

THE UNDECIDABLE

Basic Papers on Undecidable Propositions,
Unsolvable Problems and Computable Functions

Edited by

Martin Davis

THE UNDECIDABLE

BASIC PAPERS ON
UNDECIDABLE PROPOSITIONS,
UNSOLVABLE PROBLEMS
AND COMPUTABLE FUNCTIONS

EDITED BY MARTIN DAVIS

*Professor Emeritus
Courant Institute of Mathematical Sciences
New York University*

DOVER PUBLICATIONS, INC.
Mineola, New York

This One



Материал, заслуживающий доверия
FKRX-4HC-SCLP

TO
E. L. POST
1897 - 1954

Copyright

Copyright © 1965 by Raven Press Books, Ltd.
Copyright © renewed 1993 by Martin Davis
All rights reserved.

Bibliographical Note

This Dover edition, first published in 2004, is a corrected republication of the work originally published by Raven Press Books, Ltd., Hewlett, New York, in 1965. The article beginning on page 340 of the original 1965 edition, "Absolutely Unsolvable Problems and Relatively Undecidable Propositions—Account of an Anticipation" by Emil L. Post has been updated and replaced with a newer version.

Library of Congress Cataloging-in-Publication Data

The undecidable : basic papers on undecidable propositions, unsolvable problems, and computable functions / edited by Martin Davis.

p. cm.

Originally published: Hewlett, N.Y. : Raven Press, 1965.

Includes bibliographical references and index.

ISBN 0-486-43228-9 (pbk.)

1. Gödel's theorem. 2. Unsolvability (Mathematical logic) 3. Recursive functions. 4. Turing machines. 5. Computable functions. I. Davis, Martin, 1928-

QA9.65.U53 2004

511.3—dc22

2003067180

Manufactured in the United States of America
Dover Publications, Inc., 31 East 2nd Street, Mineola, N.Y. 11501

Contents

KURT GÖDEL

<u>On Formally Undecidable Propositions of the Principia Mathematica and Related Systems. I.</u>	4
On Undecidable Propositions of Formal Mathematical Systems	39
On Intuitionistic Arithmetic and Number Theory	75
On the Length of Proofs	82
Remarks Before the Princeton Bicentennial Conference on Problems in Mathematics	84

ALONZO CHURCH

An Unsolvable Problem of Elementary Number Theory	88
A Note on the Entscheidungsproblem	108

ALAN M. TURING

On Computable Numbers, with an Application to the Entscheidungsproblem	115
Systems of Logic Based on Ordinals	154

J. B. ROSSER

An Informal Exposition of Proofs of Gödel's Theorem and Church's Theorem	223
Extensions of Some Theorems of Gödel and Church	230

STEPHEN C. KLEENE

<u>General Recursive Functions of Natural Numbers</u>	236
<u>Recursive Predicates and Quantifiers</u>	254

EMIL POST

<u>Finite Combinatory Processes. Formulation I.</u>	288
Recursive Unsolvability of a Problem of Thue	292
<u>Recursively Enumerable Sets of Positive Integers and Their Decision Problems</u>	304
Absolutely Unsolvable Problems and Relatively Undecidable Propositions- Account of an Anticipation	338
<u>Index</u>	434

ON FORMALLY UNDECIDABLE PROPOSITIONS OF THE PRINCIPIA MATHEMATICA AND RELATED SYSTEMS. I.

This remarkable paper is not only an intellectual landmark, but is written with a clarity and vigor that makes it a pleasure to read.

The reader should be warned that what Gödel calls recursive functions are now called primitive recursive functions. (The revised terminology was introduced by Kleene, this anthology, pp. 237-253).

For the reader who wishes to complete the details of the proof of Theorem V (p. 22), it is suggested that for the purpose of making the induction easier, the result be strengthened to demand that the formula in question provably represent a function.

For a remark on an application of this paper to the Entscheidungsproblem, cf. editorial remarks, p. 109.

Kurt Gödel

ON FORMALLY UNDECIDABLE PROPOSITIONS OF
PRINCIPIA MATHEMATICA AND RELATED SYSTEMS I^{1* **}

{1}

It is well known that the development of mathematics in the direction of greater precision has led to the formalization of extensive mathematical domains, in the sense that proofs can be carried out according to a few mechanical rules. The most extensive formal systems constructed up to the present time are the system of Principia Mathematica (PM)², on the one hand, and, on the other hand, the Zermelo-Fraenkel axiom system for set theory³ (which has been developed further by J. v. Neumann). Both of these systems are so broad that all methods of proof used in mathematics today can be formalized in them, i.e. can be reduced to a few axioms and rules of in-

*This translation was prepared especially for this anthology by Professor Elliott Mendelson of Queens College, New York City, with the kind permission of the Monatshefte für Mathematik und Physik, and Springer-Verlag. The original German title is: "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I"; the article appeared in vol. 38 (1931) pp. 173-198.

**Received November 17, 1930.

1. Cf. the summary of the results of this paper which appeared in the Anzeiger der Akad. d. Wiss. in Wien (math.-naturw. Kl.) 1930, Nr. 19.

2. A. Whitehead and B. Russell, Principia Mathematica. 2nd edition. Cambridge, 1925. Among the axioms of the system PM we also include, in particular, the axiom of infinity (in the form: there exist precisely denumerably many individuals), the axiom of reducibility and the axiom of choice (for all types).

3. Cf. A. Fraenkel, "Zehn Vorlesungen über die Grundlegung der Mengenlehre." Wissenschaftl. u. Hyp., Vol. XXXI. J. v. Neumann, "Die Axiomatisierung der Mengenlehre." Math. Zeitschr. 27 (1928). Journ. f. reine u. angew. Math. 154 (1925), 160 (1929). We note that, in order to complete the formalization, one must add the axioms and rules of inference of the logical calculus to the set-theoretic axioms given in the literature just cited. The arguments that follow also hold for the formal systems constructed recently by D. Hilbert and his co-workers (so far as

ference. It is reasonable therefore to make the conjecture that these axioms and rules of inference are also sufficient to decide all mathematical questions which can be formally expressed in the given systems. In what follows it will be shown that this is not the case, but rather that, in both of the cited systems, there exist relatively simple problems of the theory of ordinary whole numbers which cannot be decided on the basis of the axioms.⁴ This situation does not depend upon the special nature of the constructed systems, but rather holds for a very wide class of formal systems, among which are included, in particular, all those which arise from the given systems by addition of finitely many axioms⁵, assuming that no false sentences of the kind given in footnote 4 become provable by means of the additional axioms.

Before we go into details, let us first sketch the main ideas of the proof, naturally without making any claim to rigor. The formulas of a formal system (we limit ourselves here to the system PM) are, considered from the outside, finite sequences of primitive symbols (variables, logical constants, and parentheses or dots) and one can easily make completely precise which sequences of primitive symbols are meaningful formulas and which are not⁶. Analogously, from the formal standpoint,

these have been published up to the present). Cf. D. Hilbert, Math. Ann. 88, Abh. aus d. math. Sem. der Univ. Hamburg I (1922), VI (1928); P. Bernays, Math. Ann. 90; J. v. Neumann, Math. Zeitschr. 26 (1927); W. Ackermann, Math. Ann. 93.

4. More precisely, there exist undecidable sentences in which, other than the logical constants: — (not), V (or), (x) (for all), = (identical with), the only concepts occurring are + (addition), · (multiplication) (of natural numbers), and where the prefix (z) refers only to natural numbers.

5. In PM only those axioms are considered distinct which do not arise from each other by a change of types.

6. By a "formula of PM", we always understood here and in the sequel a formula written without abbreviations (i.e. without use of definitions). Definitions serve only to make writing briefer and are therefore theoretically superfluous.

proofs are nothing but finite sequences of formulas (with certain specifiable properties). Naturally, for metamathematical considerations, it makes no difference which objects one takes as primitive symbols, and we decide to use natural numbers⁷ for that purpose. Accordingly, a formula is a finite sequence of natural numbers⁸ and a proof-figure is a finite sequence of finite sequences of natural numbers. Metamathematical concepts (assertions) thereby become concepts (assertions) about natural numbers or sequences of such,⁹ and therefore (at least partially) expressible in the symbolism of the system PM itself. It can be shown, in particular, that the concepts "formula", "proof-figure", "provable formula" are definable within the system PM, i.e. one can produce,¹⁰ for example, a formula $F(v)$ of PM with one free variable v (of the type of a sequence of numbers) such that $F(v)$, when intuitively interpreted, says: v is a provable formula. Now we obtain an undecidable proposition of the system PM, i.e. a proposition A for which neither A nor $\neg A$ is provable, as follows:

A formula of PM with exactly one free variable, which is of the type of the natural numbers (class of classes), will be called a class-expression. We think of the class-expressions ordered in a sequence in some manner¹¹, we denote the n -th by $R(n)$, and we note that the concept "class-expression" as well as the ordering relation R can be defined in the system

7. That is, we map the primitive symbols in one-to-one fashion onto the natural numbers. (Cf. page 13) to see how this is done.)

8. That is, a mapping of a segment of the natural number sequence into the natural numbers. (Numbers, of course, cannot be spatially ordered.)

9. In other words: the process described above provides an isomorphic image of the system PM in the domain of arithmetic and one can just as well carry out all metamathematical arguments in this isomorphic image. This occurs in the following sketch of the proof, i.e. by "formula", "sentence", "variable", etc., one is always to understand the corresponding objects of the isomorphic image.

10. It would be very easy (though somewhat tedious) actually to write this formula down.

11. Say, according to increasing sum of the terms, and lexicographically for equal sums.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

citable propositions. P is essentially the system which one obtains by building the logic of PM around Peano's axioms (numbers as individuals, successor relation as undefined primitive concept).¹⁶

The primitive symbols of the system P are the following:

I. Constants: “ \neg ” (not), “ \vee ” (or), “ \forall ” (for all), “ 0 ” (zero), “ f ” (the successor of), “ $($ ”, “ $)$ ” (parentheses).

