begin{aligned}
\rightarrow (x - T_k, k) &\xrightarrow{\mathcal{A}} (x - T_k, k+1) \xrightarrow{\mathcal{L}_1^2} (x - T_k, k+1, x - T_k, k+1) \\
&\xrightarrow{\mathcal{Q}} (x - T_k, k+1, x - T_{k+1}, 0) \qquad \text{if } x \geq k+1 + T_k = T_{k+1} \\
&\xrightarrow{\mathcal{D}_1\mathcal{L}_1\mathcal{D}_1^5} (x - T_{k+1}, k+1)\ ] \\
&\xrightarrow{\mathcal{Q}} (x - T_k, k+1, 0, T_{k+1} - x) \qquad \text{if } x < T_{k+1} \\
&\xrightarrow{\mathcal{D}_1^3} (x - T_k)
\end{aligned}$$

which is the desired result.

<u>Problem</u> 17. Find Turing machines $\mathcal{M}_L$ and $\mathcal{M}_{J(A,B)}$ given $\mathcal{M}_A$ and $\mathcal{M}_B$.

For $\mathcal{M}_L$, note that $J(x,y) = T_{x+y} + x = T_{x+y+1} - (x+y+1) + x$ and hence $y = T_{x+y+1} - J(x,y) - 1$. From the above computation for $\mathcal{M}_K$, we see immediately that

$$\mathcal{M}_L : \mathcal{C}[\mathcal{A}\,\mathcal{U}_2^2\,\mathcal{Q}\,\mathcal{E}\begin{cases}\mathcal{J}_1\,\mathcal{U}_2\,\mathcal{J}_3^2 \\ \mathcal{R}\,\mathcal{J}_2^3\end{cases}]$$

For $\mathcal{M}_{J(A,B)}$ we first define a machine $\mathcal{T}$ to compute T_k by

$$\mathcal{T} : \mathcal{U}_1[\mathcal{D}\mathcal{E}\begin{cases}\mathcal{S}\,\mathcal{J}_2 \\ \mathcal{R}\,\mathcal{S}\,\mathcal{B}\,\mathcal{U}_2\,\mathcal{P}\end{cases}]$$

I.e., $(k) \overset{\mathcal{U}_1}{\to} (k,k)$ and $(j,x) \to (j-1, x+j-1)$ if $j \neq 0$ in the loop. $\mathcal{M}_{J(A,B)}$ is then given by

$$\mathcal{M}_{J(A,B)} : \mathcal{U}_1\,\mathcal{M}_A\,\mathcal{U}_2\,\mathcal{M}_B\,\mathcal{J}_3\,\mathcal{U}_2\,\mathcal{P}\,\mathcal{T}\,\mathcal{P}$$

$$\mathcal{M}_{AB} : \mathcal{M}_B\,\mathcal{M}_A$$

If A and B are computable and $FJ(I,0) = A$, $FJ(K,SL) = BF$, then

$$\mathcal{M}_F : \mathcal{U}_1\,\mathcal{M}_L\,\mathcal{U}_2\,\mathcal{M}_K\,\mathcal{J}_3\,\mathcal{M}_A[\mathcal{D}\mathcal{E}\begin{cases}\mathcal{S}\,\mathcal{J}^2 \\ \mathcal{R}\,\mathcal{S}\,\mathcal{B}\,\mathcal{M}_B\end{cases}]$$

I.e., $(x) \to (x,x) \to (x, Lx) \to (x, Lx, x) \to (x, Lx, Kx) \to$ ~~(Lx, Kx)~~
$\to (Lx, Kx) \to (Lx, AKx) \to (Lx-1, BAKx)$
$\to \dots \to (0, B^{Lx}AKx) \to (Fx)$.

Finally, if B is onto,

$$\mathcal{M}_{B^{-1}} : \mathcal{C}[\mathcal{U}_2^2\,\mathcal{M}_B\,\mathcal{Q}\,\mathcal{P}\,\mathcal{E}\begin{cases}\mathcal{J}_1\,\mathcal{J}_2 \\ \mathcal{J}_1\,\mathcal{A}\end{cases}]$$

I.e., $(x) \overset{\mathcal{C}}{\to} (x,0) \overset{\mathcal{U}_2^2}{\to} (x,0,x,0) \overset{\mathcal{M}_B}{\to} (x,0,x,B0) \overset{\mathcal{Q}\mathcal{P}}{\to} (x,0,|x-B0|)$
$\to (0)$ if $|x-B0| = 0$
$\to (x,1)$ if $|x-B0| \neq 0$ and cycles until a y is found for which $|x-By| = 0$.

The same result also holds for recursive functions of more than one variable. E.g., a function F of two variables is defined by

$$F(x,y) = F' J(x,y)$$

for some recursive function F'. Then $F' = F(K, L)$ and $\mathfrak{M}_F = \mathfrak{M}_J \mathfrak{M}_{F'}$: $(x,y) \to (J(x,y)) \to (F' J(x,y))$.

The converse of the theorem also holds, so that the recursive functions are identical with the computable functions.

<u>Problem</u> 18. Show that every function computable by some Turing machine is recursive.

<u>Hint</u>: Define the weight of a square of tape by

Space Content	Weight
b	0
a	1
bq_i	$2i+2$
aq_i	$2i+3$

The state of the tape may then be represented by a finite sequence of weights or by $p_0^{w_0} p_1^{w_1} \cdots p_\ell^{w_\ell}$. In writing the table for a machine of rank r, replace ∞ by r.

Universal Turing Machines

Turing showed the existence of a universal machine $\mathfrak{U}$ which, given the input (n, x), computed the action of the n^{th} Turing machine (in some fixed enumeration) with input (x). We shall prove a similar result much more economically by using the above identification of "computable" and "recursive."

We know that every rec. function F may be represented as $Fx = A\mu y\{By = x\}$ for some p.r. A and B, where B is onto. Let $B^{-1}x = \mu y\{By = x\}$. If F is the enumerating function for the class of p.r. functions (cf. problem 12) such that $FJ(n,x) = F_n x$, then all recursive functions are contained in the enumeration

$$G_n x = F_{Kn} F_{Ln}^{-1}.$$

If F_{Ln} is not onto, G_n is not recursive, but each recursive function is G_n for some n.

We wish to construct a machine $\mathfrak{U}_1$ which has the action $(n,x) \to (G_n x)$ in case n is the index of a recursive function. I.e., $\mathfrak{U}_1$ is a universal machine for functions of one argument. Let

$$HJ(n,x) = J(n, FJ(n,x)).$$

Then $LH^{-1}J(n,y) = \mu x\{F_n x = y\} = F_n^{-1}y$ if it is defined. Define

$$\mathfrak{U}_1 = \mathcal{C}_2 \mathcal{M}_K \mathcal{C}_3 \mathcal{M}_L \mathcal{C}_3 \mathcal{J}_4^2 \mathcal{M}_J \mathcal{M}_{H^{-1}} \mathcal{M}_L \mathcal{M}_J \mathcal{M}_F.$$

$\mathfrak{U}_1$ is the desired machine since if G_n is recursive

$$\begin{aligned}(n,x) &\to (n,x,n) \to (n,x,Kn) \to (n,x,Kn,n) \to (n,x,Kn,Ln)\\ &\to (n,x,Kn,Ln,x) \to (Kn,Ln,x) \to (Kn, J(Ln,x))\\ &\to (Kn, H^{-1}J(Ln,x)) \to (Kn, LH^{-1}J(Ln,x)) = (Kn, F_{Ln}^{-1}x)\\ &\to (J(Kn, F_{Ln}^{-1}x)) \to (F_{Kn}F_{Ln}^{-1}x) = (G_n x)\end{aligned}$$

We may also construct a universal machine for functions of an arbitrary number of arguments; i.e., a machine $\mathfrak{U}$ which takes $(n; x_1, \ldots, x_k)$ into $(G_n J_{k-1}(x_1, \ldots, x_k))$, where the ";" signifies two blank spaces on the tape. To construct such a machine we first define a machine

$$\mathcal{R}: aba^k q \to a q_{00} b a^k$$
$$bba^k q \to b q_{001} b a^k$$

$\mathcal{R}$	a	b
0	L0	L1
1	P00	E00'

Now let

$$\mathcal{U} = [R\begin{cases}\mathcal{S}\mathcal{M}_J]\\ \mathcal{S}\mathcal{B}\mathcal{U}_1\end{cases}.$$

$\mathcal{U}$ has the action

$$\begin{aligned}(n; x_1, \ldots, x_k) &\to (n; x_1, \ldots, x_{k-2}, J(x_{k-1}, x_k)) && \text{by } R\mathcal{S}\mathcal{M}_J\\ &\to \ldots \to (n; J_{k-1}(x_1, \ldots, x_k))\\ &\to (n, J_{k-1}(x_1, \ldots, x_k)) && \text{by } \mathcal{B}\\ &\to (G_n J_{k-1}(x_1, \ldots, x_k)) && \text{by } \mathcal{U}_1.\end{aligned}$$

The equivalence of recursive and computable functions and the existence of such universal machines lends further weight to the argument that the recursive functions are those which are, in some sense, effectively computable.

Arithmetical Predicates and the Arithmetical Hierarchy

All arithmetical predicates may be written as $Q_1 x_1 \cdots Q_k x_k \; R(x_1, \ldots, x_k, y)$ or $Q_1 x_1 \cdots Q_k x_k \; F(x_1, \ldots, x_k, y) = 0$, where R is a recursive relation and F a recursive function. Adjacent quantifiers of like kind may be "collapsed" by pairing. E.g.,

$$\bigwedge x_1 \bigwedge x_2 \, R(x_1, x_2, y) \leftrightarrow \bigwedge x_1 \, R(Kx_1, Lx_1, y).$$

Thus all arithmetical predicates occur somewhere in the <u>arithmetical hierarchy</u>

Σ_0	$R(x)$		Π_0
Σ_1	$\bigvee_y R(x,y)$	$\bigwedge_y R(x,y)$	Π_1
Σ_2	$\bigvee_y \bigwedge_z R(x,y,z)$	$\bigwedge_y \bigvee_z R(x,y,z)$	Π_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Other hierarchies may be obtained by considering bound variables of higher type (e.g., function quantifiers). A superscript on a Σ or Π indicates the variable of highest type. From above, $\Sigma_i^0 = \Sigma_i$, etc.

$\Sigma_0 = \Pi_0$ is the class of recursive relations. Σ_1 is the class of r.e. relations. Since the negation of any predicate in Σ_1 is in Π_1, we have, by an earlier result, $\Sigma_0 = \Sigma_1 \cap \Pi_1$. Post has shown that, in general, $\Sigma_k \cap \Pi_k$ is the class of relations recursive in Σ_{k-1} (or, equivalently, in Π_{k-1}), where "A is recursive in B" is taken to mean essentially that membership in A is recursive if a list of the elements of B is available.

The hierarchy is a true hierarchy by virtue of the following proper inclusions:

$$\Sigma_0 = \Pi_0 \begin{array}{l} \subset \; \Pi_1 \subset \Pi_2 \subset \Pi_3 \subset \cdots \\ \qquad \not\subset \quad \not\subset \quad \not\subset \\ \subset \; \Sigma_1 \subset \Sigma_2 \subset \Sigma_3 \subset \cdots \end{array}$$

These inclusions are obtained by noting that $\Sigma_k \cup \Pi_k \subseteq \Sigma_{k+1} \cap \Pi_{k+1}$ by adding superfluous quantifiers, and then showing that for $k \neq 0$, $\Sigma_k \not\subset \Pi_k$ and $\Pi_k \not\subset \Sigma_k$. Thus, for example, since $\Sigma_1 \subseteq \Pi_2 \cap \Sigma_2 \subset \Sigma_2$, $\Sigma_1 \neq \Sigma_2$.

To show that $\Sigma_k \neq \Pi_k$, recall that every recursive function G may be represented as

$$Gx = A\,\dot{\iota}y\{B(x,y)=0\},$$

where A and B are primitive recursive. I.e.,

$$Gx=0 \leftrightarrow \bigvee_y (Ay=0 \wedge B(x,y)=0) \leftrightarrow \bigvee_y (Ay + B(x,y)=0).$$

Hence every recursive relation R may be represented as

$$R(\underline{x}) \leftrightarrow \bigvee_y C(\underline{x},y)=0$$

where C is primitive recursive. Now let F be the enumerating function for the class of p.r. functions and define

$$G_k(n,a,x_1,\dots,x_k) = FJ(n, J_k(a,x_1,\dots,x_k)).$$

$G_k(n,\dots)$ enumerates all p.r. functions of k+1 variables as n runs through the natural numbers.

Let $H(a,x_1,\dots,x_k)$ be a recursive function. Then, as shown, there exists a ~~recur~~ p.r. function D such that

$$H(a,x_1,\dots,x_k)=0 \leftrightarrow \bigvee_y D(a,x_1,\dots,x_k,y)=0$$

$$\bigvee_{x_k} H(a,x_1,\dots,x_k)=0 \leftrightarrow \bigvee_{x_k} D(a,x_1,\dots,x_{k-1},Kx_k,Lx_k)=0$$

$$\leftrightarrow \bigvee_{x_k} E(a,x_1,\dots,x_k)=0$$

where E is the p.r. function obtained from D as indicated. E, being p.r., is $G_k(n,\dots)$ for some n by the above enumeration. Hence for any recursive function H, there exists an n such that

$$\bigvee_{x_k} H(a,x_1,\dots,x_k)=0 \leftrightarrow \bigvee_{x_k} G_k(n,a,x_1,\dots,x_k)=0.$$

Now G_k is a recursive function, and if there existed a recursive function H such that

$$\ldots \bigvee_{x_{k-1}} \bigwedge_{x_k} G_k(a, a, x_1, \ldots, x_k) \neq 0 \leftrightarrow \ldots \bigwedge_{x_{k-1}} \bigvee_{x_k} H(a, x_1, \ldots, x_k) = 0,$$

then for some n,

$$\ldots \bigvee_{x_{k-1}} \bigwedge_{x_k} G_k(a, a, x_1, \ldots, x_k) \neq 0 \leftrightarrow \ldots \bigwedge_{x_{k-1}} \bigvee_{x_k} G_k(n, a, x_1, \ldots, x_k) = 0.$$

which gives rise to a contradiction for $a = n$. This establishes one of the relations $\Pi_k \not\subset \Sigma_k$ and $\Sigma_k \not\subset \Pi_k$ (depending on whether k is even or odd), and a similar argument establishes the other.

For future reference, we prove the following lemma (a special case of Kleene's S^m_n Theorem).

<u>Lemma</u>. To every r.e. relation $R(x, y)$ there corresponds a p.r. fct. Q such that for all k,

$$R(x, k) \leftrightarrow x \in \mathcal{S}_{Qk}.$$

<u>Proof</u>: By definition, $t \in \mathcal{S}_q$ iff $F\alpha = S^t 0$ is derivable from Σ_q. Since $R(x, y)$ is r.e., for some q, $J(x, y) \in \mathcal{S}_q \leftrightarrow R(x, y)$. We add to the equations of ~~Σ_q~~ Σ_q the equations

$$H(SD)^k D = I$$

$$F' = HF$$

and consider which values of F' are derivable. $H(SD)^k D = H J(K, SL)^k J(I, 0) = HJ(I, S^k 0) = I$, so that $F' J(x, k) = x$ iff $J(x, k) \in RF = \mathcal{S}_q$. The index for the new system of equations $\Sigma_{q'}$ depends primitive recursively on q, and hence $R(x, k) \leftrightarrow J(x, k) \in \mathcal{S}_q \leftrightarrow x \in \mathcal{S}_{q'} = \mathcal{S}_{Qk}$.

Arithmeticization of Tarski's Predicate Logic with Identity

In the arithmeticization of Tarski's PL with Identity (see p. 14), we shall use the following p.r. functions relating to finite sequences:

(i) $\# \langle t_0, \dots, t_{n-1} \rangle = p_0^{1+t_0} \cdots p_{n-1}^{1+t_{n-1}}$; # empty seq. $= 1$

(ii) $t_k = \mathrm{Pexp}_k\, t$

(iii) $\mathrm{length}\ t = \mu n \{ n \leq t \wedge (p_n \nmid t \vee t = 0) \}$

(iv) $\mathrm{end}\ t = t_{p\,\mathrm{length}\ t}$

(v) $\mathrm{root}\ t = \mu u \{ 0 \leq u \leq t \wedge \bigwedge_k (k+1 < \mathrm{length}\ t \rightarrow u_k = t_k) \}$

(vi) $\mathrm{incr}\ t \leftrightarrow t \neq 0 \wedge \bigwedge_k (k+1 < \mathrm{length}\ t \rightarrow t_k < t_{k+1})$

Tarski's predicate logic has the following symbols: $\wedge, \neg, \rightarrow, =$

$v_0, v_1, \dots$

$R_0, R_1, \dots$

We associate $=$ with R_0 and require the existence of a p.r. function ρ such that $\rho(n)$ is the rank of R_n. E.g., $\rho(0) = 2$.

All formulas of the logic may be Gödel numbered by

$$\Phi_{4n} : R_{Kn}\, v_{(Ln)_0} \cdots v_{(Ln)_{\rho Kn - 1}}$$
$$\Phi_{4n+1} : \neg \Phi_n$$
$$\Phi_{4n+2} : \Phi_{Kn} \rightarrow \Phi_{Ln}$$
$$\Phi_{4n+3} : \bigwedge_{v_{Kn}} \Phi_{Ln}.$$

Next we define a p.r. function Fr which lists the free variables of a formula Φ_n. I.e., $\mathrm{Fr}(n) = \# \langle c_0, \dots, c_{k-1} \rangle$, where Φ_n has exactly $v_{c_0}, \dots, v_{c_{k-1}}$ as free variables and $c_0 < c_1 < \dots < c_{k-1}$. Fr is defined in four cases corresponding to the above numbering of formulas:

$$Fr(4n) = \mu t \{ t \leq p^n_{\rho Kn} \wedge \text{incr } t \wedge \bigwedge_{k < \rho Kn} \bigvee_{j < \text{length } t} t_j = (Ln)_k \}$$

$$Fr(4n+1) = Fr(n)$$

$$Fr(4n+2) = \mu t \{ t \leq p^n_{\text{length } Kn + \text{length } Ln} \wedge \text{incr } t$$
$$\wedge \bigwedge_{k < \text{length } Fr(Kn)} \bigvee_{j < \text{length } t} t_j = [Fr(Kn)]_k$$
$$\wedge \bigwedge_{k < \text{length } Fr(Ln)} \bigvee_{j < \text{length } t} t_j = [Fr(Ln)]_k \}$$

$$Fr(4n+3) = \mu t \{ t \leq \text{length } Fr(Ln) \wedge \text{incr } t$$
$$\bigwedge_{k < \text{length } Ln} (Fr(Ln)_k = Kn \vee \bigvee_{j < \text{length } t} Fr(Ln)_k = t_j) \}$$

Using the function Fr, we may define a function Q giving the Gödel number of the Quine closure of a formula. I.e.,

$$Qn = \# \text{Quine closure of } \Phi_n$$
$$\Phi_{Qn} = [\Phi_n].$$

Let $HJ(t,n) = J(\text{root } t, 4J(\text{end } t, n) + 3)$. Then

$$Qn = LH^{\text{length } Fr(n)} J(Fr(n), n).$$

We now define 9 sets of natural numbers corresponding to the sets of Gödel numbers of instances of axioms B1, ..., B9:

$$n \in B1 \leftrightarrow \bigvee_{k,l,m \leq n} n = Q(4J(4J(k,l)+2, 4J(4J(l,m)+2, 4J(k,m)+2)+2)$$

$$n \in B2 \leftrightarrow \bigvee_{k \leq n} n = Q(4J(4J(4k+1, k)+2, k)+2)$$

$$n \in B3 \leftrightarrow \bigvee_{k,l \leq n} n = Q(4J(k, 4J(4k+1, l)+2)+2)$$

$$n \in B4 \leftrightarrow \bigvee_{k,\ell,m\le n} n = Q(4J(4J(k, 4J(\ell, m)+3)+3,\ 4J(\ell, 4J(k,m)+3)+3)+2)$$

$$n \in B5 \leftrightarrow \bigvee_{k,\ell,m\le n} n = Q(4J(4J(k, 4J(\ell,m)+2)+3,\ 4J(4J(k,\ell)+3, 4J(k,m)+3)+2)+2)$$

$$n \in B6 \leftrightarrow \bigvee_{k,\ell\le n} n = Q(4J(4J(k,\ell)+3,\ell)+2)$$

$$n \in B7 \leftrightarrow \bigvee_{k,\ell\le n} \{ \bigwedge_{j<\text{length } Fr(\ell)} k \ne Fr(\ell)_j \wedge n = Q(4J(\ell, 4J(k,\ell)+3)+2) \}$$

$$n \in B8 \leftrightarrow \bigvee_{k,\ell\le n} \{ k \ne \ell \wedge n = Q(16J(k, 16J(0, 2^{1+k}3^{1+\ell})+1)+3)+1) \}$$

$$n \in B9 \leftrightarrow \bigvee_{j,k,\ell,m\le n} \{ n = Q(4J(4J(0, 2^{1+j}3^{1+k}), 4J(4\ell, 4m)+2)+2)$$
$$\wedge\ \text{lh}\,\ell = \text{lh}\,m$$
$$\wedge \bigvee_{t<\text{lh}\,\ell} [(L\ell)_t = j \wedge (Lm)_t = k$$
$$\wedge \bigwedge_{q<\text{lh}\,\ell} (q = t \vee (L\ell)_q = (Lm)_q)] \}$$

Primitive recursive relations for "axiom" and "proof" may be defined in which Proof (a, b) holds iff a is the number of a sequence of formulas which is a proof of ϕ_b :

$$Ax(n) \leftrightarrow n \in B1 \vee \ldots \vee n \in B9$$

$$\text{Proof}(a,b) \leftrightarrow \text{end } a = b \wedge \text{length } a \ge 1$$
$$\bigwedge_{k<\text{length } a} \{ Ax(a_k) \vee \bigvee_{\ell,m<k} a_m = 4J(a_\ell, a_k)+2 \}$$

Since "Proof" is p.r., the set of theorems defined by

$$\text{Theorem}(b) \leftrightarrow \bigvee_a \text{Proof}(a,b)$$

is recursively enumerable. In a general theory, if the set of axioms is r.e., then so is the set of theorems.

Arithmeticization of Arithmetic

We consider a language $\mathcal{L}_0$ of arithmetic with

Logical Symbols: $\wedge, \neg, \rightarrow, =$

Constant: 0

Operation Symbols: $+, \cdot, S$

Variables: $v_0, v_1, \ldots$

Terms in $\mathcal{L}_0$ are constructed and Gödel numbered by

t_{2n}	$S^n 0$	$(=\Delta_n)$
t_{8n+1}	~~$t_{kn} + t_{Ln}$~~ v_n	
t_{8n+3}	$t_{kn} + t_{Ln}$	
t_{8n+5}	$t_{kn} \cdot t_{Ln}$	
t_{8n+7}	$S\, t_{2n+1}$	

Note that each term has a unique Gödel number.

Formulas of $\mathcal{L}_0$ are likewise numbered:

Φ_{4n}	$t_{kn} = t_{Ln}$
Φ_{4n+1}	$\neg \Phi_n$
Φ_{4n+2}	$\Phi_{kn} \rightarrow \Phi_{Ln}$
Φ_{4n+3}	$\bigwedge_{v_{kn}} \Phi_{Ln}$

As in the arithmeticization of Tarski's logic, we may define a p.r. function Fr and show that the relations "axiom" and "proof" are primitive recursive. In doing this, we change axioms B8 and B9 as follows:

B8': $[\neg \wedge \alpha \neg \alpha = \beta]$, where α is any variable and β is any term not containing α

B9': $[\alpha = \beta \rightarrow (\Phi \rightarrow \Psi)]$, where Ψ is an atomic formula obtained from Φ by replacing an occurrence of α by an occurrence of β, where α, β are terms

I.e., in B9', Φ is either $\alpha = \gamma$ or $\gamma = \alpha$ and Ψ is $\beta = \gamma$ or $\gamma = \beta$ respectively, where α, β, γ are terms.

We shall show that the set of true sentences of $\mathcal{L}_0$ is not arithmetically definable with the aid of the following "fixed point" theorem. For any formula φ_n, let $\ulcorner\varphi_n\urcorner$ be the term $\Delta_n = t_{2n}$ of $\mathcal{L}_0$.

<u>Theorem</u> To every formula Θ with one free variable v_0 there corresponds a sentence φ of $\mathcal{L}_0$ such that $\varphi \leftrightarrow \Theta(\ulcorner\varphi\urcorner)$ is true in $\mathcal{L}_0$.

<u>Proof</u>: The number of the formula

$$\wedge v_0\,(v_0 = \Delta_m \rightarrow \varphi_m)$$

is $4J(0, 4J(4J(1, 2m), m) + 2) + 3$, which is a polynomial value $P(m)$. Let $P_0(m)$ be a term obtained from m and 0 by $+, \cdot, S$ such that $P_0(m) = P(m)$ for all numbers m.

Suppose Θ is the formula φ_k. Let φ_ℓ be the formula obtained from φ_k by replacing each free occurrence of v_0 by the term $P_0(v_0)$. Now consider the formula

$$\varphi_{P(\ell)} \quad : \quad \wedge v_0\,(v_0 = \Delta_\ell \rightarrow \varphi_\ell)$$

By the nature of the substitution made,

$$\varphi_{P(\ell)} \leftrightarrow \wedge v_0\,(v_0 = P_0(\Delta\ell) \rightarrow \varphi_k)$$

holds in $\mathcal{L}_0$. But in arithmetic $P_0(\Delta_\ell)$ and $\Delta_{P(\ell)}$ have the same value, so that

$$\begin{aligned}\varphi_{P(\ell)} &\leftrightarrow \wedge v_0\,(v_0 = \Delta_{P(\ell)} \rightarrow \varphi_k)\\ &\leftrightarrow \Theta(\Delta_{P(\ell)}).\end{aligned}$$

Let $\varphi = \varphi_{P(\ell)}$. Then $\varphi \leftrightarrow \Theta(\ulcorner\varphi\urcorner)$, as required.

<u>Corollary</u> The set $\mathcal{Q} = \{n : \varphi_n \text{ is a true sentence of } \mathcal{L}_0\}$ is not arithmetically definable.

<u>Proof</u>: If $\mathcal{Q}$ is a.d., then so is $\sim\mathcal{Q}$. Let Θ be a formula with one free variable v_0 such that $\Theta(\Delta_n)$ holds iff φ_n is either false or not a sentence, and let φ_k be the formula corresponding to Θ via the fixed point theorem. Then $\Theta(\Delta_k) \leftrightarrow \varphi_k$ by the theorem and $\Theta(\Delta_k) \leftrightarrow \neg\varphi_k$ by the definition of Θ, which is a contradiction. Hence $\mathcal{Q}$ is not a.d.

The corollary establishes the undecidability of arithmetic, for the set of theorems of $\mathcal{L}_0$ is r.e. and hence cannot possibly be equal to the set of true sentences which is not even a.d. In order to establish more general results, we first strengthen the previous theorem.

<u>Fixed Point Theorem</u> To every formula Θ of $\mathcal{L}_0$ with one free variable corresponds a sentence Φ of $\mathcal{L}_0$ such that

$$\mathcal{A} \vdash \Phi \leftrightarrow \Theta(\ulcorner\Phi\urcorner),$$

where $\mathcal{A}$ is any set of sentences such that $\mathcal{A}$ yields all true equalities of the forms $\Delta_m + \Delta_n = \Delta_p$ and $\Delta_m \cdot \Delta_n = \Delta_p$ for all m, n, p.