II. Variables of the first type (for individuals, i.e. natural numbers including 0): “ x_1 ”, “ y_1 ”, “ z_1 ”,

Variables of the second type (for classes of individuals): “ x_2 ”, “ y_2 ”, “ z_2 ”,

Variables of the third type (for classes of classes of individuals): “ x_3 ”, “ y_3 ”, “ z_3 ”,

— Etc., for every natural number as type.¹⁷

Remark: Variables for functions (relations) of two or more arguments are superfluous as primitive symbols, since one can define relations as classes of ordered pairs and ordered pairs, in turn, as classes of classes, e.g. define the ordered pair a, b by $((a), (a, b))$, where (x, y) denotes the class whose only elements are x and y , and (x) that whose only element is x .¹⁸

By a term of the first type we mean a combination of symbols of the form:

$a, fa, ffa, fffa, \dots$, etc.,

where a is either 0 or a variable of the first type. In the first case we call such an expression a numeral. For $n > 1$ we mean

16. The addition of Peano's axioms, as well as all other changes made in the system PM, serve only to simplify the proof and are theoretically dispensable.

17. It is assumed that, for each type, denumerably many variables are at our disposal.

18. Inhomogeneous relations can also be defined in this way, e.g. a relation between individuals and classes as a class of elements of the form $((x_2), ((x_1), x_2))$. All theorems about relations provable in PM are, as is easily seen, also provable under this method of treatment.

by a term of the n -th type just a variable of the n -th type. Combinations of symbols of the form $a(b)$, where b is a term of the n -th type and a is a term of the $(n+1)$ st type, will be called elementary formulas. We define the class of formulas as the smallest class^{18a} to which all elementary formulas belong and to which $\neg(a)$, $(a) \vee(b)$, $x \Pi(a)$ (where x is an arbitrary variable)¹⁹ also belong whenever a and b belong. We call $(a) \vee(b)$ the disjunction of a and b , $\neg(a)$ the negation of a , and $x \Pi(a)$ a generalization of a . A sentence is a formula in which no free variables occur (free variables being defined in the usual way). A formula with exactly n free individual variables (and otherwise no free variables) is called an n -ary predicate, for $n=1$ also a class expression.

By Subst $a(\overline{b})$ (where a is a formula, v is a variable, and b is a term of the same type as v) we understand the formula which arises from a when we replace v , wherever it is free, by b ²⁰. We say that a formula a is a type elevation of another formula b when a arises from b by raising the type of all variables occurring in b by the same number.

The following formulas (I through V) are called axioms (they are written with the help of the abbreviations: \cdot , \supset , $=$, $(\exists x)$, $=$ ²¹, which are defined in the well-known way, and with the use of the usual conventions on the omission of parentheses²²):

18a. With respect to this definition (and similar ones later), cf. J. Lukasiewicz and A. Tarski, "Untersuchungen über den Aussagenkalkül." Comptes Rendus des séances de la Société des Sciences et des Lettres de Varsovie XXIII (1930) Cl. III.

19. Thus, $x \Pi(a)$ is also a formula when x does not occur or does not occur free in a . Naturally, in this case, $x \Pi(a)$ has the same meaning as a .

20. In case v does not occur as a free variable in a , then Subst $a(\overline{b}) = a$. One should note that "Subst" is a metamathematical symbol.

21. As in PM I,*13, $x_1 = y_1$ is to be thought of as defined by $x_2 \Pi(x_2(z_1) \supset z_2(y_1))$ (similarly for higher types).

22. In order to obtain the axioms from the schemata as written, one must there-

- I.
1. $\infty(fx_1 = 0)$
 2. $fx_1 = fy_1 \supset x_1 = y_1$
 3. $x_2(0). x_1 \Pi (x_2(x_1) \supset x_2(fx_1)) \supset x_1 \Pi (x_2(x_1)).$

II. Every formula which arises from the following schemata by substitution of arbitrary formulas for p, q, r .

- | | |
|-------------------------|---|
| 1. $p \vee p \supset p$ | 3. $p \vee q \supset q \vee p$ |
| 2. $p \supset p \vee q$ | 4. $(p \supset q) \supset (r \vee p \supset r \vee q).$ |

III. Every formula which results from one of the two schemata

1. $v \Pi (a) \supset \text{Subst } a (\frac{v}{c})$
2. $v \Pi (b \vee a) \supset b \vee v \Pi (a)$

by making one of the following substitutions for a, v, b, c (and carrying out in 1. the operation indicated by "Subst"):

For a an arbitrary formula; for v an arbitrary variable; for b a formula in which v does not occur free; and for c a term of the same type as v , assuming that c contains no variable which is bound at a place in a at which v is free²³.

IV. Every formula which results from the schema

1. $(Eu)(v \Pi (u(v) \equiv a))$

by substituting for v (for u) an arbitrary variable of the type

fore (after performing the permitted substitutions in II, III, IV)

1. eliminate abbreviations,
2. add omitted parentheses.

One should observe that the resulting expressions must be "formulas" in the above sense. (Cf. also the precise definitions of the metamathematical concepts on page 17 ff.)

23. c is therefore either a variable or 0 or a term of the form $f \dots f u$, where u is either 0 or a variable of the first type. With respect to the concept "free (bound) at a place of a ", cf. I A5 of the paper cited in footnote 24.



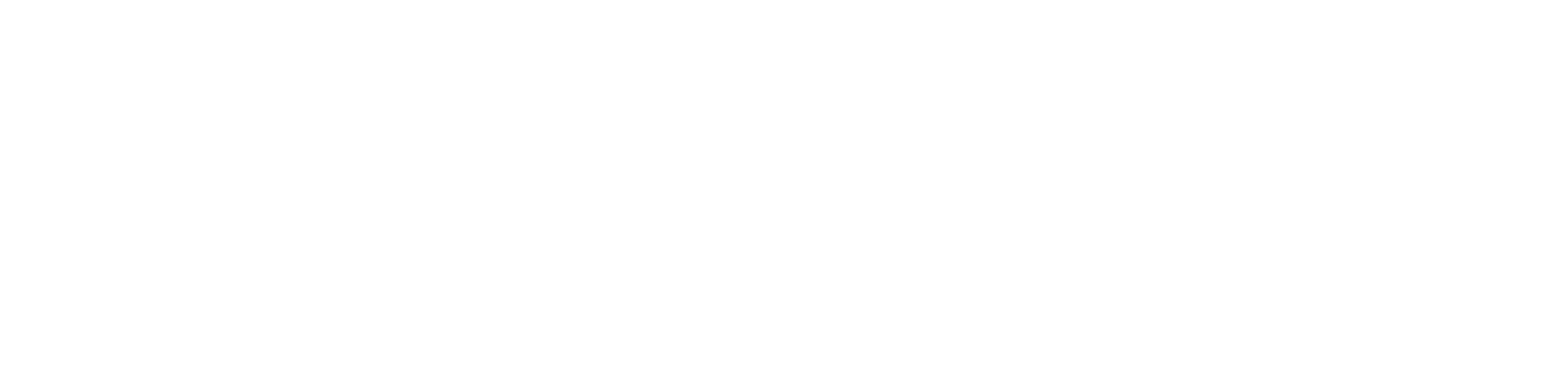
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

3. $0 \Pr x = 0$

($n+1$) $\Pr x \equiv \epsilon y [y \leq x \& \text{Prim}(y) \& x/y \& y > n \Pr x]$

$n \Pr x$ is the n -th prime factor of x (according to magnitude)^{34a}

4. $0! \equiv 1$

$(n+1)! \equiv (n+1).n!$

5. $\Pr(0) \equiv 0$

$\Pr(n+1) \equiv \epsilon y [y \leq \{\Pr(n)\}! + 1 \& \text{Prim}(y) \& y > \Pr(n)]$

$\Pr(n)$ is the n -th prime number (according to magnitude).

6. $n Gl x \equiv \epsilon y [y > x \& x/(n \Pr x)^y \& x/(n \Pr x)^{y+1}]$

$n Gl x$ is the n -th term of the sequence of numbers corresponding to the number x (for $n > 0$ and n not greater than the length of this sequence).

7. $l(x) \equiv \epsilon y [y \leq x \& y \Pr x > 0 \& (y+1) \Pr x = 0]$

$l(x)$ is the length of the sequence of numbers correlated with x

8. $x * y \equiv \epsilon z \{ z \leq [\Pr(l(x)+l(y))]^{x+y} \&$

$(n)[n \leq l(x) \rightarrow n Gl z = n Gl x] \&$

$(n)[0 < n \leq l(y) \rightarrow (n+l(x)) Gl z = n Gl y]\}$

$x * y$ corresponds to the operation of juxtaposing two finite sequences of numbers.

9. $R(x) \equiv 2^x$

$R(x)$ corresponds to the sequence of numbers consisting of only the number x (for $x > 0$).

10. $E(x) \equiv R(11) * x * R(13)$

$E(x)$ corresponds to the operation of placing in parentheses (11 and 13 are correlated with the primitive symbols "(" and ")").

11. $n \text{Var } x \equiv (Ex)[13 < z < x \& \text{Prim}(z) \& x = z^n] \& n \neq 0$

x is a VARIABLE OF THE n -TH TYPE.

12. $\text{Var}(x) \equiv (En)[n \leq x \& n \text{Var } x]$

x is a VARIABLE.

13. $\text{Neg}(x) \equiv R(5) * E(x)$

$\text{Neg}(x)$ is the NEGATION of x .

34a. For $0 < n \leq z$, where z is the number of distinct prime numbers dividing x . Observe that, for $n = z + 1$, $n \Pr x = 0$.

14. $x \text{ Dis } y \equiv E(x) * R(7) * E(y)$

$x \text{ Dis } y$ is the DISJUNCTION of x and y .

15. $x \text{ Gen } y \equiv R(x) * R(9) * E(y)$

$x \text{ Gen } y$ is the GENERALIZATION of y by means of the VARIABLE x (assuming that x is a VARIABLE).

16. $0 N x \equiv x$

$(n+1)N x \equiv R(3) * n N x$

$n N x$ corresponds to the n -fold prefixing of the symbol “ f ” in front of x .

17. $Z(n) \equiv n N [R(1)]$

$Z(n)$ is the NUMERAL for the number n .

18. $\text{Typ}_1'(x) \equiv (E n, n) \{ m, n \leq x \& [m=1 \vee 1 \text{ Var } m] \& x = n N [R(m)]\}^{34b}$

x is a TERM OF THE FIRST TYPE.

19. $\text{Typ}_n(x) \equiv [n=1 \& \text{Typ}_1'(x)] \vee [n > 1 \& (E v) \{ v \leq x \& n \text{ Var } v \& x = R(v)\}]$

x is a TERM OF THE n -TH TYPE.