<u>Proof</u>: Let $P(m)$ be a number of the formula

$$\wedge v_0 (v_0 = \Delta_m \rightarrow \Phi_m)$$

and let $P_0(v_0)$ be a term of $\mathcal{L}_0$ such that

$$\mathcal{A} \vdash P_0(\Delta_m) = \Delta_{P(m)}$$

for all natural numbers m. As before let ℓ be the number of the formula obtained from Θ by replacing each free occurrence of v_0 by $P_0(v_0)$. Then

$$\vdash \wedge v_0 (v_0 = \Delta_\ell \rightarrow \Phi_\ell) \leftrightarrow \wedge v_0 (v_0 = P_0(\Delta_\ell) \rightarrow \Theta)$$

$$\mathcal{A} \vdash \wedge v_0 (v_0 = P_0(\Delta_\ell) \rightarrow \Theta) \leftrightarrow \wedge v_0 (v_0 = \Delta_{P(\ell)} \rightarrow \Theta)$$

since $P_0(\Delta_m) = \Delta_{P(m)}$ is provable, and hence

$$\mathcal{A} \vdash \Phi_{P(\ell)} \leftrightarrow \Theta(\Delta_{P(\ell)})$$

$$\mathcal{A} \vdash \Phi \leftrightarrow \Theta(\ulcorner\Phi\urcorner).$$

Note that given the number of Θ we may compute the number of Φ since ℓ and P may be computed.

Undecidability

Let $\mathcal{Q}$ be a theory of arithmetic, and denote by Theorems ($\mathcal{Q}$) the set of theorems of $\mathcal{Q}$. Let $\mathcal{T}_{\mathcal{Q}}$ be the set of numbers of theorems of $\mathcal{Q}$; i.e., $n \in \mathcal{T}_{\mathcal{Q}} \leftrightarrow \mathcal{Q}_n \in$ Theorems ($\mathcal{Q}$). Similarly, let $R_{\mathcal{Q}}$ be the set of numbers of disprovable (refutable) statements of $\mathcal{Q}$.

We illustrate the nature of the results to be proved by the following example:

<u>Definition</u> A set $\mathcal{S}$ is <u>definable</u> in a theory $\mathcal{Q}$ iff there exists a formula Θ of one free variable such that

$$n \in \mathcal{S} \text{ iff } \mathcal{Q} \vdash \Theta(\Delta_n)$$
$$n \notin \mathcal{S} \text{ iff } \mathcal{Q} \vdash \neg\Theta(\Delta_n).$$

<u>Theorem.</u> If $\mathcal{Q}$ satisfies the hypothesis of the Fixed Point Theorem, then there is no definable set $\mathcal{S}$ of natural numbers such that $R_{\mathcal{Q}} \subset \mathcal{S}$ and $\mathcal{S} \cap \mathcal{T}_{\mathcal{Q}} = \emptyset$.

<u>Proof</u>: Suppose Θ defines $\mathcal{S}$ in $\mathcal{Q}$, and let $\mathcal{Q}_n$ be given by the Fixed Point Theorem so that

$$\mathcal{Q} \vdash \mathcal{Q}_n \leftrightarrow \Theta(\Delta_n).$$

Then $n \in \mathcal{S} \Rightarrow \mathcal{Q} \vdash \Theta(\Delta_n) \Rightarrow \mathcal{Q} \vdash \mathcal{Q}_n \Rightarrow n \in \mathcal{T}_{\mathcal{Q}}$

$n \notin \mathcal{S} \Rightarrow \mathcal{Q} \vdash \neg\Theta(\Delta_n) \Rightarrow \mathcal{Q} \vdash \neg\mathcal{Q}_n \Rightarrow n \in R_{\mathcal{Q}}$,

which in any case is a contradiction.

<u>Corollary</u> If $\mathcal{Q}$ satisfies the hypothesis of the FP Theorem and if every recursive set is definable in $\mathcal{Q}$, then $\mathcal{T}_{\mathcal{Q}}$ and $R_{\mathcal{Q}}$ are not recursively separable. I.e., (cf. p. 138), $\mathcal{Q}$, and every consistent extension of $\mathcal{Q}$, is undecidable.

In order to generalize this result, we define the following notions:

<u>essentially</u> <u>undecidable</u> - all consistent extensions are undecidable (e.u.)

<u>hereditarily</u> <u>undecidable</u> - all subtheories are undecidable (h.u.)

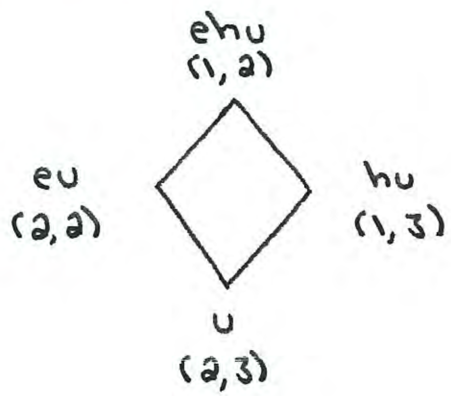
<u>essentially</u> <u>hereditarily</u> <u>undecidable</u> - all compatible theories are undecidable (e.h.u.)

The notion of definability may also be generalized by considering the following relations between sets $\mathcal{S}$ and formulas Θ with one free variable:

1. $n \in \mathcal{S} \Rightarrow \quad \vdash \Theta(\Delta_n)$
2. $n \in \mathcal{S} \Rightarrow \quad \mathcal{A} \vdash \Theta(\Delta_n)$
3. $n \in \mathcal{S} \Rightarrow$ not $\mathcal{A} \vdash \neg\Theta(\Delta_n)$.

A set $\mathcal{S}$ is said to be <u>(a, b)</u> <u>definable</u> iff there exists a formula Θ with one free variable such that the relation (a) holds between $\mathcal{S}$ and Θ and the relation (b) between $\sim\mathcal{S}$ and $\neg\Theta$.

The definability introduced before corresponds to (2, 2) definability, and by the corollary above, we have seen that if a theory $\mathcal{A}$ satisfies the hypothesis of the FP Theorem, then (2, 2) definability of recursive sets implies the essential undecidability of $\mathcal{A}$. In general, we shall establish the following correspondances between definability of recursive sets and undecidability, with no restriction on $\mathcal{A}$:



<u>Theorem</u> If every recursive set $\mathcal{S}$ is (2,3) definable in a theory $\mathcal{T}$, then $\mathcal{T}$ is undecidable.

<u>Proof</u>: For every recursive set $\mathcal{S}$ there exists a formula Θ of one free variable such that

$$n \in \mathcal{S} \text{ iff } \mathcal{T} \vdash \Theta(\Delta_n).$$

If Φ_k has one free variable, let

$$\mathcal{S}_k = \{n : \mathcal{T} \vdash \Phi_k(\Delta_n)\};$$

otherwise let $\mathcal{S}_k = \emptyset$. Now let $\mathcal{D} = \{n : n \notin \mathcal{S}_n\}$. If $\mathcal{T}$ is decidable, then $\mathcal{D}$ is recursive. But by (2,3) definability, all recursive sets are $\mathcal{S}_k$ for some k, and we have the usual contradiction.

<u>Corollary 1</u>. (1,3) $\Rightarrow$ h.u.

<u>Proof</u>: Suppose $\mathcal{T}' \subseteq \mathcal{T}$. Then every recursive set is (1,3) definable in $\mathcal{T}'$ and hence also (2,3) definable in $\mathcal{T}'$. Thus $\mathcal{T}'$ is undecidable.

<u>Corollary 2</u>. (2,2) $\Rightarrow$ e.u.

<u>Proof</u>: Suppose $\mathcal{T} \subseteq \mathcal{T}'$. Then every recursive set is (2,2) definable in $\mathcal{T}'$ and hence also (2,3) definable in $\mathcal{T}'$.

<u>Corollary 3</u>. (1,2) $\Rightarrow$ e.h.u.

<u>Proof</u>: Suppose $\mathcal{T} \subseteq \mathcal{T}'$ and $\mathcal{T}'' \subseteq \mathcal{T}'$. Then every recursive set is (1,2) definable in $\mathcal{T}'$, (1,3) definable in $\mathcal{T}'$, (1,3) definable in $\mathcal{T}''$, and hence (2,3) definable in $\mathcal{T}''$.

Note that in the above theorems the only property which we require of $\{\Delta_n\}$ is that it forms a r.e. set of terms. Using the above theorems, we may establish undecidability results for various theories of arithmetic by proving the appropriate definability results.

A Sentence Undecidable in Arithmetic

Let $\mathcal{Q}$ be a recursive set of true sentences of arithmetic which satisfies the hypothesis of the Fixed Point Theorem and such that every recursive relation of natural numbers is definable in $\mathcal{Q}$; i.e., to every recursive relation $R(x,y)$ there corresponds a formula Φ such that if $R(\Delta_m, \Delta_n)$ holds in arithmetic, then $\mathcal{Q} \vdash \Phi(\Delta_m, \Delta_n)$ and if $\neg R(\Delta_m, \Delta_n)$ holds, then $\mathcal{Q} \vdash \neg \Phi(\Delta_m, \Delta_n)$.

As shown above the relation $\mathrm{Proof}(a,b)$ is p.r., and furthermore is arithmetically definable by a formula "Proof" with the properties

(i) $\mathcal{Q} \vdash \mathrm{Proof}(\Delta_m, \Delta_n)$ iff m is the number of a proof of Φ_n and

(ii) $\mathcal{Q} \vdash \neg \mathrm{Proof}(\Delta_m, \Delta_n)$ iff m is not the number of a proof of Φ_n.

Now consider the formula $\Lambda v_1 \neg \mathrm{Proof}(v_1, v_0)$. By the FP Theorem there exists a sentence Φ such that $\mathcal{Q} \vdash \Phi \leftrightarrow \Lambda v_1 \neg \mathrm{Proof}(v_1, \ulcorner\Phi\urcorner)$. We claim that Φ is true but not provable. For suppose Φ is provable in $\mathcal{Q}$ and let k be the number of a proof. Then

$$\mathcal{Q} \vdash \mathrm{Proof}(\Delta_k, \ulcorner\Phi\urcorner)$$
$$\mathcal{Q} \vdash \mathrm{V} v_1 \, \mathrm{Proof}(v_1, \ulcorner\Phi\urcorner)$$
$$\mathcal{Q} \vdash \neg \Phi$$

which is a contradiction. Hence Φ is unprovable. By (ii) we have

$$\mathcal{Q} \vdash \neg \mathrm{Proof}(\Delta_k, \ulcorner\Phi\urcorner)$$

for every k. Thus $\neg \mathrm{Proof}(\Delta_k, \ulcorner\Phi\urcorner)$ is true for every k and so is $\Lambda v_1 \neg \mathrm{Proof}(v_1, \ulcorner\Phi\urcorner)$ by the definition of truth. Hence Φ is true.

Note that the formula "proof" may be written out explicitly by retracing previous definitions.

Undecidability in Arithmetic

We now apply our theorems concerning undecidability to various theories of arithmetic. In particular we consider the theories R_0 and Q defined in Tarski's Undecidable Theories:

Theory R_0

$$\Delta_m + \Delta_n = \Delta_{m+n} \quad (m, n \text{ natural numbers})$$
$$\Delta_m \Delta_n = \Delta_{mn}$$
$$\Delta_m \neq \Delta_n \quad \text{for } m \neq n$$
$$x \leq \Delta_m \to x = \Delta_0 \vee \ldots \vee x = \Delta_m$$

where $\alpha \leq \beta \leftrightarrow \bigvee_w (w + \alpha = \beta)$. Note that R_0 has an infinite number of axioms; i.e., all instances of the above schemata.

Theory Q

$$Sx = Sy \to x = y$$
$$0 \neq Sx$$
$$x \neq 0 \to \bigvee_y x = Sy$$
$$x + 0 = x$$
$$x + Sy = S(x+y)$$
$$x \cdot 0 = 0$$
$$x \cdot (Sy) = x \cdot y + x$$

Thus Q is finitely axiomatizable, and as shown in Tarski, Q is stronger than R_0; i.e., every model of Q is a model of R_0.

Theorem. Every recursive set is $(2,2)$ definable in R_0.

Proof: Let $\mathcal{S}$ be a recursive set and let F_1, F_2, G_1, G_2 be the polynomials corresponding to $\mathcal{S}$ and $\sim\mathcal{S}$ by Davis' Theorem; i.e.,

$$n \in \mathcal{S} \text{ iff } \bigvee_x \bigwedge_{y \leq x} \bigvee_{u_1 \ldots u_k \leq x} F_1(n, x, y, \underline{u}) = F_2(n, x, y, \underline{u})$$

$$n \notin \mathcal{S} \text{ iff } \bigvee_x \bigwedge_{y \leq x} \bigvee_{u_1 \ldots u_k \leq x} G_1(n, x, y, \underline{u}) = G_2(n, x, y, \underline{u}).$$

Set

$$\Theta_1(t, x) \leftrightarrow \bigwedge_{y \le x} \bigvee_{u_1 \dots u_k \le x} F_1(t, x, y, \underline{u}) = F_2(t, x, y, \underline{u})$$

$$\Theta_2(t, x) \leftrightarrow \bigwedge_{y \le x} \bigvee_{u_1 \dots u_k \le x} G_1(t, x, y, \underline{u}) = G_2(t, x, y, \underline{u}),$$

and let $\Psi(t)$ be the formula

$$\bigwedge_x \{((\Theta_1(t,x) \vee \Theta_2(t,x)) \wedge \bigwedge_{x'} (\Theta_1(t,x') \vee \Theta_2(t,x')) \to \neg x' < x) \to \Theta_1(t,x)$$

Ψ asserts that the least bound for which we can determine membership in S by the Davis Normal form will give the result that $t \in S$.

Suppose $n \in S$ and let m be the least natural number for which $\Theta_1(\Delta_n, \Delta_m)$ holds.

$$R_0 \vdash z \le \Delta_m \to z = \Delta_0 \vee \dots \vee z = \Delta_m$$

Hence

$$R_0 \vdash \Theta_1(\Delta_n, \Delta_m)$$

since all combinations of bound variables may be checked by the axioms of R_0. Similarly

$$R_0 \vdash \neg \Theta_2(\Delta_n, \Delta_k)$$

$$R_0 \vdash \neg \Theta_1(\Delta_n, \Delta_k)$$

for $k < m$, again by checking the computation. Thus $R_0 \vdash \Psi(\Delta_n)$.

Similarly we may show that if $n \notin S$, then $R_0 \vdash \neg\Psi(\Delta_n)$. These two results show that S is (2, 2) definable by Ψ:

$$n \in S \Rightarrow R_0 \vdash \Psi(\Delta_n)$$

$$n \notin S \Rightarrow R_0 \vdash \neg \Psi(\Delta_n).$$

<u>Corollary</u> R_0 is essentially undecidable.

<u>Theorem</u> Every recursive set is (1, 2) definable in Q.

<u>Proof</u>: Let $\Theta(x)$ be the formula $Q \to \Psi(x)$, where Q is the conjunction of the axioms of Q and Ψ is the formula corresponding to a recursive set $\mathcal{S}$ by the previous theorem. If $n \in \mathcal{S}$, then $\vdash Q \to \Psi(\Delta_m)$ since Q is stronger than R_0. If $n \notin \mathcal{S}$, then $R_0 \vdash \neg\Psi(\Delta_n)$, $\vdash Q \to \neg\Psi(\Delta_n)$, and hence

$$Q \vdash \neg(Q \to \Psi(\Delta_n)).$$

Thus $\mathcal{S}$ is (1, 2) definable by Θ in Q.

<u>Corollary</u>. Q is essentially hereditarily undecidable.

<u>Corollary</u> Every recursive set is (1, 3) definable in R_0, and hence R_0 is hereditarily undecidable.

<u>Proof</u>: Given $\mathcal{S}$, Θ as above, we have

$n \in \mathcal{S} \Rightarrow \vdash \Theta(\Delta_n)$

$n \notin \mathcal{S} \Rightarrow$ not $R_0 \vdash \Theta(\Delta_n)$, since $Q \vdash \neg\Theta(\Delta_n)$ and Q is stronger than R_0.

We may actually show that every recursive set is (1, 2) decidable in R_0 and hence that R_0 is e.h.u. To do this we introduce Dana Scott's Theory Ω of arithmetic:

1. $0 \leq x$
2. $x \leq y \wedge y \leq x \to x = y$
3. $x \leq y \wedge y \leq z \to x \leq z$
4. $x \leq Sx$
5. $y \leq x \vee Sx \leq y$
6. $x = Sx \to y \leq x$
7. $x + 0 = x$
8. $x + Sy = S(x+y)$
9. $x \cdot 0 = 0$
10. $x \cdot Sy = x \cdot y + x$

Ω has as models

$\mathfrak{N} = \langle \text{Nat.}, 0, S, +, \cdot, \leq \rangle$

$\mathfrak{N}_n = \langle \{0, 1, \ldots, n\}, 0, S_n, +_n, \cdot_n, \leq_n \rangle$,

where $x +_n y = \min\{n, x+y\}$

$x \leq_n y \leftrightarrow x \leq y \leq n$, etc.

In fact all finite models of Ω are isomorphic to $\mathfrak{N}_n$ for some n; for suppose $\mathfrak{M}$ is a finite model of Ω with $m+1$ elements. Let ℓ be the least natural number such that there exists a natural number $k < \ell$ for which $S^k 0 = S^\ell 0$.

$S^k 0 \leq S^{k+1} 0 \leq \ldots \leq S^{\ell-1} 0 \leq S^\ell 0$ by 4.

$S^{k+1} 0 \leq S^\ell 0 = S^k 0$ by 3.

$S^{k+1} 0 = S^k 0$ by 2.

Hence, by our choice of ℓ, $\ell = k+1$.

$y \leq S^{k-1} 0 \vee S^k 0 \leq y$ by 5.

$y \leq S^k 0$ by 6.

Thus $y \leq S^{k-1} 0 \vee y = S^k 0$

Continuing in this manner we obtain

$y \leq 0 \vee y = S0 \vee \ldots \vee y = S^{k-1} 0 \vee y = S^k 0$

$y = 0 \vee y = S0 \vee \ldots \vee y = S^{k-1} 0 \vee y = S^k 0$ by 1.

Hence $\mathfrak{M}$ is isomorphic to $\mathfrak{N}_k$.

The above argument also shows that all infinite models have a submodel isomorphic to $\mathfrak{N}$, for if $S^k 0 = S^\ell 0$ for $k \neq \ell$, then the model is finite.

<u>Lemma</u>. If P is a polynomial with natural number coefficients, then the value of $P(x_0, \ldots, x_k)$ in the model $\mathfrak{N}_n$ is the minimum of n and the value of $P(x_0, \ldots, x_k)$ in the model $\mathfrak{N}$.

<u>Proof</u>: By induction on the formation of P.

<u>Theorem</u> (Scott) To every r.e. set $\mathcal{S}$ of natural numbers there corresponds a formula Φ with one free variable v_0 such that

(i) $m \in \mathcal{S}$ iff $\Phi(\Delta_m)$ is true in some finite model of Ω; and

(ii) $m \in \mathcal{S}$ iff $\Phi(\Delta_m)$ is true in all infinite models of Ω.

<u>Proof</u>: Let $\mathcal{S}$ be r.e. By the Davis Normal Form there exist polynomials P, Q such that

$$m \in \mathcal{S} \text{ iff } \bigvee_{u} \bigwedge_{v \leq u} \bigvee_{w_1 \cdots w_k \leq u} P(m, u, v, \underline{w}) = Q(m, u, v, \underline{w}).$$

Let $\Phi(x)$ be the formula

$$x \neq Sx \wedge \bigvee_{u} \bigwedge_{v \leq u} \bigvee_{w_1 \cdots w_k \leq u} \{ P(x, u, v, \underline{w}) = Q(x, u, v, \underline{w}) \wedge P(x, u, v, \underline{w}) \neq SP(x, u, v, \underline{w}) \}.$$

Suppose $m \in \mathcal{S}$. Then $\Phi(\Delta_m)$ holds in all infinite models by the Davis Normal Form. By choosing $n > m$ and also greater than all relevant values of P and Q occurring in the evaluation of Φ, we also have $\Phi(\Delta_m)$ holding in $\mathcal{N}_n$.

Conversely, if $m \notin \mathcal{S}$, then $\Phi(\Delta_m)$ does not hold in the standard infinite model, and likewise $\Phi(\Delta_m)$ cannot hold in any finite model.

<u>Corollary 1</u>. The set of finitely satisfiable sentences (i.e., those having finite models) is not recursive.

<u>Proof</u>: Let $\mathcal{S}$ be r.e. but not recursive, and let Φ correspond to $\mathcal{S}$ by Scott's Theorem. Then $\Omega \wedge \Phi(\Delta_m)$ has a finite model iff $m \in \mathcal{S}$, and hence the set of finitely satisfiable sentences cannot be recursive.

<u>Corollary</u> 2. The set of sentences valid in all finite models is not r.e.

<u>Proof</u>: Let $\mathcal{S}$ and Φ be as in Corollary 1. Then $m \notin \mathcal{S}$ iff $\Omega \wedge \Phi(\Delta_m)$ is not true in any finite model, and hence $m \notin \mathcal{S}$ iff $\neg(\Omega \wedge \Phi(\Delta_m))$ is true in all valid models. Since $\sim\mathcal{S}$ is not r.e., the set of sentences valid in all finite models cannot be r.e.

<u>Corollary</u> 3. (Trachténbrot, <u>Doklady</u>, 1953) The set of universally valid sentences is not recursively separable from the set of finitely refutable sentences.

<u>Proof</u>: Let $\mathcal{S}$ and $\mathcal{T}$ be two disjoint r.e. sets which are not recursively separable, and let Φ, Ψ be the formulas corresponding to $\mathcal{S}$, $\mathcal{T}$ respectively by Scott's Theorem. Let $\Theta(x)$: $\Omega \wedge \Psi(x) \rightarrow \Phi(x)$. If $m \in \mathcal{S}$, then $\vdash \Theta(\Delta_m)$ by the completeness theorem since $\Phi(\Delta_m)$ holds in all infinite models of Ω and $\Psi(\Delta_m)$ holds in no finite model of Ω. If $m \notin \mathcal{S}$, but $m \in \mathcal{T}$, then there is a finite model $\mathfrak{N}_n$ in which $\Psi(\Delta_m)$ holds and $\Phi(\Delta_m)$ is false. Hence $\Theta(\Delta_m)$ is finitely refutable.

Now if the set $\mathcal{U}$ of universally valid sentences and the set R of finitely refutable sentences were recursively separable by a set $\mathcal{B}$, then we could define a recursive set $\mathcal{A}$ by $m \in \mathcal{A}$ iff $\Theta(\Delta_m) \in \mathcal{B}$. From the above, $\mathcal{A}$ would recursively separate $\mathcal{S}$ and $\mathcal{T}$, which is contrary to our assumption. Hence $\mathcal{U}$ and R are not recursively separable.

<u>Corollary</u> <u>4</u>. (Problem 20). All recursive sets are (1, 3) definable in Ω, and hence Ω is hereditarily undecidable.

<u>Proof</u>: Let $\mathcal{S}$ be recursive and let Ψ, Ψ' be the formulas corresponding to $\mathcal{S}, \sim\mathcal{S}$ respectively by Scott's Theorem. Let $\Phi(x) \leftrightarrow \Psi(x) \vee \neg\Psi'(x)$. If $m \in \mathcal{S}$, then $\vdash \Omega \rightarrow \Phi(\Delta_m)$ by the completeness theorem. If $m \notin \mathcal{S}$, suppose $\Omega \vdash \Omega \rightarrow \Phi(\Delta_m)$. Then $\Omega \vdash \Psi(\Delta_m) \vee \neg\Psi'(\Delta_m)$, and since $\Psi'(\Delta_m)$ holds in some finite model $\mathfrak{N}_n$, $\neg\Psi'(\Delta_m)$ does not hold in $\mathfrak{N}_n$, and hence $\Psi(\Delta_m)$ does; i.e., $m \in \mathcal{S}$. But this is a contradiction, so that if $m \notin \mathcal{S}$, we cannot have $\Omega \vdash \Omega \rightarrow \Phi(\Delta_m)$. Thus $\mathcal{S}$ is (1, 3) definable by $\Omega \rightarrow \Phi(x)$.

The result of Corollary 4 is in fact the best result possible: If all recursive sets were (2, 2) definable in Ω, then Ω would be essentially undecidable. But this cannot be since the theory of a given ~~model~~ finite model of Ω is a decidable extension of Ω.

The theory Ω was introduced to show that every recursive set is (1, 2) definable in R_0. In order to complete this demonstration, we first introduce a slight modification of R_0:

<u>Theory</u> <u>R_1</u>

$$\Delta_m + \Delta_n = \Delta_{m+n}$$
$$\Delta_m \cdot \Delta_n = \Delta_{m \cdot n}$$
$$\Delta_m \neq \Delta_n \quad \text{for } m \neq n$$
$$x \leq \Delta_n \leftrightarrow x = \Delta_0 \vee \dots \vee x = \Delta_n$$

The only differences between R_1 and R_0 is that in the last axiom schema, $\rightarrow$ has been replaced by $\leftrightarrow$, and that $\leq$ is taken as a primitive symbol rather than being defined by $\bigvee_w (w+x=y) \leftrightarrow x \leq y$. In R_0, if $k \leq \ell$, then $\Delta_k \leq \Delta_\ell$ since $\bigvee_w (w+\Delta_k = \Delta_\ell)$; i.e., $w = \Delta_{\ell-k}$. Hence every model of R_0 is a model of R_1. The converse is not true since the axioms of R_1 do not specify any relation between $+$ and $\leq$ onthe non-standard part of a model.

Now to show that every recursive set is (1,2) definable in R_0, it suffices to establish the result for the weaker theory R_1.

<u>Theorem</u> (Cobham) Every recursive set is (1, 2) definable in R_1.

<u>Proof</u>: We define relatarized operations corresponding to $S, +, \cdot$ by

$$S_a x = y \leftrightarrow (Sx \leq a \wedge Sx = y) \vee (\neg Sx \leq a \wedge y = a)$$
$$x +_a y = z \leftrightarrow (x+y \leq a \wedge x+y = z) \vee (\neg x+y \leq a \wedge z = a)$$
$$x \cdot_a y = z \leftrightarrow (x \cdot y \leq a \wedge x \cdot y = z) \vee (\neg x \cdot y \leq a \wedge z = a).$$

Let $\phi^{(a)}$ be the formula in the language with $0, S, +, \cdot, \leq$ obtained from ϕ by relatavizing all quantifiers to $\leq a$ and by replacing the operations $S, +, \cdot$ by the definitions of $S_a, +_a, \cdot_a$. By the definitions, we have

$$\vdash a \leq a \rightarrow S_a x \leq a \wedge x +_a y \leq a \wedge x \cdot_a y \leq a.$$

Let $\mathfrak{M}$ be any model of the language $\mathcal{L}$ with $0, S, +, \cdot, \leq$, and let $a \in \mathfrak{M}$ be an element with $0 \leq a$ and $a \leq a$. Consider the set $\mathcal{S} = \{x : x \leq a\}$. $S_a, +_a, \cdot_a$ are operations on $\mathcal{S}$, and $\mathfrak{M}_a = \langle \mathcal{S}, 0, S_a, +_a, \cdot_a, \leq \rangle$ is a model of $\mathcal{L}$. Furthermore, $\mathfrak{M}_a$ is a model of a sentence ϕ iff $\mathfrak{M}$ is a model of $\phi^{(a)}$.

If $\Omega \vdash \phi$, then $\vdash 0 \leq a \wedge a \leq a \wedge \Omega^{(a)} \rightarrow \phi^{(a)}$. For if $\mathfrak{M}$ is a model of $\Omega^{(a)}$, then $\mathfrak{M}_a$ is a model of Ω and hence of ϕ, so that $\mathfrak{M}$ is a model of $\phi^{(a)}$, and the result follows from the completeness theorem.