20. $Elf(x) \equiv (E y, z, n) [y, z, n \leq x \& \text{Typ}_n(y) \& \text{Typ}_{n+1}(z) \& x = z * E(y)]$

x is an ELEMENTARY FORMULA.

21. $Op(x, y, z) \equiv x = \text{Neg}(y) \vee x = y \text{ Dis } z \vee (E v) [v \leq x \& \text{Var}(v) \& x = v \text{ Gen } y]$

22. $FR(x) \equiv (n) \{ 0 < n \leq l(x) \rightarrow Elf(n Gl x) \vee$

$(E p, q) [0 < p, q < n \& Op(p Gl x, p Gl x, q Gl x)]\} \& l(x) > 0$

x is a sequence of FORMULAS each one of which is either an ELEMENTARY FORMULA or comes from preceding ones by the operations of NEGATION, DISJUNCTION, or GENERALIZATION.

23. $\text{Form}(x) \equiv (E n) \{ n \leq (Pr[l(x)]^2) x [l(x)]^2 \& FR(n) \& x = [l(n)] Gl n\}^{35}$

34b. $m, n \leq x$ stands for: $m \leq x \& n \leq x$ (and similarly for more than two variables).

35. One finds the bound $n \leq (Pr[l(x)]^2) x [l(x)]^2$ as follows: the length of the shortest sequence of formulas belonging to x can be at most equal to the number of SUBFORMULAS of x . There are, however, at most $l(x)$ subformulas of length 1, at most $l(x)-1$ of length 2, etc., and, therefore, all together, at most $\frac{l(x)[l(x)+1]}{2} \leq [l(x)]^2$. The prime divisors of n can therefore all be taken

smaller than $Pr\{[l(x)]^2\}$, their number $\leq l(x)^2$ and their exponents (which are SUBFORMULAS of x) $\leq x$.

x is a FORMULA (i.e. last term of a SEQUENCE OF FORMULAS n).

24. $v \text{ Geb } n, x \equiv \text{Var}(v) \& \text{Form}(x) \&$

$(Ea, b, c)[a, b, c \leq x \& x = a * (v \text{ Gen } b) * c]$

$\& \text{Form}(b) \& l(a) + 1 \leq n \leq l(a) + l(v \text{ Gen } b)$

The VARIABLE v is BOUND at the n -th place in x .

25. $v Fr n, x \equiv \text{Var}(v) \& \text{Form}(x) \& v = n Gl x \& n \leq l(x) \& \overline{v \text{ Geb } n, x}$

The VARIABLE v is FREE at the n -th place in x .

26. $v Fr x \equiv (En)[n \leq l(x) \& v Fr n, x]$

v occurs in x as a FREE VARIABLE.

27. $Su x(\frac{n}{y}) \equiv \epsilon z \{z \leq [Pr(l(x) + l(y))]^{z+v} \& [(Eu, v)(u, v \leq x \& x = u * R(n Gl x) * v \& z = u * y * v \& n = l(u) + 1)]\}$

$Su x(\frac{n}{y})$ arises from x by substituting y in place of the n -th term of x (assuming that $0 < n \leq l(x)$).

28. $0 St v, x \equiv \epsilon n \{n \leq l(x) \& v Fr n, x \& (\overline{Ep})[n < p \leq l(x) \& v Fr p, x]\}$

$(k+1) St v, x \equiv \epsilon n \{n < k St v, x \& v Fr n, x \& (\overline{Ep})[n < p < k St v, x \& v Fr p, x]\}$

$k St v, x$ is the $(k+1)$ st place in x (counting from the end of the FORMULA x) at which v is FREE in x (and 0, in case there is no such place).

29. $A(v, x) \equiv \epsilon n \{n \leq l(x) \& n St v, x = 0\}$

$A(v, x)$ is the number of places at which v is FREE in x .

30. $Sb_0(x \frac{v}{y}) \equiv x$

$Sb_{k+1}(x \frac{v}{y}) \equiv Su[Sb_k(x \frac{v}{y})] ({}^k St \frac{v}{y}, x)$

31. $Sb(x \frac{v}{y}) \equiv Sb_{A(v, x)}(x \frac{v}{y})^{36}$

$Sb(x \frac{v}{y})$ is the concept $Subst a(\frac{v}{b})$ defined above.³⁷

32. $x Imp y \equiv [Neg(x)] Dis y$

$x Con y \equiv Neg \{[Neg(x)] Dis[Neg(y)]\}$

$x Aeq y \equiv (x Imp y) Con(y Imp x)$

$v Ex y \equiv Neg \{v Gen[Neg(y)]\}$

33. $n Th x \equiv \epsilon y \{y \leq x^{(zn)} \& (k)[k \leq l(x) \rightarrow$

$(k Gl x \leq 13 \& k Gl y = k Gl x) \vee$

$(k Gl x > 13 \& k Gl y = k Gl x \cdot [1 Pr(k Gl x)]^n]\}$

36. In case v is not a variable or x is not a formula, then $Sb(x \frac{v}{y}) = x$

37. Instead of $Sb[Sb(x \frac{v}{y})^w]$ we write $Sb(x \frac{v}{y}^w)$ (and similarly for more than two VARIABLES).



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Then:

Lemma 1: If f is an arbitrary sequence of natural numbers and k is an arbitrary natural number, then there exists a pair of natural numbers n, d such that $f^{(n,d)}$ and f coincide in their first k terms.

Proof: Let l be the greatest of the numbers $k, f_0, f_1, \dots, f_{k-1}$. Determine n so that

$$n \equiv f_i \pmod{1+(i+1)l!} \quad \text{for } i=0, 1, \dots, k-1,$$

which is possible, since any two of the numbers $1+(i+1)l!$ ($i=0, 1, \dots, k-1$) are relatively prime. For, a prime dividing two of these numbers must also divide the difference $(i_1 - i_2)l!$ and therefore, since $i_1 - i_2 < l$, must also divide $l!$, which is impossible. The number pair $n, l!$ fulfills our requirement.

Since the relation $x = [n]_p$ is defined by

$$x \equiv n \pmod{p} \quad \& \quad x < p$$

and is therefore arithmetical, then so also is the relation $P(x_0, x_1, \dots, x_n)$ defined as follows:

$$P(x_0, \dots, x_n) \equiv (En, d) \{ S([n]_{d+1}, x_2, \dots, x_n) \& (k)[k < x_1 \rightarrow T([n]_{1+d(k+2)}, k, [n]_{1+d(k+1)}, x_2, \dots, x_n)] \& x_0 = [n]_{1+d(x_1+1)} \}$$

which, according to (17) and Lemma 1, is equivalent to $x_0 = \phi(x_1, \dots, x_n)$ (in the sequence f in (17) only its values up to the (x_1+1) th term matter). Thus, Theorem VII is proved.

According to Theorem VII, for every problem of the form $(x)F(x)$ (F recursive), there is an equivalent arithmetical problem, and since the whole proof of Theorem VII can be formulated (for each particular F) within the system P , this equivalence is provable in P . Therefore we have:

Theorem VIII: There exist undecidable arithmetical propositions in each of the formal systems⁵³ mentioned in Theorem VI.

53. They are those ω -consistent systems which result from P by addition of a recursively definable class of axioms.

The same holds also (according to the remark on page 28) for the axiom system of set theory and its extensions by ω -consistent recursive classes of axioms.

Finally, we derive the following result:

Theorem IX: In all of the formal systems⁵³ mentioned in Theorem VI there exist undecidable problems of the restricted functional calculus⁵⁴ (i.e. formulas of the restricted functional calculus for which neither the universal validity nor the existence of a counter-example is provable).⁵⁵

This is based upon:

Theorem X: Every problem of the form $(x)F(x)$ (F recursive) can be reduced to the question of the satisfiability of a formula of the restricted functional calculus (i.e. for each recursive F one can produce a formula of the restricted functional calculus whose satisfiability is equivalent to the truth of $(x)F(x)$).

We consider as formulas of the restricted functional calculus (r.f.) those formulas which are built up from the primitive symbols: —, \vee , (x) , $=$; x , y , ... (individual variables); $F(x)$, $G(x, y)$, $H(x, y, z)$, ... (variables for properties and relations), where (x) and $=$ refer only to individuals.⁵⁶ We add to these

54. Cf. Hilbert-Ackermann, Grundzüge der theoretischen Logik. In the system P by formulas of the restricted functional calculus we are to understand those which arise from formulas of the restricted functional calculus of PM by the substitution indicated on p. 10 of classes of higher type for relations.

55. In my paper: "Die Vollständigkeit der Axiome des logischen Functionenkalküls", Monatsch. f. Math. u. Phys. XXXVII, 2, I have shown that every formula of the restricted functional calculus either can be proved to be universally valid or has a counter-example; the existence of this counter-example is, however, according to Theorem IX, not always provable (in the given formal systems).

56. D. Hilbert and W. Ackermann, in the book cited above, do not consider the symbol $=$ as belonging to the restricted functional calculus. However, for every formula in which the symbol $=$ occurs, there exists a formula without this symbol which is satisfiable if and only if the original one is (cf. the paper cited in footnote 55).

symbols a third kind of variable $\phi(x)$, $\psi(x, y)$, $x(x, y, z)$, etc., which represent objective functions (i.e. $\phi(x)$, $\psi(x, y)$, etc. denote single valued functions whose arguments and values are individuals⁵⁷). A formula which, in addition to the symbols of the r.f. initially mentioned above also contains variables of the third kind ($\phi(x)$, $\psi(x, y)$, ..., etc.), shall be called a formula in the wider sense (i.w.s.).⁵⁸ The concepts "satisfiable", "universally valid" carry over without any further ado to formulas i.w.s., and we have the theorem that, for every formula i.w.s. A , one can give an ordinary formula B of the r.f. such that the satisfiability of A is equivalent with that of B . One obtains B from A by replacing the variables of the third kind $\phi(x)$, $\psi(x, y)$, ... occurring in A by expressions of the form $(\exists z)F(z, x)$, $(\exists z)G(z, x, y)$, ..., then by eliminating the "descriptive" functions in the sense of PM. I*14, and by logically multiplying⁵⁹ the formula thus obtained by an expression which says that the F , G , ... replacing ϕ , ψ , ... are single valued with respect to the first argument.

We shall now show that, for every problem of the form $(x)F(x)$ (F recursive), there is an equivalent problem concerning the satisfiability of a formula i.w.s., from which, according to the remark just made, Theorem X follows.