For every n, $R_1 \vdash \Omega^{(\Delta n)}$, as can be verified by checking the axioms of Ω. E.g., the relativization of $x \leq Sx$ is

$$\bigwedge_{x \leq \Delta_n} \{(Sx \leq \Delta_n \wedge x \leq Sx) \vee (\neg Sx \leq \Delta_n \wedge x \leq \Delta_n)\}$$

which is verifiable by the axioms of R_1.

If σ is a sentence which is true in $\mathfrak{N}_n$, then $R_1 \vdash \sigma^{(\Delta n)}$: For let $\mathfrak{R}$ be any model of R_1. Then $\mathfrak{R}_{\Delta n}$ is a model of Ω with $n+1$ elements, and hence is isomorphic to $\mathfrak{N}_n$. $\mathfrak{R}_{\Delta n}$ is then a model of σ, so that $\mathfrak{R}$ is a model of $\sigma^{(\Delta n)}$.

Now let $\mathcal{S}$ be any recursive set and choose ϕ, ψ by Scott's Theorem to correspond to $\mathcal{S}, \sim\mathcal{S}$ respectively. For $n \in \mathcal{S}$,

$$\Omega \vdash \psi(\Delta_n) \rightarrow \phi(\Delta_n)$$

as in Corollary 4. By the completeness theorem and the above remarks,

$$\vdash \bigwedge_a (0 \leq a \wedge a \leq a \wedge \Omega^{(a)} \rightarrow [\psi^{(a)}(\Delta_n) \rightarrow \phi^{(a)}(\Delta_n)]).$$

If $n \notin \mathcal{S}$, let m be such that $\psi(\Delta_n)$ holds in $\mathfrak{N}_m$. Then $R_1 \vdash \psi^{(\Delta m)}(\Delta_n)$ and hence

$$R_1 \vdash \bigvee_a (0 \leq a \wedge a \leq a \wedge \Omega^{(a)} \wedge \psi^{(a)}(\Delta_n) \wedge \neg \phi^{(a)}(\Delta_n)).$$

Thus $\mathcal{S}$ is (1, 2) definable in R_1 by

$$\bigwedge_a \{0 \leq a \wedge a \leq a \wedge \Omega^{(a)} \rightarrow [\psi^{(a)}(x) \rightarrow \phi^{(a)}(x)]\}.$$

<u>Corollary</u> (Cobham) R_1 is essentially hereditarily undecidable.

We note that we may loosen the requirements on $+, \cdot, S$ in the theory R_1 by requiring them to be operations only on numerals and relations elsewhere. I.e., the proof given above is also valid for the theory R_2 in which $+, \cdot, S$ are ~~op~~ relations and the axioms are

<u>Theory R_2.</u>

$$\Delta_m + \Delta_n = \Delta_p \quad \text{for } m+n = p$$
$$\Delta_m + \Delta_n \neq \Delta_p \quad \text{for } m+n \neq p$$
$$\Delta_m \cdot \Delta_n = \Delta_p \quad \text{for } m \cdot n = p$$
$$\Delta_m \cdot \Delta_n \neq \Delta_p \quad \text{for } m \cdot n \neq p$$
$$\Delta_m \neq \Delta_n \quad \text{for } m \neq n$$
$$x \leq \Delta_n \leftrightarrow x = \Delta_0 \vee \ldots \vee x = \Delta_n$$

We may furthermore omit the first axioms concerning $+$ and still have an e.h.u. theory, for $+$ is definable in terms of $\cdot$ and S. Hence the theory involving such a definition is stronger than R_1 (or R_2) and is consequently e.h.u. Thus we have an example of a theory with one unary relation (S) and one binary relation $(\cdot)$ which is e.h.u.

Finally, we note still another corollary to Scott's Theorem: For every r.e. set $\mathcal{S}$ there exists a formula Φ with one free variable such that $m \in \mathcal{S}$ iff $\Omega \vdash \Phi(\Delta_m)$. For if Ψ is the formula corresponding to $\mathcal{S}$ by Scott's Theorem, we may take $\Phi(x) \leftrightarrow \Psi(x) \vee \bigvee_y (y = Sy)$

The Theory of Groups

We shall show that the theory Q is interpretable in the theory of groups, and that consequently the theory of groups is undecidable.

Consider the theory of $1, +, |$, and the integers. $\cdot$ may be defined in this theory by first defining

$$n = k(k+1) \leftrightarrow \bigwedge_m (n|m \leftrightarrow k|m \wedge k+1|m \wedge 2k+1|2n-k)$$

and then

$$n = k\cdot \ell \leftrightarrow (k+\ell)\cdot(k+\ell+1) = k(k+1) + \ell(\ell+1) + 2n.$$

The first definition is justified since the condition on the right guarantees that $n = \text{lcm}(k, k+1) = \pm k(k+1)$, with the '$-$' being excluded by $2k+1|2n-k$.

Q may therefore be interpreted in this theory, since the natural numbers may be defined as those integers which are the sum of four squares. Hence every recursive set is (1, 2) definable in the theory, and the theory is e.h.u.

We now proceed to interpret this theory of $1, +, |$, Int. in the theory of a particular group G of all permutations of the integers. Let S be a constant of G corresponding to the successor function and define

$$\begin{aligned}
\text{Int } X &\leftrightarrow X \circ S = S \circ X \\
X = Y + Z &\leftrightarrow X = Y \circ Z \\
X = 1 &\leftrightarrow X = S \\
X \mid Y &\leftrightarrow X \circ S = S \circ X \wedge Y \circ S = S \circ Y \\
&\quad \wedge \bigwedge_Z (X \circ Z = Z \circ X \rightarrow Y \circ Z = Z \circ Y).
\end{aligned}$$

From the above definitions, we conclude that the interpretation "Int" of the integers is the set of powers of S; for if $X \circ S = S \circ X$, let $X(0) = a = S^n 0$. Then $X(1) = X \circ S(0) = S \circ X(0) = S^{n+1}(0) = S^n(1)$, and by induction $X = S^n$.

The interpretation preserves the properties of + and |, when acting on the integers. For + this is obvious. For |, [redacted] suppose that $X = S^m$ and $Y = S^n$. If $m|n$ and $S^m \circ Z = Z \circ S^m$, then

$$S^n \circ Z = S^{n-m} \circ (S^m \circ Z) = S^{n-m} \circ (Z \circ S^m)$$
$$= (S^{n-m} \circ Z) \circ S^m = \ldots = Z \circ S^n,$$

so that $X|Y$. Conversely, if $m \nmid n$, we define

$$H(u) = \begin{cases} u+m & \text{if } m|u \\ u & \text{if } m \nmid u. \end{cases}$$

H is a permutation which displaces multiples of m. Now

$$S^m \circ H(u) = \begin{cases} u+2m & \text{if } m|u \\ u+m & \text{if } m \nmid u \end{cases}$$

and hence $S^m \circ H = H \circ S^m$. But

$$S^n \circ H(u) = \begin{cases} u+n+m & \text{if } m|u \\ u+n & \text{if } m \nmid u \end{cases}$$

$$H \circ S^n(u) = \begin{cases} u+n+m & \text{if } m|u+n \\ u+n & \text{if } m \nmid u+n. \end{cases}$$

Thus $S^n \circ H(0) = n+m \neq n = H \circ S^n(0)$ if $m \neq 0$ and $m \nmid n$, so that $S^n \circ H \neq H \circ S^n$ and $X \nmid Y$.

Thus if $\mathcal{D} = \langle \text{Int.}, 1, +, | \rangle$ and $\mathcal{G} = \langle G, S, \circ \rangle$, we can interpret $\mathcal{D}$ in $\mathcal{G}$. Corresponding to every formula ϕ in the language $\mathcal{L}$ with $1, +, |$, there is a formula $\phi^{(s)}$ in the language $\mathcal{L}'$ with $S, \circ$ which is the interpretation of ϕ. Since Q is interpretable in the theory of $\mathcal{D}$, there exists a sentence Δ of $\mathcal{L}$ which is true in $\mathcal{D}$ but is essentially undecidable (e.g., take Δ to be the interpretation of the axioms of Q).

$\bigvee_S \Delta^{(s)}$ is consistent (since it is true by choosing S to be the successor function as above). If $\Delta \vdash \phi$, then

$$(*) \quad \bigvee_S \Delta^{(s)} \vdash \bigwedge_S (\Delta^{(s)} \to \phi^{(s)})$$

The set of sentences φ of $\mathcal{L}$ for which (*) holds form a consistent extension of Δ, and consequently must be undecidable. Thus $\bigvee_s \Delta^{(s)}$ is also essentially undecidable.

Furthermore the theory of $\bigvee_s \Delta^{(s)}$ is e.h.u.: Let $\mathcal{T}$ be any compatible theory. Then

$$\{\varphi : \mathcal{T} \vdash \bigvee_s \Delta^{(s)} \to \varphi\}$$

is an extension of the theory of $\bigvee_s \Delta^{(s)}$ and hence is undecidable. But then $\mathcal{T}$ is also undecidable.

Finally, the theory of groups is compatible with the theory of $\bigvee_s \Delta^{(s)}$ since $\mathcal{G}$ is a common model. Hence the theory of groups is undecidable.

We note that the above proof collapses for the theory of abelian groups since the interpretation of $\mathcal{D}$ is no longer valid. In fact Wanda Szmielew has show that the theory of abelian groups is decidable.

Note that our result does not mean that every non-abelian group is undecidable, nor does Szmielew's result mean that every abelian group is decidable.

Cobham has shown that the theory of finite groups is undecidable.

Method of Rabin and Scott

We shall illustrate a method developed by Rabin and Scott for establishing undecidability which proceeds by defining every model of a theory known to be undecidable in a model of the theory in question.

Let $\mathcal{L}$ be a predicate logic with identity and relation symbols $R_1, R_2, \ldots$ of ranks $r_1, \ldots,$ and suppose $\mathcal{L}$ is known to be undecidable. (E.g., $\mathcal{L}$ may be a language of arithmetic). Then if $\mathcal{L}'$ is the predicate logic with identity and ~~equal~~ one binary relation R, we know that the set of valid sentences of $\mathcal{L}'$ is undecidable from above since $\mathcal{L}$ is compatible with $\bigvee_s \Delta^{(s)}$. This result may also be obtained in the following manner:

We define (in the language $\mathcal{L}'$)

$$xR^1y \leftrightarrow xRy$$

$$xR^{k+1}y \leftrightarrow \bigvee_z (xRy \wedge yR^kz),$$

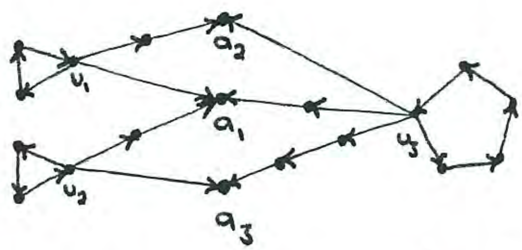
so that xR^ky means that x is "connected" to y by a chain of k element. Also

$$\mathrm{Dom}(x) \leftrightarrow \neg \bigvee_y xRy$$

$$R_i(x_1, \ldots, x_{r_i}) \leftrightarrow \bigvee_u (uR^{r_i}u \wedge uR^1x_1 \wedge \ldots \wedge uR^{r_i}x_{r_i}).$$

Now every formula ϕ of $\mathcal{L}$ may be translated into a formula ϕ^* of $\mathcal{L}'$ by relativizing all quantifiers to Dom and using the above interpretation of the relation symbols.

Corresponding to every model $\mathfrak{A}$ of $\mathcal{L}$ we may construct a model $\mathfrak{B}$ of $\mathcal{L}'$ in which this interpretation is "faithful": To each element in the domain of $\mathfrak{A}$ corresponds an element of $\mathfrak{B}$ satisfying $\mathrm{Dom}(x)$; i.e., which is a "terminal" element of the relation R. Then for each relation R_i we include cycles of length p_i with "pointers" to the elements in the relation R_i. E.g., suppose a_1, a_2, a_3 are elements of the domain of $\mathfrak{A}$ and that $R_2(a_1, a_2)$, $R_2(a_3, a_1)$ $R_3(a_2, a_1, a_3)$ hold in $\mathfrak{A}$. Then, letting $x \longrightarrow y$ stand for xRy, part of the diagram of $\mathfrak{B}$ would be



Conversely, to every model of $\mathcal{L}'$ corresponds a model (possibly empty) of $\mathcal{L}$ whose elements are the terminal states of the relation R and whose relations are determined by the cycles and chains of elements of the model of $\mathcal{L}'$.

Hence if Φ is a sentence of $\mathcal{L}$ and Φ^* the corresponding sentence of $\mathcal{L}'$, then $\vdash_{\mathcal{L}} \Phi$ iff $\vdash_{\mathcal{L}'} \bigvee_x Dom(x) \rightarrow \Phi^*$. Thus if $\mathcal{L}'$ is decidable, $\mathcal{L}$ would also be decidable, contrary to hypothesis.

Myhill employs a still different technique to prove the undecidability of a predicate logic with equality and one binary relation: he interprets arithmetic in the language with one relation by the definition

$$xRy \leftrightarrow x \neq 0 \wedge x-1 \mid y.$$

Finite Associative Systems

Finite associative systems are models of the sentence $(x \circ y) \circ z = x \circ (y \circ z)$ in the language with one binary operation. The theory of such systems may be shown to be undecidable using a modification R^+ of R_0. Instead of operations, R^+ has the relations

$$\Delta_1(x), \quad Suc(x,y), \quad Prod(x,y,z), \quad Less(x,y)$$

and, upon defining

$$\Delta_{n+1}(x) \leftrightarrow \bigvee_y (\Delta_n(y) \wedge Suc(y,x)),$$

R^+ has as axioms

1. $\bigvee_x \Delta_m(x)$ for $m \geq 1$
2. $\Delta_m(x) \to \neg \Delta_n(x)$ for $m \neq n$
3. $\Delta_m(x) \wedge \Delta_n(y) \to \bigwedge_z (Prod(x,y,z) \leftrightarrow \Delta_{m \cdot n}(z))$
4. $\Delta_n(y) \to [Less(x,y) \to \Delta_1(x) \vee \dots \vee \Delta_n(x)]$

Any theory compatible with R^+ is also compatible with R_0, so that R^+ is e.h.u.

Now let $\mathfrak{M}_n$ be the model whose domain is the set of all functions mapping $\{0, 1, \dots, n\}$ into itself, and let $\circ$ be the operation of composition. We can interpret the relations of R^+ in this model via the definitions

$$\Delta_1(F) \leftrightarrow \bigwedge_G FG = F$$

$$Prod(F,G,H) \leftrightarrow \bigvee_{K,L} \bigwedge_{u,v} \{u \in RF \wedge v \in RG \to \bigvee_x (x \in RH \wedge Kx = u \wedge Lx = v) \wedge \bigwedge_x (x \in RH \to Kx \in RF \wedge Lx \in RG)\}$$

$$Less(F,G) \leftrightarrow \bigvee_{U,V,W} (UF = GV \wedge UW = I)$$

$$Suc(F,G) \leftrightarrow \bigwedge_H (\neg Less(G,H) \wedge Less(H,G) \to Less(H,F)).$$

I.e., $\Delta_1(F)$ expresses the fact that F is a constant function, and in the subsequent definitions small letters stand for such constant functions. The numerals Δ_m are thereby represented by a class of functions whose range has m elements (for $m \leq n$). The definition of "Prod (F, G, H)" gives the desired result if the product of the number of elements in the range of F times the number of elements in RG is less than n. "Less" is defined by saying that RF may be mapped biuniquely into the range of G (I is the identity function). "Suc" is then defined from "Less" in the normal manner.

In a model $\mathfrak{M}_N$, instances of axiom (1) are satisfied for all $m \leq N$ under the given interpretation; (2) is satisfied for all m, n; (3) for $m \cdot n \leq N$; and (4) for $n \leq N$. Hence all axioms of R^+ are satisfied in some model $\mathfrak{M}_N$, and thus the theory of finite associative systems is compatible with R^+. Since R^+ is e.h.u., the theory of finite associative systems is undecidable.

Gödel's Second Theorem

Gödel's Second Theorem roughly states that the consistency of any sufficiently strong theory of arithmetic cannot be proved within that theory. In terms of our notion of proof we may define

$$\pi(\Delta_n) \leftrightarrow \bigvee_y \text{proof}(y, \Delta_n).$$

Then Gödel's result may be obtained by showing that not $\mathcal{Q} \vdash \neg\pi(\ulcorner \neg 0 = 0 \urcorner)$.

Some remarks concerning the theory $\mathcal{Q}$ and the formula "proof" are in order. If k is the number of a proof of φ_n, then we would like to be able to prove $\mathcal{Q} \vdash \text{proof}(\Delta_k, \Delta_n)$. This can be done in the theories we have considered, and in fact can be done in any theory where $\mathcal{Q}$ is sufficiently strong and the formula defining the set of axioms is "nice." Feferman, Kreisel, Mostowski, and others, have isolated the following requirements on the formula "π" as sufficient for the proof of the theorem:

I. If $\mathcal{Q} \vdash \varphi$, then $\mathcal{Q} \vdash \pi(\ulcorner\varphi\urcorner)$.

II. $\mathcal{Q} \vdash \pi(\ulcorner\varphi \to \psi\urcorner) \to (\pi(\ulcorner\varphi\urcorner) \to \pi(\ulcorner\psi\urcorner))$

III. $\mathcal{Q} \vdash \pi(\ulcorner\varphi\urcorner) \to \pi(\ulcorner\pi(\ulcorner\varphi\urcorner)\urcorner)$

(Feferman has shown that III is not an essential requirement, though it does simplify the proof.) The theorem may then be stated by saying that if $\mathcal{Q}$ satisfies I-III and the hypothesis of the FP Theorem, then not $\mathcal{Q} \vdash \neg\pi(\ulcorner\neg 0 = 0\urcorner)$.

Another problem connected with the theorem is the meaning of the term "consistency." We can give a number of metamathematical definitions, but there is no reason to believe that the translations of these definitions into arithmetic are equivalent (since arithmetic is incomplete). In fact we can formulate a definition of consistency which is provable in arithmetic:

If $\mathcal{Q}$ is a consistent theory, then we may define a predicate proof' as follows:

$$\text{proof}'(x,y) \leftrightarrow \text{proof}(x,y) \wedge \bigwedge_{r,s,\ell \leq x} \neg [\text{proof}(r,s) \wedge \text{proof}(\ell, \ulcorner \neg \varphi_s \urcorner)]$$

I.e., proof'(x,y) holds iff x is the number of a proof of φ_y and no inconsistency occurs among the proofs with numbers less than ore equal to x. Then

$$\mathcal{Q} \vdash \bigwedge_{x,y,z} \neg [\text{proof}'(x,y) \wedge \text{proof}'(z, \ulcorner \neg \varphi_y \urcorner)]$$

is a provable statement of consistency.

Gödel's Second Theorem holds for Peano's arithmetic P and for all consistent extensions of P. Using this result Feferman has shown that P is not finitely axiomatizable as follows:

A consistent system $\mathcal{S}$ containing Q is <u>reflexive</u> iff for every finite subset $\mathcal{F}$ of axioms of $\mathcal{S}$, $\mathcal{S} \vdash Con_{\mathcal{F}}$, where $Con_{\mathcal{F}}$ is the formula $\neg \pi_{\mathcal{F}}(\ulcorner \neg 0 = 0 \urcorner)$ in which $\pi_{\mathcal{F}}$ is the notion of proof deriving from using $\mathcal{F}$ as the set of axioms. I.e., in a reflexive system the consistency of any finite subset of axioms is provable.

Mostowski has shown that P is reflexive and that so is any consistent extension of P with the same constants. Thus neither P nor any consistent extension of P is finitely axiomatizable (for otherwise the reflexivity of P would contradict Gödel's Second Theorem).

Existential Definability

We shall work towards proving that every r.e. set is existentially definable from the operation of exponentiation.

<u>Definition</u>. A relation $R(x_1, \ldots, x_k)$ is <u>exponential diophantine</u> iff there is an existential formula Θ whose matrix is a conjunction of equations of the form $\alpha^\beta = \gamma$, where α, β, γ are variables or particular positive integers, and $R(x_1, \ldots, x_k) \leftrightarrow \Theta(x_1, \ldots, x_k)$

Addition and multiplication are exponential diophantine relations:

$$x \cdot y = z \leftrightarrow \bigvee_{u,v} (2^x = u \wedge u^y = v \wedge 2^z = v)$$

$$x + y = z \leftrightarrow 2^x \cdot 2^y = 2^z$$

Hence, as before, the matrix of an exponential diophantine predicate may be expressed as a single equation with integer coefficients. E.g.,

$$x \cdot y = z \leftrightarrow \bigvee_{u,v} ((2^x - u)^2 + (u^y - v)^2 + (2^z - v)^2 = 0).$$

<u>Definition</u>. $E(x_1, \ldots, x_k) = 0$ is an <u>exponential diophantine</u> <u>equation</u> iff $E(x_1, \ldots, x_n)$ is a linear combination with integer coefficients of products of terms of the sort α^β.

Thus an exponential diophantine relation may be expressed as a quantified (existentially) exponential diophantine equation. This equations are of interest to number theorists in themselves. E.g., some problems concern solutions to the equations $x^x y^y = z^z$ $\quad 2^x + 11^y = 5^z$

$$2^y - 7 = x^2 \qquad x^n + y^n = z^n.$$

In order to facilitate later definitions, we show that the binomial coefficient

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!},$$

where $\alpha > k$ and α is rational, is exponentially definable. I.e., we define a relation

$$R(p,q,k,x,y) \leftrightarrow \binom{p/q}{k} = \frac{x}{y} \wedge (x,y)=1 \wedge \frac{p}{q} > k.$$

By the binomial theorem with the Lagrange estimate for the remainder, we have

$$(1+x)^{\alpha} = \sum_{j=0}^{k} \binom{\alpha}{j} x^j + \binom{\alpha}{k+1} (1+\Theta x)^{\alpha-k+1} x^{k+1}$$

for some $0 \le \Theta \le 1$. Hence

$$a^{2k+1}\left(1+\frac{1}{a^2}\right)^{\alpha} = \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1} + \binom{\alpha}{k+1}\left(1+\frac{\Theta}{a^2}\right)^{\alpha-k-1} a^{-1}.$$

An upper estimate for the value of the last term of the sum is $\alpha^{k+1} 2^{\alpha-k-1} a^{-1}$, so that by letting

$$S_k^{(\alpha)}(a) = \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1},$$

we have

$$a^{2k+1}\left(1+\frac{1}{a^2}\right)^{\alpha} = S_k^{(\alpha)}(a) + \Theta' \alpha^{k+1} 2^{\alpha-k-1} a^{-1}.$$

Also,

$$\binom{\alpha}{k} = \frac{1}{a} S_k^{(\alpha)}(a) - a S_{k-1}^{(\alpha)}(a).$$

<u>Case 1.</u> α an integer

We may choose a large enough so that the remainder in the above expansion is less than one. I.e., for $\alpha > 2^{n-k-1} n^{k+1}$,

$$S_k^{(n)}(a) = \left[a^{2k+1}\left(1+\frac{1}{a^2}\right)^n\right]$$

$$S_{k-1}^{(n)}(a) = \left[a^{2k-1}\left(1+\frac{1}{a^2}\right)^n\right].$$

$[\frac{x}{y}]$ may be defined by

$$[\tfrac{x}{y}] = z \leftrightarrow \bigvee_u (zy = x \vee (zy = x+u \wedge u<y)),$$

so that an exponential diophantine definition for $\binom{n}{k}$ is

$$\binom{n}{k} = t \leftrightarrow \bigvee_a (a > 2^{n-k-1} n^{k+1} \wedge at = [a^{2k+1}(1+\tfrac{1}{a^2})^n] - a^2[a^{2k-1}(1+\tfrac{1}{a^2})^n])$$

Case 2. $\alpha = p/q$

We first make some more preliminary definitions. For r sufficiently large, we have

$$n! = \left[\frac{r^n}{\binom{r}{n}} \right],$$

as follows:

$$\frac{r^n}{\binom{r}{n}} = n! \frac{r \cdot r \cdots r}{r(r-1)\cdots(r-n+1)}$$

$$= n! \left(1 \cdot \frac{1}{1-\frac{1}{r}} \cdots \frac{1}{1-\frac{n}{r}}\right)$$

$$\leq n! \left(\frac{1}{1-\frac{n}{r}}\right)^n \qquad \text{for } r>n.$$

But $\frac{1}{1-\theta} \leq 1+2\theta$ for $0 \leq \theta \leq \frac{1}{2}$ (since $\frac{1}{1-\theta} = 1 + \frac{\theta}{1-\theta} \leq 1+2\theta$) and hence

$$\frac{r^n}{\binom{r}{n}} \leq n! \left(1+\frac{2n}{r}\right)^n \qquad \text{for } r > 2n.$$

Also $(1+\theta)^n \leq 1+2^n\theta$ since 2^n is the sum of the binomial coefficients and θ is the largest value of $\theta, \theta^2, \theta^3, \ldots$ for $\theta < 1$. Hence

$$\frac{r^n}{\binom{r}{n}} \leq n!\left(1+2^{n+1}\frac{n}{r}\right) = n! + \frac{2^{n+1} n n!}{r}.$$

Consequently we may define

$$x = n! \leftrightarrow \bigvee_r \left(r > (2n)^{n+1} \wedge x = \left[\frac{r^n}{\binom{r}{n}} \right] \right).$$

In terms of n! we define

$$\text{prime}(x) \leftrightarrow x \nmid (x-1)!^2 .$$

Now if $q^k k! \mid a$, then $S_k^{(\frac{p}{q})}(a)$ is an integer, so that

$$\binom{p/q}{k} = \frac{x}{y} \leftrightarrow \bigvee_a \{ q^k k! \mid a \wedge a > p^{k+1} 2^{p-k-1}$$

$$\wedge\ ax = y[a^{2k+1}(1+\tfrac{1}{a^2})^{p/q}] - a^2 y [a^{2k-1}(1+\tfrac{1}{a^2})^{p/q}]$$

$$\wedge\ (x,y) = 1 \wedge p > qk \}.$$

Thus $\binom{p/q}{k}$ is exponential diophantine.

Next we may define rational powers of integers by

$$[x^{p/q}] = z \leftrightarrow z^q \leq x^p < (z+1)^q .$$

<u>Definition</u> $T(u,v,x) = \prod_{t=1}^{x} (u + vt)$

T is exponential diophantine since

$$\binom{\frac{u}{v}+x}{x} = \frac{(u+v)(u+2v)\cdots(u+xv)}{v^x \ x!}$$

and hence

$$T(u,v,x) = \binom{\frac{u}{v}+x}{x} v^x x! .$$

<u>Lemma</u>. Let $F(x, y, k, z_1, \ldots, z_m)$ be any polynomial of degree $n > 0$ with integer coefficients, and let $G(x,y)$ be any polynomial such that

(i) $G(x,y) \geq y$

(ii) $\bigwedge_{k \leq y} \bigwedge_{z_1 \cdots z_m \leq y} |F(x,y,k,z_1,\ldots,z_m)| \leq G(x,y)$.

Then

$$\bigwedge_{k \leq y} \bigvee_{z_1 \cdots z_m \leq y} F(x,y,k,z_1,\ldots,z_m) = 0$$

$$\leftrightarrow \bigvee_{c, \ell, a_1, \ldots, a_m} \Big\{ \ell = G(x,y)! \wedge 1 + c\ell = \prod_{k=1}^{y} (1 + k\ell)$$

$$\wedge \; 1 + c\ell \mid F(x, y, c, a_1, \ldots, a_m)$$

$$\wedge \bigwedge_{i \leq m} \Big[a_i > y - 1 \wedge 1 + c\ell \mid \prod_{j=1}^{y} (a_i - j) \Big] \Big\}.$$

<u>Theorem</u>. Every r.e. set is exponential diophantine.