Since F is recursive, there is a recursive function $\Phi(x)$ such that $F(x) \sim [\Phi(x)=0]$, and for Φ there is a sequence of functions $\Phi_1, \Phi_2, \dots, \Phi_n$ such that $\Phi_n = \Phi$, $\Phi_1(x) = x+1$ and, for every Φ_k ($1 < k \leq n$), either:

$$1. (x_2, \dots, x_m)[\Phi_k(0, x_2, \dots, x_m) = \Phi_p(x_2, \dots, x_m)] \quad (18)$$

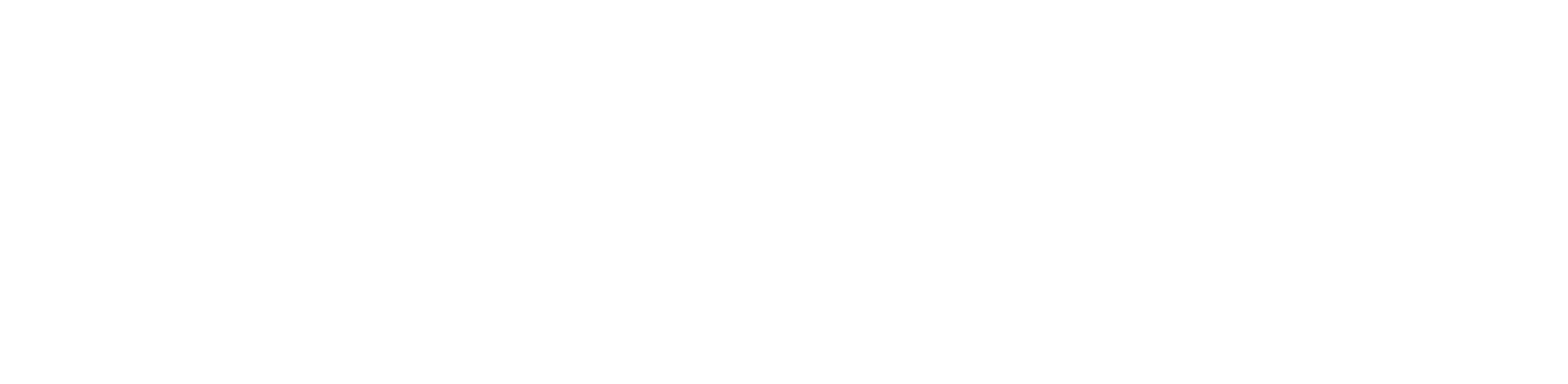
$$(x, x_2, \dots, x_m)\{\Phi_k[\Phi_1(x), x_2, \dots, x_m] = \Phi_q[x, \Phi_k(x, x_2, \dots, x_m), x_2, \dots, x_m]\}$$

$$p, q < k$$

57. And, in addition, the domain of definition shall always be the entire domain of individuals.

58. Variables of the third kind are permitted to replace individual variables at all argument places, e.g.: $y = \phi(x)$, $F(x, \phi(y))$, $G(\psi(x, \phi(y)), x)$, etc.

59. I.e. forming the conjunction.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



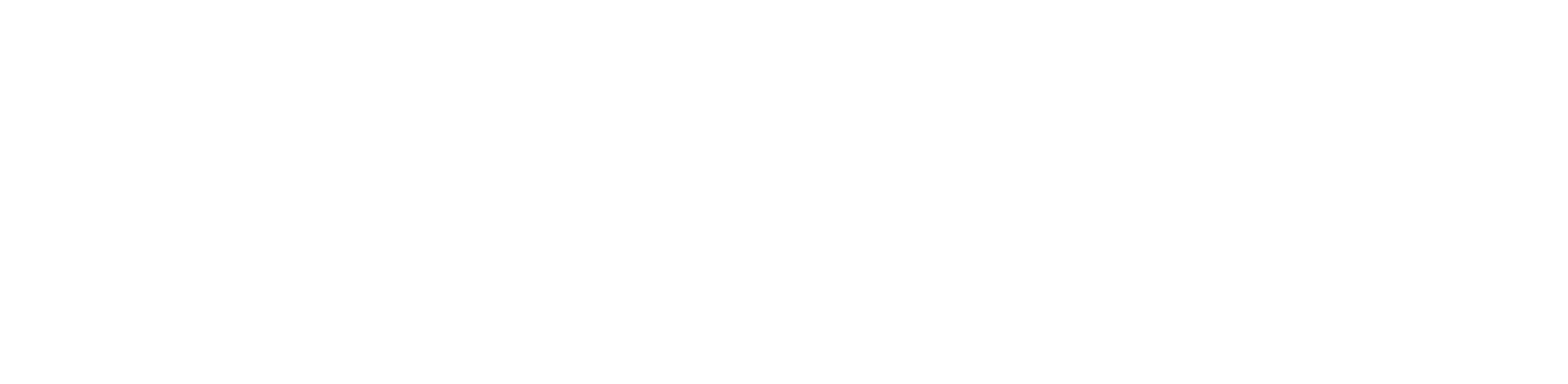
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



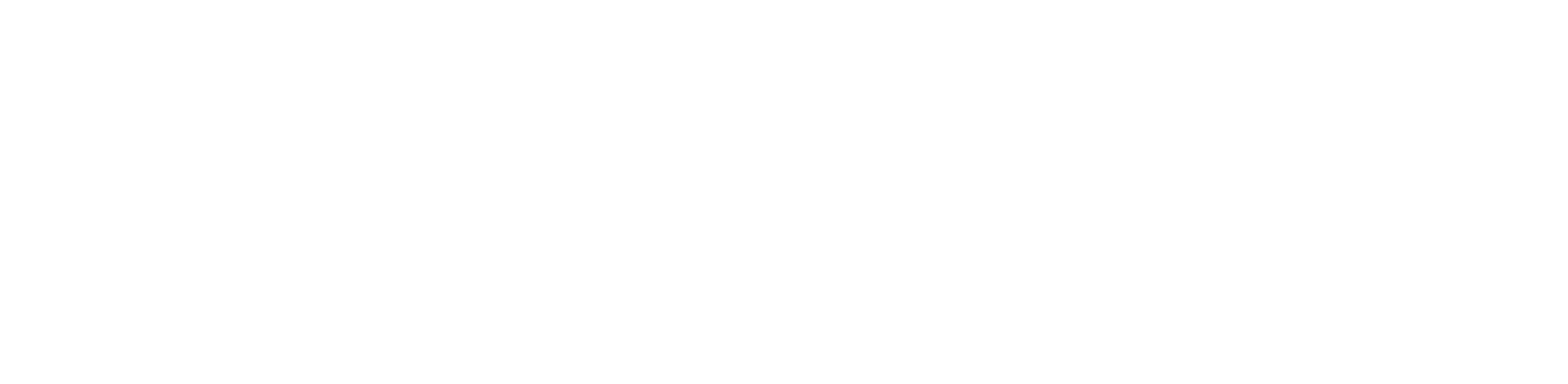
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

2. Suppose that A is meaningful,¹⁴ that t is a variable, and that t does not occur in A .

- If $(A) \rightarrow (B)$, then $(A) \rightarrow (\Pi t(B))$.
- If $(A) \rightarrow (\Pi t(B))$, then $(A) \rightarrow (B)$.

3. Suppose that A is meaningful, that t is a variable, and t does not occur in B .

- If $(A) \rightarrow (B)$, then $(\Sigma t(A)) \rightarrow (B)$.
- If $(\Sigma t(A)) \rightarrow (B)$, then $(A) \rightarrow (B)$.

4a. Suppose that x is a variable for a number, that A contains x as a free variable, that G is an expression of the first kind, and that no free variable of G is bound in F .

If A , then Subst $[A_G^x]$.

4b. Suppose that f is a variable for a function, that A contains f as a free variable, that x is a variable for a number, that $G(x)$ is an expression of the 1st kind in which x occurs as a free variable, and that no free variable of $G(x)$ or A is bound in either $G(x)$ or A , and that, moreover, $G(x)$ and A have no common bound variables.}

If A , then Subst $[A_{G(x),x}^f]$.

4c. Suppose that p is a variable for a proposition, that A contains p as a free variable, that P is an expression of the IIInd kind, and that no free variable of P is bound in A .

If A , then Subst $[A_P^p]$.

4d. Suppose that x is a variable for a number, and that $F(x)$ is meaningful and contains x as a free variable, {and no free variable of F occurs as a bound variable in F .}

If $(A) \rightarrow (F(x))$, then $(A) \rightarrow (F(\epsilon x[F(x)]))$.¹⁵

14. This condition ensures that, when $(A) \rightarrow (B)$ is a meaningful formula, the occurrence of \rightarrow which separates (A) from (B) in $(A) \rightarrow (B)$ should be the last occurrence of \rightarrow introduced in the construction of $(A) \rightarrow (B)$ according to the definition of meaningful formula. (We may say then that the main operation of $(A) \rightarrow (B)$ is an implication, whose first and second terms are A and B , respectively.) It excludes such possibilities as that A be $p \rightarrow q \rightarrow ((q \rightarrow r, \text{ when } (A) \rightarrow (B) \text{ is Axiom A1.})$

15. If $F(x)$ is an expression of the IIInd kind containing the variable x for a num-

5. Suppose that x is a variable for a number, and that $F(x)$ is a meaningful formula in which x occurs as a free variable.

If $F(0)$ and $(F(x)) \rightarrow (F(N(x)))$, then $F(x)$.

6. Suppose that s and t are variables of the same kind, that s does not occur in A as a free variable, and that t does not occur in A . Let A' denote the result of substituting t for s throughout A . Suppose that A is meaningful, and let B' denote the expression obtained from B by the substitution of A' for a given occurrence of A in B .

If B , then B' .¹⁶

One process used in mathematical proof is not represented in this system, namely the definition and introduction of new symbols. However, this process is not essential, but merely a matter of abbreviation.

ber as a free variable, then, with the aid of this rule, $\Sigma x F(x) \rightarrow F(\epsilon x [F(x)])$ is provable in our formal system. For Rule 4c allows us to infer $(p \rightarrow [(\neg p) \rightarrow p]) \rightarrow (([(\neg p) \rightarrow p] \rightarrow p) \rightarrow (p \rightarrow p))$ from Axiom A1 (i.e., by substituting $(\neg p) \rightarrow p$ for q and p for r), and $p \rightarrow [(\neg p) \rightarrow p]$ from Axiom A3 (by substituting p for q). Then Rule 1 allows us from these two results to infer $(([\neg p) \rightarrow p] \rightarrow p) \rightarrow (p \rightarrow q)$, and then from the latter and Axiom A2 to infer $p \rightarrow p$. Thence we can successively infer $F(x) \rightarrow F(x)$ by Rule 4c (by substituting $F(x)$ for p), $F(x) \rightarrow F(\epsilon x [F(x)])$ by Rule 4d, $F(x) \rightarrow F(\epsilon y [F(y)])$ by one or more applications of Rule 6, $\Sigma x [F(x)] \rightarrow F(\epsilon y [F(y)])$ by Rule 3a, and $\Sigma x [F(x)] \rightarrow F(\epsilon z [F(z)])$ by Rule 6. Thus the last formula, which expresses the essential property of ϵ , is proved in our formal system. If the system admitted the use of ϵ with variables for functions (i.e., if a rule of inference 4d', obtained from 4d by replacing "x" by "f" and "number" by "function", were added), then similarly, for any expression $G(x)$ containing the variable f for a function as a free variable, $\Sigma f [F(f) \rightarrow G(\epsilon f [G(f)])]$ would be provable. The latter formula expresses the axiom of choice for classes of functions of integers.

Note that by our formal rule for ϵ we cannot prove that $\epsilon x F(x)$ is the smallest integer x for which $F(x)$, nor that $\epsilon x F(x) = 0$ if there is no such integer, but we can prove only that if there are integers x satisfying $F(x)$, then $\epsilon x F(x)$ is one of them (i.e. $\Sigma x [F(x) \rightarrow F(\epsilon x [F(x)])]$). This however suffices for all applications.

¹⁶Note that B may be A itself (then B' is A').

4. A representation of the system by a system of positive integers

For the considerations which follow, the meaning of the symbols is immaterial, and it is desirable that they be forgotten. Notions which relate to the system considered purely formally may be called *metamathematical*.

The undefined terms (hence the formulas and proofs) are countable, and hence a representation of the system by a system of positive integers can be constructed, as we shall now do.

We order the numbers 1-13 to symbols thus:

$$\begin{array}{ccccccccccccc} 0 & N & = & \infty & \vee & \& \rightarrow & = & \Pi & \Sigma & \epsilon & (&) \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13, \end{array}$$

the integers > 13 and $\equiv 0 \pmod{3}$ to the variables for propositions, the integers $> 13, \equiv 1 \pmod{3}$ to the variables for numbers, and the integers $> 13, \equiv 2 \pmod{3}$ to the variables for functions. Thus a one-to-one correspondence is established between the undefined terms and the positive integers.

We order single integers to finite sequences of positive integers by means of the scheme

$$k_1, \dots, k_n \text{ corresponds to } 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \dots p_n^{k_n},$$

where p_i is the i -th prime number (in order of magnitude). A formula is a finite sequence of undefined terms, and a proof a finite sequence of formulas. To each formula we order the integer which corresponds to the sequence of the integers ordered to its symbols; and to each proof we order the integer which corresponds to the sequence of the integers which are then ordered to its member formulas. Then a one-to-one correspondence is determined between formulas (proofs) and a subset of the positive integers.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



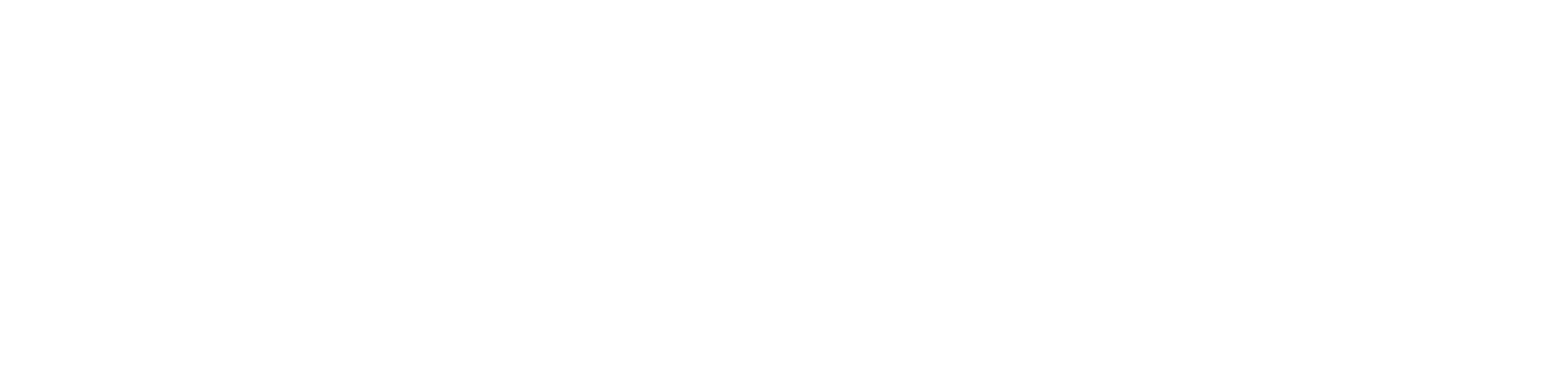
You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

(1a) Any expression obtained by replacing all the variables of one of the given equations by natural numbers shall be a derived equation.

(1b) $\psi_{ij}(k_1, \dots, k_n) = m$ shall be a derived equation if k_1, \dots, k_n , are natural numbers, and $\psi_{ij}(k_1, \dots, k_n) = m$ is a true equality.

(2a) If $\psi_{ij}(k_1, \dots, k_n) = m$ is a derived equation, the equality obtained by substituting m for an occurrence of $\psi_{ij}(k_1, \dots, k_n)$ in a derived equation shall be a derived equation.

(2b) If $\phi(k_1, \dots, k_l) = m$ is a derived equation where k_1, \dots, k_l, m are natural numbers, the expression obtained by substituting m for an occurrence of $\phi(k_1, \dots, k_l)$ on the right-hand side of a derived equation shall be a derived equation.

Now our second restriction on Herbrand's definition of recursive function is that for each set of natural numbers k_1, \dots, k_l , there shall be one and only one m such that $\phi(k_1, \dots, k_l) = m$ is a derived equation.

Using this definition of the notion of a recursive function, we can prove that, if $\phi(x_1, \dots, x_l)$ is recursive, there is an arithmetical expression $A(x_1, \dots, x_l, y)$ such that $\phi(x_1, \dots, x_l) = y \equiv A(x_1, \dots, x_l, y)$.

-POSTSCRIPTUM-

In consequence of later advances, in particular of the fact that, due to A.M. Turing's work, a precise and unquestionably adequate definition of the general concept of formal system can now be given, the existence of undecidable arithmetical propositions and the non-demonstrability of the consistency of a system in the same system can now be proved rigorously for every consistent formal system containing a certain amount of finitary number theory.

Turing's work gives an analysis of the concept of "mechanical procedure" (alias "algorithm" or "computation procedure" or "finite combinatorial procedure"). This concept is shown to be equivalent with that of a "Turing machine". * A formal system can simply be defined to be any mechanical procedure for producing formulas, called provable formulas. For any formal system in this sense there exists one in the sense of page 41 above that has the same provable formulas (and likewise vice versa), provided the term "finite procedure" occurring on page 41 is understood to mean "mechanical procedure". This meaning, however, is required by the concept of formal system, whose essence it is that reasoning is completely replaced by mechanical operations on formulas. (Note that the question of whether there exist finite non-mechanical procedures** not equivalent with any algorithm, has nothing whatsoever to do with the adequacy of the definition of "formal system" and of "mechanical procedure".)

On the basis of the definitions just mentioned, condition (1) in §6 becomes superfluous, because for any formal system provability is a predicate of the form $(Ex)x\mathfrak{B}y$, where \mathfrak{B} is primitive recursive. Moreover, the two incompleteness results mentioned in the end of §8 can now be proved in the definitive form: "There exists no formalized theory that answers all Diophantine questions of the form $(P)[F=0]$ ", and: "There is no algorithm for deciding relations in which both + and \times occur." (For theories and procedures in the more general sense indicated in footnote ** the situation may be different. Note

* See A. Turing, Proc. London Math. Soc., vol. 42 (1937), p. 249 (this anthology, p. 135) and the almost simultaneous paper by E.L. Post in J. S. L. 1 (1936) p. 103 (this anthology, p. 289). As for previous equivalent definitions of computability, which, however, are much less suitable for our purpose, see A. Church, Am. J. Math., vol. 58 (1936), pp. 356-358 (this anthology, pp. 100-102). One of those definitions is given in §9 of these lectures.

** I.e., such as involve the use of abstract terms on the basis of their meaning. See my paper in Dial. 12 (1958), p. 280.

that the results mentioned in this postscript do not establish any bounds for the powers of human reason, but rather for the potentialities of pure formalism in mathematics.) Thirdly, if "finite procedure" is understood to mean "mechanical procedure", the question raised in footnote 3 can be answered affirmatively for recursiveness as defined in §9, which is equivalent with general recursiveness as defined today (see S. C. Kleene, Math. Ann. 112 (1936), p. 730 [this anthology p. 240] and Introduction to Metamathematics, 1952, p. 220ff, p. 232ff).

As for the elimination of ω -consistency (first accomplished by J.B. Rosser [cf. this anthology, pp. 231-235]) see A. Tarski, Undecidable Theories, 1953, p. 49, Cor. 2. The proof of the unprovability in the same system of the consistency of a system was carried out for number theory in Hilbert-Bernays, Grundlagen der Mathematik, vol. 2 (1939), pp. 297-324. The proof carries over almost literally to any system containing, among its axioms and rules of inference, the axioms and rules of inference of number theory. As to the consequences for Hilbert's program see my paper in Dial. 12 (1958), p. 280 and the material cited there. See also: G. Kreisel, Dial. 12 (1958), p. 346.

By slightly strengthening the methods used above in §8, it can easily be accomplished that the prefix of the undecidable proposition consists of only one block of universal quantifiers followed by one block of existential quantifiers, and that, moreover, the degree of the polynomial is 4. (unpublished result.)

A number of misprints and oversights in the original mimeographed lecture notes have been corrected in this volume. I am indebted to Professor Martin Davis for calling my attention to some of them.

Kurt Gödel

Princeton, N. J.
June 3, 1964

[EDITOR'S NOTE- In addition to the corrections and emendations supplied by Dr. Gödel for this anthology and incorporated into the body of the text, a number of additional items received too late for inclusion in the text proper are listed below.]