<u>Proof</u>: By the Davis Normal Form there exists a polynomial F' with ~~[illegible]~~ integer coefficients such that

$$x \in \mathcal{S} \leftrightarrow \bigvee_{y} \bigwedge_{k \leq y} \bigvee_{z_1 \cdots z_m \leq y} F(x, y, k, z_1, \ldots, z_m) = 0.$$

The ranges of the quantifiers may be changed from natural numbers to positive integers by substituting $y-1$ for y, etc., so that the normal form holds for polynomials F over the integers.

For any F we can find a G satisfying (i) and (ii) of the Lemma by taking $G(x,y) = cx^n y^n$, where c is the sum of the absolute values of the coefficients of F and n is the degree of F. That $\mathcal{S}$ is exponential diophantine follows from the Lemma. (see note later)

<u>Proof of Lemma</u>

($\Leftarrow$) Assume $c, t, a_1, \ldots, a_m$ satisfy the condition in { }.

(a) $(1+kt, 1+\ell t) = 1$ for $k, \ell \le y$ and $k \ne \ell$

<u>Proof</u>: If $p \mid 1+kt$ and $p \mid 1+\ell t$, then $p \mid (k-\ell)t$.
$k-\ell \mid t$ since $t = G(x,y)!$ and $G(x,y) \ge y \ge k-\ell$.
Therefore $p \mid t$, which contradicts $p \nmid 1+kt$.

Let p_k be any prime which divides $1+kt$.
Then $p_k > G(x,y) \ge y$ and

$$
\begin{aligned}
F(x,y,c,a_1,\ldots,a_m) &\equiv 0 \mod ct+1 && \text{by hypothesis}\\
&\equiv 0 \mod 1+kt && \text{since } 1+kt \mid 1+ct\\
&\equiv 0 \mod p_k && \text{since } p_k \mid 1+kt.
\end{aligned}
$$

Let $z_{ik} = \text{Rem}(a_i, p_k)$. Since $1+ct \mid \prod_{j=1}^{y} (a_i - j)$, there exists a j such that $1 \le j \le y$ and

$$a_i - j \equiv 0 \mod p_k.$$

Since $p_k \ge y \ge j \ge 1$, $j = \text{Rem}(a_i, p_k)$, and hence $1 \le z_{ik} \le y$.

$$
\begin{aligned}
1+ct &\equiv 1+kt && \mod 1+kt && \text{since } 1+kt \mid 1+ct\\
ct &\equiv kt && \mod 1+kt\\
c &\equiv k && \mod 1+kt && \text{since } (t, 1+kt) = 1\\
c &\equiv k && \mod p_k
\end{aligned}
$$

Thus

$$F(x,y,c,a_1,\ldots,a_m) \equiv F(x,y,k,z_{1k},\ldots,z_{mk}) \mod p_k$$
$$F(x,y,k,z_{1k},\ldots,z_{mk}) \equiv 0 \mod p_k$$

But $|F(x,y,k,z_{1k},\ldots,z_{mk})| \le G(x,y) < p_k$, so that $F(x,y,k,z_{1k},\ldots,z_{mk}) = 0$.

($\Rightarrow$) Set $t = G(x,y)!$, $1+ct = \prod_{k=1}^{y}(1+kt)$.

By the Chinese Remainder Theorem, and by (a) above, there exist a_i such that

$$a_i \equiv z_{ik} \mod 1+kt$$

for all $k \le y$. (Note that the a_i may be bounded by $1+ct$, so that we could strengthen the Lemma.)

Then

$$1+k\ell \mid a_i - z_{ik}$$

$$1+k\ell \mid \prod_{j=1}^{y} (a_i - j) \qquad \text{since } 1 \le z_{ik} \le y$$

Hence $1+c\ell \mid \prod_{j=1}^{y} (a_i - j)$ since the factors $(1+k\ell)$ are relatively prime by (a). As above,

$$F(x, y, c, a_1, \ldots, a_m) \equiv F(x, y, k, z_{1k}, \ldots, z_{1m}) \mod 1+k\ell$$
$$\equiv 0$$

Thus $1+k\ell \mid F(x, y, c, a_1, \ldots, a_m)$

$1+c\ell \mid F(x, y, c, a_1, \ldots, a_m)$,

and the proof is completed.

<u>Note</u>: The expression in { } is actually exponential diophantine since the quantifier $\bigwedge_{i \le m}$ may be replaced by a conjunction, and the last product defined by

$$\prod_{j=1}^{y} (a_i - j) = \prod_{n=1}^{y} (a_i - y - 1 + n).$$

<u>Reference</u>: Davis, Putnam, & Robinson, <u>Annals of Mathematics</u> (1961)

From the previous theorem we conclude that there is no effective method of determining whether or not a given exponential diophantine equation is solvable in positive integers. In fact, given any proposed decision procedure, we can actually produce an equation for which the procedure fails: We number all exponential diophantine equations in some effective manner and let E_i be the i^{th} equation. For the particular variable x, we let $E_i(u)$ be obtained from E_i by substituting u for x. By the proposed decision procedure, we may list the "unsolvable" equations in a sequence $F_1, F_2, \ldots$ Let

$$V = \{ v : E_v(v) \text{ is } F_s \text{ for some } s \}.$$

V is r.e., and hence by the preceding theorem there exists an n such that

$$v \in V \text{ iff } E_n(v) \text{ is solvable.}$$

The equation $E_n(n)$ is therefore solvable iff it is unsolvable, which is a contradiction, so that the proposed procedure fails for $E_n(n)$.

In an axiomatized system of arithmetic we can list the equations which can be proved to be unsolvable. By the above argument we may construct an equation which is unsolvable but cannot be proved to be unsolvable.

Various other results (see next section) may also be proved concerning the existential definability of r.e. sets in arithmetic. These results will hopefully prove useful in answering Hilbert's Tenth Problem (whether there exists a decision procedure for solving diophantine equations) and in determining whether every r.e. set is in fact diophantine.

We shall now establish the following two theorems:

<u>Theorem 1</u>. The relation $x^y = z$ can be defined existentially in terms of $+, \cdot,$ and any infinite set of primes.

<u>Theorem 2</u>. The relation $x^y = z$ can be defined existentially in terms of $+, \cdot,$ and any binary relation $\emptyset$ satisfying

(i) $\bigvee_n \bigwedge_{u,v} (\emptyset(u,v) \rightarrow v < u * n)$,

(ii) $\neg \bigvee_n \bigwedge_{u,v} (\emptyset(u,v) \rightarrow v < u^n)$,

where $u * n$ is defined recursively by

$u * 0 = 1$

$u * (n+1) = u^{u*n}$. (I.e., $u*n = u^{u^{\cdot^{\cdot^{\cdot^{u}}}}}$ n times).

Combining these results with the preceding theorems, we obtain two further types of definability for r.e. sets. Theorem 1 gives two directions in which we may procede: We may try to show that some infinite set of primes is diophantine in order to show that every r.e. set is diophantine and hence that Hilbert's Tenth Problem is unsolvable; or we may try to produce a set which is r.e. but not diophantine.

Theorems 1 and 2 are proved using properties of Pell's Equation

$$x^2 - ay^2 = 1$$

which has solutions if a is not a square. We will be interested in the case where a is one less than a square.

<u>Lemma</u> 1. $x^2 - (a^2-1)y^2 = 1 \leftrightarrow \bigvee_n [x + y\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n]$.

<u>Proof</u>: If u, v is a solution of Pell's equation, then
$$(u + v\sqrt{a^2-1})(u - v\sqrt{a^2-1}) = 1.$$
If w, z is also a solution, then the pair r, s determined by
$$r + s\sqrt{a^2-1} = (u + v\sqrt{a^2-1})(w + z\sqrt{a^2-1})$$
is also a solution. Hence "powers" of a given solution are themselves solutions. The pair $a, 1$ is obviously a solution, and thus all pairs x, y determined by
$$x + y\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n$$
are solutions.

Conversely suppose u, v is a solution which is not a "power" of $a + \sqrt{a^2-1}$. Then there exists an n for which
$$(a + \sqrt{a^2-1})^n < u + v\sqrt{a^2-1} < (a + \sqrt{a^2-1})^{n+1}$$
Or $$1 < (u + v\sqrt{a^2-1})(a - \sqrt{a^2-1})^n < a + \sqrt{a^2-1}.$$
Let $$s + t\sqrt{a^2-1} = (u + v\sqrt{a^2-1})(a - \sqrt{a^2-1})^n.$$
As above, s, t is a solution of Pell's equation. Since for solutions x, y, $x - y\sqrt{a^2-1} \leq x + y\sqrt{a^2-1}$, we conclude that $t > 0$. Since $s + t\sqrt{a^2-1} < a + \sqrt{a^2-1}$, $s - t\sqrt{a^2-1} > a - \sqrt{a^2-1}$, and hence $t < 1$, which is impossible. Therefore all solutions of Pell's equation are "powers" of $a + \sqrt{a^2-1}$.

From Lemma 1, we may number all solutions of Pell's equation for $a > 1$ by setting
$$a_n + a_n'\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n.$$
Thus $a_0 = 1 \quad a_0' = 0$

$a_1 = a \quad a_1' = 1,$

and a recursive definition may be given for the remaining a_n, a_n'.

<u>Lemma</u> <u>2</u>. $a_{n+2} = 2a a_{n+1} - a_n$
$a'_{n+2} = 2a a'_{n+1} - a'_n$

<u>Proof</u>: (i) $a_{n+1} = a a_n + (a^2-1) a'_n$
(ii) $a'_{n+1} = a_n + a \cdot a'_n$

$$
\begin{aligned}
a_{n+2} &= a \cdot a_{n+1} + (a^2-1) a'_{n+1} \\
&= a \cdot a_{n+1} + (a^2-1) a_n + a(a^2-1) a'_n && \text{by (ii)} \\
&= a a_{n+1} + (a^2-1) a_n + a[a_{n+1} - a a_n] && \text{by (i)} \\
&= 2a a_{n+1} - a_n
\end{aligned}
$$

The other formula is proved similarly.

<u>Example</u> For $a=2$, the solutions of $x^2-3y^2=1$ are

x:	1	2	7	26	97	...
y:	0	1	4	15	56	...

<u>Lemma</u> <u>3</u>. $a_n - a'_n(a-y) \equiv y^n \mod 2ay-y^2-1$

<u>Proof</u>:

$$
\begin{aligned}
a_0 - a'_0(a-y) &= 1 \equiv y^0 \\
a_1 - a'_1(a-y) &= a-a+y = y \\
a_{n+2} - a'_{n+2}(a-y) &= 2a[a_{n+1} - a'_{n+1}(a-y)] - [a_n - a'_n(a-y)] \\
&\equiv 2a y^{n+1} - y^n \\
&\equiv (y^2+1) y^n - y^n \\
&\equiv y^{n+2}
\end{aligned}
$$

<u>Lemma</u> <u>4</u>. $a'_n \equiv n \mod a-1$

<u>Proof</u>:

$$
\begin{aligned}
a'_{n+2} &= 2a a'_{n+1} - a'_n \\
&\equiv 2a(n+1) - n \\
&\equiv 2(n+1) - n && \text{since } a \equiv 1 \mod a-1 \\
&\equiv n+2
\end{aligned}
$$

<u>Definition</u> Let $\Psi(a,u)$ be the relation

$$\bigvee_{x,y} [x^2 - (a^2-1)(a-1)^2 y^2 = 1 \wedge a>1 \wedge u = ax].$$

<u>Lemma 5</u>. $\Psi(a,u) \rightarrow u \geq a^a$

$$a>1 \rightarrow \bigvee_u [\Psi(a,u) \wedge u < a^{2a}]$$

<u>Proof</u>: Suppose $\Psi(a,u)$ holds for the particular values x,y of the bound variables. Then $x, (a-1)y$ is a solution of Pell's Equation: for some n, $x = a_n$

$$(a-1)y = a_n'$$

By Lemma 4, $0 \equiv n \mod (a-1)$.
Since we are restricting all quantifiers to positive integers, y is positive and therefore $n \neq 0$. Hence $n \geq a-1$. Since $a_n + a_n'\sqrt{a^2-1} = (a+\sqrt{a^2-1})$, we have $a_n \geq a^n$. Thus

$$u = ax = a \cdot a_n \geq a \cdot a_{a-1} \geq a \cdot a^{a-1} = a^a,$$

since the sequence $a_0, a_1, \ldots$ is increasing.

For the second part, set

$$x = a_{a-1}$$
$$(a-1)y = a'_{a-1}.$$

By Lemma 4, y is integral. Since $a \geq 2$,

$$a^{2n} \geq (2a)^n \geq a_n.$$

Setting $u = ax$, $\Psi(a,u)$ holds and

$$u = a \cdot a_{a-1} \leq a^{2(a-1)} < a^{2a}.$$

The particular definition of Ψ is unimportant, as the properties of Lemma 5 plus the fact that Ψ is existentially definable are all that is needed for the proofs of Theorems 1 and 2.

<u>Theorem 1</u>. Exponentiation is existentially definable in terms of $+$, $\cdot$, and any infinite set of primes.

<u>Proof</u>: We shall show that

$$x = y^z \leftrightarrow \bigvee_{a,r,s,p,u} \{ \text{prime}(p) \wedge \Psi(y+z,u) \wedge u \le p \wedge r^2 - (a^2-1)s^2 = 1 \wedge s \equiv z \bmod (a-1) \wedge p \mid 2ay - y^2 - 1 \wedge p-1 \mid a-1 \wedge x = \text{Rem}(r - s(a-y), p) \}.$$

Suppose a, r, s, p, u satisfy the conditions in $\{\}$. Then p is prime,

$$(y+z)^{y+z} \le u < p \quad \text{by Lemma 5}$$
$$y^z < p.$$

For some n,

$$
\begin{array}{lrcll}
 & r &=& a_n & \\
 & s &=& a_n' & \\
 & s &\equiv& n \bmod (a-1) & \text{by Lemma 4} \\
 & z &\equiv& n \bmod (a-1) & \text{since } s \equiv z \\
\text{(a)} & z &\equiv& n \bmod (p-1) & \text{since } p-1 \mid a-1 \\
 & r - s(a-y) &\equiv& y^n \bmod (2ay - y^2 - 1) & \text{by Lemma 3} \\
\text{(b)} & r - s(a-y) &\equiv& y^n \bmod p & \text{since } p \mid 2ay - y^2 - 1 \\
 & y^{z+m(p-1)} &\equiv& y^n \bmod p & \text{by (a)} \\
 & y^z &\equiv& y^n \bmod p & \text{by Fermat's Little Thm.} \\
 & r - s(a-y) &\equiv& y^z \bmod p & \text{by (b)} \\
 & x &\equiv& y^z \bmod p & \text{since } x = \text{Rem}(r - s(a-y), p)
\end{array}
$$

But $x, y^z < p$, so that $x = y^z$.

Conversely, let p be any prime (in the given set) greater than $(y+z)^{2(y+z)}$. By Lemma 5 there is a u satisfying

$$\Psi(y+z, u) \wedge u \le p.$$

Now it suffices to find an a satisfying the two divisibility conditions, for by taking $r = a_z$, $s = a_z'$, the other conditions are satisfied as above. But such an a may always be found by the Chinese Remainder Theorem.

<u>Lemma</u> <u>6</u>. If ϕ is a relation satisfying

(i) $\bigvee_n \bigwedge_{u,v} (\phi(u,v) \to v < u * n)$

(ii) $\neg \bigvee_n \bigwedge_{u,v} (\phi(u,v) \to v < u^n)$,

then there is a relation $\rho(x,y)$ definable existentially in terms of $\phi, +, \cdot$ such that

(a) $\rho(x,y) \to y < x^x$

(b) $\neg \bigvee_n \bigwedge_{u,v} (\rho(x,y) \to y < x^n)$.

<u>Proof</u>: <u>Case 1</u>: $\bigvee_k [\phi(x,y) \to y < x^{kx}]$

Let k be such a bound and define
$$\rho(x,y) \leftrightarrow \bigvee_v [\phi(x,v) \wedge y^k < v].$$
$$\rho(x,y) \to \bigvee_v [v < x^{kx} \wedge y^k < v]$$
$$\to x^{kx} > y^k$$
$$\to x^x > y.$$
By (ii), for any n, there exist u,v such that $\phi(u,v) \wedge u^{nk} \leq v$. Hence $\rho(u,u^n)$ holds, and (b) is satisfied.

<u>Case 2</u>: $\phi(x,y) \to y \leq x * n \wedge \neg \bigvee_k [\phi(x,y) \to y < x^{kx}]$.

We proceed by induction on n, defining a new function ϕ_1 for which
$$\phi_1(x,y) \to y \leq x * (n-1);$$
ϕ_1 may then be treated either under Case 1 or Case 2. Specifically, we define
$$\phi_1(x,y) \leftrightarrow \bigvee_a [\Psi(a,x) \wedge \phi(a,y)].$$
Then $\phi_1(x,y) \to \bigvee_a [x \geq a^a \wedge y \leq a * n]$ by Lemma 5

But $a * n \leq a^a * (n-1)$ ~~since a*1 = a~~ for $n > 1$ since $a * 2 = a^a = a^a * 1$ and
$$a * n = a^{a * (n-1)} \leq a^{[a^a * (n-2)]}$$
$$\leq (a^a)^{[a^a * (n-2)]} = a^a * (n-1).$$
Hence $\phi_1(x,y) \to y \leq x * (n-1)$. ~~Again by (ii),~~ For any n there exist u,v such that $\phi(u,v) \wedge v \geq u^{2nu}$ (by assumption). By Lemma 5, there is an x such that $\Psi(u,x) \wedge x < u^{2u}$. Hence $\phi_1(x,v)$ holds and $x^n < v$, so that (b) is satisfied.

<u>Theorem 2</u>. Exponentiation is existentially definable from $+, \cdot,$ and any binary relation ϕ satisfying conditions (i)-(ii) of Lemma 6.

<u>Proof</u>: Let ρ be defined from ϕ as in Lemma 6. Then we assert

$$x = y^z \leftrightarrow \bigvee_{u,a,r,r',s} \{ \Psi(y+z, u) \wedge u \le 2ay - y^2 - 1 \wedge \rho(a, r') \wedge r < r' \wedge r^2 - (a^2-1)s^2 = 1 \wedge \mathrm{Rem}(s, a-1) = z \wedge \mathrm{Rem}(r - s(a-y), 2ay - y^2 - 1) = x \}$$

Suppose u, a, r, r', s satisfy the conditions in $\{\}$. Then by Lemma 5 $\Psi(y+z, u)$ implies

$(y+z)^{y+z} \le u$

Hence $y^z < 2ay - y^2 - 1$

$r < r' < a^a$ by Lemma 6

$r < a_a$ as in Lemma 5.

For some n we have

$r = a_n$

$s = a_n'$

$s \equiv n \mod (a-1)$ by Lemma 4

$n \le a-1$ since $a_n < a_a$

Hence $z = n$ since $z = \mathrm{Rem}(s, a-1)$.

Consequently $r = a_z$ and $s = a_z'$, and by Lemma 3,

$r - s(a-y) \equiv y^z \mod 2ay - y^2 - 1$.

Thus $x = y^z$.

Conversely, by Lemma 5 there exists a u satisfying $\Psi(y+z, u)$. By Lemma 6 (arguing from both (a) and (b)), we can find an a large enough so that $u \le 2ay - y^2 - 1$ and $\rho(a, r')$ holds for some $r' > a^{2z}$. Then

$r' > a^{2z} > (a + \sqrt{a^2-1})^z = a_z$.

Hence we may take $r = a_z$ and $s = a_z'$ to satisfy the remaining conditions.

<u>Corollary</u> If there exists a r.e. set which is not diophantine then for any diophantine equation $P(x, y, u_1, \ldots, u_k) = 0$, either for all n there exists a solution of $P = 0$ with $y \geq x * n$ or there exists an n such that every solution of $P = 0$ satisfies $y < x^n$.

<u>Proof</u>: If this were not the case, P would satisfy the hypothesis of Theorem 6, and every r.e. set would be existentially definable in terms of $P, +, \cdot$; i.e., every r.e. set would be diophantine, contrary to hypothesis.

As an illustration of the corollary we consider the equation

$$x^2 = y^3 + a$$

which is known to have finitely many solutions for each a. If there were a non-diophantine r.e. set, then either there would be solutions with $y \geq x * n$ for all n or there would be an n such that $y < x^n$. Since the number of solutions is finite, the first alternative is impossible, and hence we could conclude that for some n, all solutions satisfied $y < x^n$.

Myhill Normal Form

Lemma Every r.e. set is definable in the form
$$x \in \mathcal{S} \leftrightarrow \bigvee_{u_1,\ldots,u_k,\,p} \{ P(x, p, u_1, \ldots, u_k) = 0 \wedge \text{prime}(p) \},$$

where P is a polynomial with integral coefficients.

Proof: If we examine the proof of Theorem 1 of the preceding ~~theor~~ section, we see that we may choose a single prime p sufficiently large to satisfy the definitions of all equations $x^y = z$ occurring in the exponential diophantine definition of a given r.e. set.

Theorem. (Myhill) Every r.e. set $\mathcal{S}$ is definable by a formula of the form
$$x \in \mathcal{S} \leftrightarrow \bigvee_{y} \bigwedge_{u_1 \cdots u_k} P(x, y, u_1, \ldots, u_k) \neq 0,$$

where P is a polynomial with integral coefficients.

Proof: By the Lemma there exists a P such that
$$x \in \mathcal{S} \leftrightarrow \bigvee_{\underline{u},\,p} \bigwedge_{y,z} \{ P(x, p, \underline{u}) = 0 \wedge p \neq (y+2)(z+2) \}$$
$$\leftrightarrow \bigvee_{t} \bigwedge_{\underline{u},p,y,z} \{ t = J_{k+1}(u_1, \ldots, u_k, p) \rightarrow P = 0 \wedge p \neq (y+2)(z+2) \}$$
$$\leftrightarrow \bigvee_{t} \bigwedge_{\underline{u},p,y,z,w} \{ t = J_{k+1}(\underline{u}, p) \rightarrow P^2 \neq 1 + w \wedge p \neq (y+2)(z+2) \}$$

But $f \neq g \wedge n \neq m \leftrightarrow (f-g)(n-m) \neq 0$, and $t = J_{k+1}(\underline{u}, p)$ can be written as a polynomial equation $F = G$ by multiplying both sides by 2^{k+1}. Hence $\mathcal{S}$ is expressible in the form
$$x \in \mathcal{S} \leftrightarrow \bigvee_{t} \bigwedge_{\underline{u},p,y,z,w} \{ F \neq G \vee Q \neq 0 \}$$
$$\leftrightarrow \bigvee_{t} \bigwedge_{\underline{u},p,y,z,w} (F-G)^2 + Q^2 \neq 0.$$

The quantifiers in the Myhill Normal Form may be bounded. Myhill originally conjectured falsely that we could take $u_1 \dots u_k \le y$. However it is possible to take $u_1 \dots u_k$ less than some polynomial in x and y, or to take $u_1 \dots u_k \le y$ provided that $y > x$.

As a consequence of Myhill's Theorem, we prove the following result of Putnam:

<u>Theorem</u> There does not exist a decision procedure for determining whether or not an arbitrary polynomial with integral coefficients assumes all values for integral arguments.

<u>Proof</u>: Let $\mathcal{S}$ be a r.e. but not recursive set. By Myhill's Theorem, there exists a polynomial P with integral coefficients such that

$$x \notin \mathcal{S} \leftrightarrow \bigwedge_{y} \bigvee_{\underline{u}} P(x, y, \underline{u}) = 0.$$

Hence we could decide membership in $\sim\mathcal{S}$ if we could tell if $\bigvee_{\underline{u}} P(x, y, \underline{u}) = 0$ represented all positive integers y for a fixed x. Let

$$F(x, y, \underline{u}, v, z) = y(1 - P^2) - (z-1)(y+v-1),$$

where all variables range over positive integers. (F can be made into an equation in integer variables by writing each positive variable as the sum of four squares.)

If P has a solution for $y > 0$, then

$$P(x, y, \underline{u}) = 0 \rightarrow F(x, y, \underline{u}, v, 1) = y.$$

If P has no solution for $y > 0$, then $1 - P^2 \le 0$ and $P(x, y, \underline{u}) \ne 0 \rightarrow F(x, y, \underline{u}, v, z) < 0$.

Also $F(x, 0, \underline{u}, v, 2) = 1 - v$, so that F takes on all negative values, 0, and all positive values y for which P is solvable. Hence if we had a decision procedure which enabled us to tell if F took on all values, we could decide if $\underset{\sim}{\forall}\, P(x, y, \underset{\sim}{u}) = 0$ represented all positive integers y, and thus we could decide if $x \in \sim \mathcal{S}$, contrary to assumption.

As a final comment on the relationship between diophantine and r.e. sets, we mention the following result due to Rabin (Logic and Methodology Proceedings, Stanford):

Theorem. Let $\mathfrak{A}$, $\mathfrak{B}$ be two models of the true sentences of arithmetic. $\mathfrak{B}$ is a cofinal extension of $\mathfrak{A}$ iff $\mathfrak{A} < \mathfrak{B}$ and for all b in the domain of $\mathfrak{B}$ there exists an a in the domain of $\mathfrak{A}$ such that $b < a$ holds in $\mathfrak{B}$. If there exist (non-standard) models $\mathfrak{A}$, $\mathfrak{B}$ of arithmetic such that $\mathfrak{B}$ is a cofinal but not an elementary extension of $\mathfrak{A}$, then every r.e. set is diophantine.

Final Exam - 225A

1. Prove that every consistent set of sentences of a denumerable logic without equality, individual constants, or operation symbols has a model.

2. What can a sentence containing no predicate symbols other than equality say about the size of the universe of its models? Justify your answer using the method of elimination of quantifiers.

3. Contrast the notions of completeness and model completeness. Show that the theory of a given structure is model complete iff the class of existentially definable relations in the structure is closed under complementation.

4. State Beth's Theorem carefully defining the terms you use. What is its significance?

5. Let $\mathcal{L}$ be a first order predicate logic with equality and one binary relation symbol '$<$'.

   Let $\mathcal{L}'$ be obtained from $\mathcal{L}$ by adjoining additional variables (capital letters) to represent finite sets of individuals and the relation symbol $\in$ with its usual interpretation.

   Let $\mathcal{L}''$ be obtained from $\mathcal{L}$ by adjoining additional variables (Greek letters) to represent arbitrary sets of individuals and the relation symbol $\in$ as before.

   (a) Can you characterize $<$ as an ordering relation of type ω in $\mathcal{L}$? in $\mathcal{L}'$? in $\mathcal{L}''$? If so, do so; if not, why not?

   (b) Can you characterize $<$ as a well-ordering relation in $\mathcal{L}''$? in $\mathcal{L}$?

Final Exam - 225 B

1. Discuss for 30 minutes classes of sets and functions which we have studied.

2. Let $\mathcal{T}$ be a theory in the language of arithmetic such that every recursive set is (1,2) definable. Give an informal proof that $\mathcal{T}$ is essentially hereditarily undecidable.

3. Is there a finite system Σ of functional equations in S, F, and auxiliary functions such that Σ has a solution with $F = F_0$ iff F_0 is recursive?

4. Show that the theory $\mathcal{T}$ of finite models of the following axioms

$$\left.\begin{array}{l}\Delta_m + \Delta_n = \Delta_{m+n} \\ \Delta_m \cdot \Delta_n = \Delta_{m \cdot n}\end{array}\right\} \text{for all } m, n$$

is undecidable.

5. (a) Show that there is a recursively enumerable set $\mathcal{M}$ with an infinite complement such that each infinite r.e. set has an infinite intersection with $\mathcal{M}$.

(b) Same as (a) with each occurrence of "r.e." replaced by "diophantine".