Page 43, footnote 2: replace "could have been" by "should be".

Page 44, footnote 3:{this statement is outdated; see the Postscript.}

Page 69, footnote 29a: "Note that the axioms about all sets or about classes of sets that are assumed today do not carry any farther, because they are assumed to hold also for the sets of some definite type (or "rank", according to current terminology). See A. Levy, Fund. Math. 49 (1960), p. 1. The principles of proof of intuitionistic mathematics are not taken into account here, because, at any rate up to now, they have proved weaker than those of classical mathematics.}"

Page 69, footnote 30: substitute the following: "By a complete theory of some class of problems on the basis of certain principles of proof we here mean a theorem, demonstrable on this basis, which states that (and how) the solution of any problem of the class can be obtained on this basis. For a different and more definitive version of this incompleteness result see the postscript.}"



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

A function F , for which the range of the dependent variable is contained in the class of positive integers and the range of the independent variable, or of each independent variable, is a subset (not necessarily the whole) of the class of positive integers, will be called *potentially recursive*, if it is possible to find a recursive function F' of positive integers (for which the range of the independent variable, or of each independent variable, is the whole of the class of positive integers), such that the value of F' agrees with the value of F in all cases where the latter is defined.

By an *operation on* well-formed formulas we shall mean a function for which the range of the dependent variable is contained in the class of well-formed formulas and the range of the independent variable, or of each independent variable, is the whole class of well-formed formulas. And we call such an operation recursive if the corresponding function obtained by replacing all formulas by their Gödel representations is potentially recursive.

Similarly any function for which the range of the dependent variable is contained either in the class of positive integers or in the class of well-formed formulas, and for which the range of each independent variable is identical either with the class of positive integers or with the class of well-formed formulas (allowing the case that some of the ranges are identical with one class and some with the other), will be said to be recursive if the corresponding function obtained by replacing all formulas by their Gödel representations is potentially recursive. We call an infinite sequence of well-formed formulas recursive if the corresponding infinite sequence of Gödel representations is recursive. And we call a property of, or relation between, well-formed formulas recursive if the corresponding property of, or relation between, their Gödel representations is potentially recursive. A set of well-formed formulas is said to be recursively enumerable if there exists a recursive infinite sequence which consists entirely of formulas of the set and contains every formula of the set at least once.¹¹

In terms of the notion of recursiveness we may also define a *proposition of elementary number theory*, by induction as follows. If ϕ is a recursive propositional function of n positive integers (defined by giving a particular set of recursion equations for the corresponding function whose values are 2 and 1) and if x_1, x_2, \dots, x_n are variables which take on positive integers as values, then $\phi(x_1, x_2, \dots, x_n)$ is a proposition of elementary number theory. If P is a proposition of elementary number theory involving x as a free

¹¹ It can be shown, in view of Theorem V below, that, if an infinite set of formulas is recursively enumerable in this sense, it is also recursively enumerable in the sense that there exists a recursive infinite sequence which consists entirely of formulas of the set and contains every formula of the set exactly once.

variable, then the result of substituting a particular positive integer for all occurrences of x as a free variable in P is a proposition of elementary number theory, and $(x)P$ and $(\exists x)P$ are propositions of elementary number theory, where (x) and $(\exists x)$ are respectively the universal and existential quantifiers of x over the class of positive integers.

It is then readily seen that the negation of a proposition of elementary number theory or the logical product or the logical sum of two propositions of elementary number theory is equivalent, in a simple way, to another proposition of elementary number theory.

5. Recursiveness of the Kleene φ -function. We prove two theorems which establish the recursiveness of certain functions which are definable in words by means of the phrase, "The least positive integer such that," or, "The n -th positive integer such that."

THEOREM IV. *If F is a recursive function of two positive integers, and if for every positive integer x there exists a positive integer y such that $F(x, y) > 1$, then the function F^* , such that, for every positive integer x , $F^*(x)$ is equal to the least positive integer y for which $F(x, y) > 1$, is recursive.*

For a set of recursion equations for F^* consists of the recursion equations for F together with the equations,

$$\begin{array}{ll} i_2(1, 2) = 2, & g_2(x, 1) = i_2(f_2(x, 1), 2), \\ i_2(S(x), 2) = 1, & g_2(x, S(y)) = i_2(f_2(x, S(y)), g_2(x, y)), \\ i_2(x, 1) = 3, & h_2(S(x), y) = x, \\ i_2(x, S(S(y))) = 3, & h_2(g_2(x, y), x) = j_2(g_2(x, y), y), \\ j_2(1, y) = y, & f_1(x) = h_2(1, x), \\ j_2(S(x), y) = x, & \end{array}$$

where the functional variables f_2 and f_1 denote the functions F and F^* respectively, and 2 and 3 are abbreviations for $S(1)$ and $S(S(1))$ respectively.¹²

THEOREM V. *If F is a recursive function of one positive integer, and if there exist an infinite number of positive integers x for which $F(x) > 1$, then the function F^o , such that, for every positive integer n , $F^o(n)$ is equal to the n -th positive integer x (in order of increasing magnitude) for which $F(x) > 1$, is recursive.*

¹² Since this result was obtained, it has been pointed out to the author by S. C. Kleene that it can be proved more simply by using the methods of the latter in *American Journal of Mathematics*, vol. 57 (1935), p. 231 *et seq.* His proof will be given in his forthcoming paper already referred to.

For a set of recursion equations for F^0 consists of the recursion equations for F together with the equations,

$$\begin{aligned}g_2(1, y) &= g_2(f_1(S(y)), S(y)), \\g_2(S(x), y) &= y, \\g_1(1) &= k, \\g_1(S(y)) &= g_2(1, g_1(y)),\end{aligned}$$

where the functional variables g_1 and f_1 denote the functions F^0 and F respectively, and where k is the numeral to which corresponds the least positive integer x for which $F(x) > 1$.¹³

6. Recursiveness of certain functions of formulas. We list now a number of theorems which will be proved in detail in a forthcoming paper by S. C. Kleene¹⁴ or follow immediately from considerations there given. We omit proofs here, except for brief indications in some instances.

Our statement of the theorems and our notation differ from Kleene's in that we employ the set of positive integers $(1, 2, 3, \dots)$ in the rôle in which he employs the set of natural numbers $(0, 1, 2, \dots)$. This difference is, of course, unessential. We have selected what is, from some points of view, the less natural alternative, in order to preserve the convenience and naturalness of the identification of the formula $\lambda ab \cdot a(b)$ with 1 rather than with 0.

THEOREM VI. *The property of a positive integer, that there exists a well-formed formula of which it is the Gödel representation is recursive.*

THEOREM VII. *The set of well-formed formulas is recursively enumerable.*

This follows from Theorems V and VI.

THEOREM VIII. *The function of two variables, whose value, when taken of the well-formed formulas \mathbf{F} and \mathbf{X} , is the formula $\{\mathbf{F}\}(\mathbf{X})$, is recursive.*

THEOREM IX. *The function, whose value for each of the positive integers $1, 2, 3, \dots$ is the corresponding formula $1, 2, 3, \dots$, is recursive.*

THEOREM X. *A function, whose value for each of the formulas $1, 2, 3, \dots$ is the corresponding positive integer, and whose value for other well-formed formulas is a fixed positive integer, is recursive. Likewise the function, whose value for each of the formulas $1, 2, 3, \dots$ is the corresponding positive integer*

¹³ This proof is due to Kleene.

¹⁴ S. C. Kleene, "λ-definability and recursiveness," forthcoming (abstract in *Bulletin of the American Mathematical Society*, vol. 41). In connection with many of the theorems listed, see also Kurt Gödel, *Monatshefte für Mathematik und Physik*, vol. 38 (1931), p. 181^{et seq.}, observing that every function which is recursive in the sense in which the word is there used by Gödel is also recursive in the present more general sense.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Further examples.

(In the explanations the symbol “ \rightarrow ” is used to signify “the machine goes into the m -configuration. . . ”)

$e(\mathfrak{C}, \mathfrak{B}, a)$	$f(e_1(\mathfrak{C}, \mathfrak{B}, a), \mathfrak{B}, a)$	From $e(\mathfrak{C}, \mathfrak{B}, a)$ the first a is erased and $\rightarrow \mathfrak{C}$. If there is no $a \rightarrow \mathfrak{B}$.
$e_1(\mathfrak{C}, \mathfrak{B}, a)$	E	

$e(\mathfrak{B}, a)$	$e(e(\mathfrak{B}, a), \mathfrak{B}, a)$	From $e(\mathfrak{B}, a)$ all letters a are erased and $\rightarrow \mathfrak{B}$.
----------------------	--	---

The last example seems somewhat more difficult to interpret than most. Let us suppose that in the list of m -configurations of some machine there appears $e(b, x)$ ($= q$, say). The table is

$e(b, x)$	$e(e(b, x), b, x)$
or	q

Or, in greater detail:

q	$e(q, b, x)$
$e(q, b, x)$	$f(e_1(q, b, x), b, x)$
$e_1(q, b, x)$	E

In this we could replace $e_1(q, b, x)$ by q' and then give the table for f (with the right substitutions) and eventually reach a table in which no m -functions appeared.

$pe(\mathfrak{C}, \beta)$	$f(pe_1(\mathfrak{C}, \beta), \mathfrak{C}, \Theta)$	From $pe(\mathfrak{C}, \beta)$ the machine prints β at the end of the sequence of symbols and $\rightarrow \mathfrak{C}$.
$pe_1(\mathfrak{C}, \beta)$	$\begin{cases} \text{Any } R, R \\ \text{None } P\beta \end{cases}$	$pe_1(\mathfrak{C}, \beta)$
$I(\mathfrak{C})$	L	\mathfrak{C}
$r(\mathfrak{C})$	R	\mathfrak{C}
$f'(\mathfrak{C}, \mathfrak{B}, a)$	$f(I(\mathfrak{C}), \mathfrak{B}, a)$	From $f'(\mathfrak{C}, \mathfrak{B}, a)$ it does the same as for $f(\mathfrak{C}, \mathfrak{B}, a)$ but moves to the left before $\rightarrow \mathfrak{C}$.
$f''(\mathfrak{C}, \mathfrak{B}, a)$	$f(r(\mathfrak{C}), \mathfrak{B}, a)$	
$c(\mathfrak{C}, \mathfrak{B}, a)$	$f'(c_1(\mathfrak{C}), \mathfrak{B}, a)$	$c(\mathfrak{C}, \mathfrak{B}, a)$. The machine writes at the end the first symbol marked a and $\rightarrow \mathfrak{C}$.
$c_1(\mathfrak{C})$	β	$pe(\mathfrak{C}, \beta)$



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

ON COMPUTABLE NUMBERS.

$q(\Sigma)$	$\begin{cases} \text{Any} & R \\ \text{None} & R \end{cases}$	$q(\Sigma)$	$q(\Sigma, a)$. The machine finds the last symbol of form a . $\rightarrow \Sigma$.
$q_1(\Sigma)$	$\begin{cases} \text{Any} & R \\ \text{None} & \Sigma \end{cases}$	$q(\Sigma)$	
$q(\Sigma, a)$		$q(q_1(\Sigma, a))$	
$q_1(\Sigma, a)$	$\begin{cases} a & \Sigma \\ \text{not } a & L \end{cases}$	$q_1(\Sigma, a)$	
$pe_2(\Sigma, a, \beta)$		$pe(pe(\Sigma, \beta), a)$	$pe_2(\Sigma, a, \beta)$. The machine prints $a \beta$ at the end.
$ce_2(\mathfrak{B}, a, \beta)$		$ce(ce(\mathfrak{B}, \beta), a)$	
$ce_3(\mathfrak{B}, a, \beta, \gamma)$		$ce(ce_2(\mathfrak{B}, \beta, \gamma), a)$	$ce_3(\mathfrak{B}, a, \beta, \gamma)$. The machine copies down at the end first the symbols marked a , then those marked β , and finally those marked γ ; it erases the symbols a, β, γ .
$e(\Sigma)$	$\begin{cases} e & R \\ \text{Not } e & L \end{cases}$	$e_1(\Sigma)$	From $e(\Sigma)$ the marks are erased from all marked symbols. $\rightarrow \Sigma$.
$e_1(\Sigma)$	$\begin{cases} \text{Any} & R, E, R \\ \text{None} & \Sigma \end{cases}$	$e_1(\Sigma)$	

5. Enumeration of computable sequences.

A computable sequence γ is determined by a description of a machine which computes γ . Thus the sequence 001011011101111... is determined by the table on p.120, and, in fact, any computable sequence is capable of being described in terms of such a table.

It will be useful to put these tables into a kind of standard form. In the first place let us suppose that the table is given in the same form as the first table, for example, I on p.119. That is to say, that the entry in the operations column is always of one of the forms $E : E$, $R : E$, $L : Pa : Pa$, $R : Pa$, $L : R : L$: or no entry at all. The table can always be put into this form by introducing more m -configurations. Now let us give numbers to the m -configurations, calling them q_1, \dots, q_R , as in §1. The initial m -configuration is always to be called q_1 . We also give numbers to the symbols S_1, \dots, S_m



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

From (vi) we deduce that all real algebraic numbers are computable.

From (vi) and (x) we deduce that the real zeros of the Bessel functions are computable.

Proof of (ii).

Let $H(x, y)$ mean " $\eta(x) = y$ ", and let $K(x, y, z)$ mean " $\phi(x, y) = z$ ".

\mathfrak{U}_ϕ is the axiom for $\phi(x, y)$. We take \mathfrak{U}_η to be

$$\begin{aligned} \mathfrak{U}_\phi &\ \& P \ \& \left(F(x, y) \rightarrow G(x, y) \right) \ \& \left(G(x, y) \ \& G(y, z) \rightarrow G(x, z) \right) \\ &\ \& \left(F^{(r)} \rightarrow H(u, u^{(r)}) \right) \ \& \left(F(v, w) \ \& H(v, x) \ \& K(w, x, z) \rightarrow H(w, z) \right) \\ &\ \& \left[H(w, z) \ \& G(z, t) \vee G(t, z) \rightarrow (-H(w, t)) \right]. \end{aligned}$$

I shall not give the proof of consistency of \mathfrak{U}_η . Such a proof may be constructed by the methods used in Hilbert and Bernays, *Grundlagen der Mathematik* (Berlin, 1934), p. 209 *et seq.* The consistency is also clear from the meaning.

Suppose that, for some n, N , we have shown

$$\mathfrak{U}_\eta \ \& F^{(N)} \rightarrow H(u^{(n-1)}, u^{(\eta(n-1))}),$$

then, for some M ,

$$\mathfrak{U}_\phi \ \& F^{(M)} \rightarrow K(u^{(n)}, u^{(\eta(n-1))}, u^{(\eta(n))}),$$

$$\mathfrak{U}_\eta \ \& F^{(M)} \rightarrow F(u^{(n-1)}, u^{(n)}) \ \& H(u^{(n-1)}, u^{(\eta(n-1))})$$

$$\quad \& K(u^{(n)}, u^{(\eta(n-1))}, u^{(\eta(n))}),$$

and

$$\mathfrak{U}_\eta \ \& F^{(M)} \rightarrow [F(u^{(n-1)}, u^{(n)}) \ \& H(u^{(n-1)}, u^{(\eta(n-1))})$$

$$\quad \& K(u^{(n)}, u^{(\eta(n-1))}, u^{(\eta(n))}) \rightarrow H(u^{(n)}, u^{(\eta(n))})].$$

Hence

$$\mathfrak{U}_\eta \ \& F^{(M)} \rightarrow H(u^{(n)}, u^{(\eta(n))}).$$

Also

$$\mathfrak{U}_\eta \ \& F^{(r)} \rightarrow H(u, u^{(\eta(0))}).$$

Hence for each n some formula of the form

$$\mathfrak{U}_\eta \ \& F^{(M)} \rightarrow H(u^{(n)}, u^{(\eta(n))})$$

is provable. Also, if $M' \geq M$ and $M' \geq m$ and $m \neq \eta(u)$, then

$$\mathfrak{U}_\eta \ \& F^{(M')} \rightarrow G(u^{\eta(n)}, u^{(m)}) \vee G(u^{(m)}, u^{(\eta(n))})$$

and

$$\begin{aligned} \mathfrak{U}_\eta \& F^{(M)} \rightarrow & \left[\{G(u^{(\eta(n))}, u^{(m)}) \nu G(u^{(m)}, u^{(\eta(n))}) \right. \\ & \& H(u^{(n)}, u^{(\eta(n))}) \rightarrow \left. (-H(u^{(n)}, u^{(m)})) \right]. \end{aligned}$$

Hence

$$\mathfrak{U}_\eta \& F^{(M)} \rightarrow (-H(u^{(n)}, u^{(m)})).$$

The conditions of our second definition of a computable function are therefore satisfied. Consequently η is a computable function.

Proof of a modified form of (iii).

Suppose that we are given a machine \mathfrak{N} , which, starting with a tape bearing on it $\epsilon\epsilon$ followed by a sequence of any number of letters “ F ” on F -squares and in the m -configuration b , will compute a sequence γ_n depending on the number n of letters “ F ”. If $\phi_n(m)$ is the m -th figure of γ_n , then the sequence β whose n -th figure is $\phi_n(n)$ is computable.

We suppose that the table for \mathfrak{N} has been written out in such a way that in each line only one operation appears in the operations column. We also suppose that Ξ , Θ , $\bar{0}$, and $\bar{1}$ do not occur in the table, and we replace ϵ throughout by Θ , 0 by $\bar{0}$, and 1 by $\bar{1}$. Further substitutions are then made. Any line of form

$$\mathfrak{U} \quad a \quad P\bar{0} \quad \mathfrak{B}$$

we replace by

$$\mathfrak{U} \quad a \quad P\bar{0} \quad \text{re}(\mathfrak{B}, u, h, k)$$

and any line of the form

$$\mathfrak{U} \quad a \quad P\bar{1} \quad \mathfrak{B}$$

by $\mathfrak{U} \quad a \quad P\bar{1} \quad \text{re}(\mathfrak{B}, v, h, k)$

and we add to the table the following lines:

$$\begin{array}{lll} u & & \text{pe}(u_1, 0) \\ u_1 & R, Pk, R, P\Theta, R, P\Theta & u_2 \\ u_2 & & \text{re}(u_3, u_3, k, h) \\ u_3 & & \text{pe}(u_2, F) \end{array}$$

and similar lines with v for u and 1 for 0 together with the following line

$$c \quad R, P\Xi, R, Ph \quad b.$$

We then have the table for the machine \mathfrak{N}' which computes β . The initial m -configuration is c , and the initial scanned symbol is the second ϵ .

11. Application to the Entscheidungsproblem.

The results of § 8 have some important applications. In particular, they can be used to show that the Hilbert Entscheidungsproblem can have no solution. For the present I shall confine myself to proving this particular theorem. For the formulation of this problem I must refer the reader to Hilbert and Ackermann's *Grundzüge der Theoretischen Logik* (Berlin, 1931), chapter 3.

I propose, therefore, to show that there can be no general process for determining whether a given formula \mathfrak{U} of the functional calculus K is provable, i.e. that there can be no machine which, supplied with any one \mathfrak{U} of these formulae, will eventually say whether \mathfrak{U} is provable.

It should perhaps be remarked that what I shall prove is quite different from the well-known results of Gödel†. Gödel has shown that (in the formalism of Principia Mathematica) there are propositions \mathfrak{U} such that neither \mathfrak{U} nor $-\mathfrak{U}$ is provable. As a consequence of this, it is shown that no proof of consistency of Principia Mathematica (or of K) can be given within that formalism. On the other hand, I shall show that there is no general method which tells whether a given formula \mathfrak{U} is provable in K , or, what comes to the same, whether the system consisting of K with $-\mathfrak{U}$ adjoined as an extra axiom is consistent.

If the negation of what Gödel has shown had been proved, i.e. if, for each \mathfrak{U} , either \mathfrak{U} or $-\mathfrak{U}$ is provable, then we should have an immediate solution of the Entscheidungsproblem. For we can invent a machine \mathcal{K} which will prove consecutively all provable formulae. Sooner or later \mathcal{K} will reach either \mathfrak{U} or $-\mathfrak{U}$. If it reaches \mathfrak{U} , then we know that \mathfrak{U} is provable. If it reaches $-\mathfrak{U}$, then, since K is consistent (Hilbert and Ackermann, p. 65), we know that \mathfrak{U} is not provable.

Owing to the absence of integers in K the proofs appear somewhat lengthy. The underlying ideas are quite straightforward.

Corresponding to each computing machine M we construct a formula $Un(M)$ and we show that, if there is a general method for determining whether $Un(M)$ is provable, then there is a general method for determining whether M ever prints 0.

The interpretations of the propositional functions involved are as follows :

$R_{S_i}(x, y)$ is to be interpreted as "in the complete configuration x (of M) the symbol on the square y is S ".

† Loc. cit.^a

$I(x, y)$ is to be interpreted as “in the complete configuration x the square y is scanned”.

$K_{q_m}(x)$ is to be interpreted as “in the complete configuration x the m -configuration is q_m .

$F(x, y)$ is to be interpreted as “ y is the immediate successor of x ”.

$\text{Inst}\{q_i S_j S_k L q_l\}$ is to be an abbreviation for

$$(x, y, x', y') \left\{ \begin{array}{l} \left(R_{S_j}(x, y) \& I(x, y) \& K_{q_i}(x) \& F(x, x') \& F(y', y) \right) \\ \rightarrow \left(I(x', y') \& R_{S_k}(x', y) \& K_{q_l}(x') \right. \\ \left. \& (z) \left[F(y', z) \vee \left(R_{S_j}(x, z) \rightarrow R_{S_k}(x', z) \right) \right] \right) \end{array} \right\}.$$

$\text{Inst}\{q_i S_j S_k R q_l\}$ and $\text{Inst}\{q_i S_j S_k N q_l\}$

are to be abbreviations for other similarly constructed expressions.

Let us put the description of \mathcal{M} into the first standard form of § 6. This description consists of a number of expressions such as “ $q_i S_j S_k L q_l$ ” (or with R or N substituted for L). Let us form all the corresponding expressions such as $\text{Inst}\{q_i S_j S_k L q_l\}$ and take their logical sum. This we call $\text{Des}(\mathcal{M})$.

The formula $\text{Un}(\mathcal{M})$ is to be

$$\begin{aligned} (\exists u) \left[N(u) \& (x) \left(N(x) \rightarrow (\exists x') F(x, x') \right) \right. \\ & \& (y, z) \left(F(y, z) \rightarrow N(y) \& N(z) \right) \& (y) R_{S_0}(u, y) \\ & \& I(u, u) \& K_{q_1}(u) \& \text{Des}(\mathcal{M}) \left. \right] \\ & \rightarrow (\exists s) (\exists t) [N(s) \& N(t) \& R_{S_1}(s, t)]. \end{aligned}$$

$[N(u) \& \dots \& \text{Des}(\mathcal{M})]$ may be abbreviated to $A(\mathcal{M})$.

When we substitute the meanings suggested on p.146-46 we find that $\text{Un}(\mathcal{M})$ has the interpretation “in some complete configuration of \mathcal{M} , S_1 (i.e. 0) appears on the tape”. Corresponding to this I prove that

- (a) If S_1 appears on the tape in some complete configuration of \mathcal{M} , then $\text{Un}(\mathcal{M})$ is provable.
- (b) If $\text{Un}(\mathcal{M})$ is provable, then S_1 appears on the tape in some complete configuration of \mathcal{M} .

When this has been done, the remainder of the theorem is trivial.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

In the present paper we shall make considerable use of Church's identification of effective calculability with λ -definability, or, what comes to the same thing, of the identification with computability and one of the equivalence theorems. In most cases where we have to deal with an effectively calculable function, we shall introduce the corresponding W.F.F. with some such phrase as "the function f is effectively calculable, let F be a formula λ defining it", or "let F be a formula such that $F(n)$ is convertible to . . . whenever n represents a positive integer". In such cases there is no difficulty in seeing how a machine could in principle be designed to calculate the values of the function concerned; and, assuming this done, the equivalence theorem can be applied. A statement of what the formula F actually is may be omitted. We may immediately introduce on this basis a W.F.F. w with the property that

$$w(m, n) \text{ conv } r,$$

if r is the greatest positive integer, if any, for which m^r divides n and r is 1 if there is none. We also introduce Dt with the properties

$$Dt(n, n) \text{ conv } 3,$$

$$Dt(n+m, n) \text{ conv } 2,$$

$$Dt(n, n+m) \text{ conv } 1.$$

There is another point to be made clear in connection with the point of view that we are adopting. It is intended that all proofs that are given should be regarded no more critically than proofs in classical analysis. The subject matter, roughly speaking, is constructive systems of logic, but since the purpose is directed towards choosing a particular constructive system of logic for practical use, an attempt at this stage to put our theorems into constructive form would be putting the cart before the horse.

Those computable functions which take only the values 0 and 1 are of particular importance, since they determine and are determined by computable properties, as may be seen by replacing "0" and "1" by "true" and "false". But, besides this type of property, we may have to consider a different type, which is, roughly speaking, less constructive than the computable properties, but more so than the general predicates of classical mathematics. Suppose that we have a computable function of the natural numbers taking natural numbers as values, then corresponding to this function there is the property of being a value of the function. Such a property we shall describe as "axiomatic"; the reason for using this term is that it is possible to define such a property by giving a set of axioms, the property to hold for a given argument if and only if it is possible to deduce that it holds from the axioms.

Axiomatic properties may also be characterized in this way. A property ψ of positive integers is axiomatic if and only if there is a computable property ϕ of two positive integers, such that $\psi(x)$ is true if and only if there is a positive integer y such that $\phi(x, y)$ is true. Or again ψ is axiomatic if and only if there is a W.F.F. \mathbf{F} such that $\psi(n)$ is true if and only if $\mathbf{F}(n) \text{ conv } 2$.

3. Number-theoretic theorems.

By a *number-theoretic theorem*[†] we shall mean a theorem of the form “ $\theta(x)$ vanishes for infinitely many natural numbers x ”, where $\theta(x)$ is a primitive recursive[‡] function.

We shall say that a problem is number-theoretic if it has been shown that any solution of the problem may be put in the form of a proof of one or more number-theoretic theorems. More accurately we may say that a class of problems is number-theoretic if the solution of any one of them can be transformed (by a uniform process) into the form of proofs of number-theoretic theorems.

I shall now draw a few consequences from the definition of “number theoretic theorems”, and in section 5 I shall try to justify confining our consideration to this type of problem.

[†] I believe that there is no generally accepted meaning for this term, but it should be noticed that we are using it in a rather restricted sense. The most generally accepted meaning is probably this: suppose that we take an arbitrary formula of the functional calculus of the first order and replace the function variables by primitive recursive relations. The resulting formula represents a typical number-theoretic theorem in this (more general) sense.

[‡] Primitive recursive functions of natural numbers are defined inductively as follows. Suppose that $f(x_1, \dots, x_{n-1})$, $g(x_1, \dots, x_n)$, $h(x_1, \dots, x_{n+1})$ are primitive recursive, then $\phi(x_1, \dots, x_n)$ is primitive recursive if it is defined by one of the sets of equations (a) to (e).

$$(a) \quad \phi(x_1, \dots, x_n) = h(x_1, \dots, x_{m-1}, g(x_1, \dots, x_m), x_{m+1}, \dots, x_{n-1}, x_n) \quad (1 \leq m \leq n);$$

$$(b) \quad \phi(x_1, \dots, x_n) = f(x_2, \dots, x_n);$$

$$(c) \quad \phi(x_1) = a, \text{ where } n = 1 \text{ and } a \text{ is some particular natural number};$$

$$(d) \quad \phi(x_1) = x_1 + 1 \quad (n = 1);$$

$$(e) \quad \phi(x_1, \dots, x_{n-1}, 0) = f(x_1, \dots, x_{n-1});$$

$$\phi(x_1, \dots, x_{n-1}, x_n + 1) = h(x_1, \dots, x_n, \phi(x_1, \dots, x_n)).$$

The class of primitive recursive functions is more restricted than the class of computable functions, but it has the advantage that there is a process whereby it can be said of a set of equations whether it defines a primitive recursive function in the manner described above.

If $\phi(x_1, \dots, x_n)$ is primitive recursive, then $\phi(x_1, \dots, x_n) = 0$ is described as a primitive recursive relation between x_1, \dots, x_n .

An alternative form for number-theoretic theorems is “for each natural number x there exists a natural number y such that $\phi(x, y)$ vanishes”, where $\phi(x, y)$ is primitive recursive. In other words, there is a rule whereby, given the function $\theta(x)$, we can find a function $\phi(x, y)$, or given $\phi(x, y)$, we can find a function $\theta(x)$, such that “ $\theta(x)$ vanishes infinitely often” is a necessary and sufficient condition for “for each x there is a y such that $\phi(x, y) = 0$ ”. In fact, given $\theta(x)$, we define

$$\phi(x, y) = \theta(x) + a(x, y),$$

where $a(x, y)$ is the (primitive recursive) function with the properties

$$\begin{aligned} a(x, y) &= 1 \quad (y \leq x), \\ &= 0 \quad (y > x). \end{aligned}$$

If on the other hand we are given $\phi(x, y)$ we define $\theta(x)$ by the equations

$$\theta_1(0) = 3,$$

$$\begin{aligned} \theta_1(x+1) &= 2^{(1+\varpi_2(\theta_1(x)))\sigma(\phi(\varpi_3(\theta_1(x))-1, \varpi_2(\theta_1(x))))} 3^{\varpi_3(\theta_1(x))+1-\sigma(\phi(\varpi_3(\theta_1(x))-1, \varpi_2(\theta_1(x))))}, \\ \theta(x) &= \phi(\varpi_3(\theta_1(x))-1, \varpi_2(\theta_1(x))), \end{aligned}$$

where $\varpi_r(x)$ is defined so as to mean “the largest s for which r^s divides x ”. The function $\sigma(x)$ is defined by the equations $\sigma(0) = 0$, $\sigma(x+1) = 1$. It is easily verified that the functions so defined have the desired properties.

We shall now show that questions about the truth of the statements of the form “does $f(x)$ vanish identically”, where $f(x)$ is a computable function, can be reduced to questions about the truth of number-theoretic theorems. It is understood that in each case the rule for the calculation of $f(x)$ is given and that we are satisfied that this rule is valid, i.e. that the machine which should calculate $f(x)$ is circle free (Turing [1], 233).[†] The function $f(x)$, being computable, is general recursive in the Herbrand-Gödel sense, and therefore, by a general theorem due to Kleene[‡], is expressible in the form

$$\psi(\epsilon y[\phi(x, y) = 0]), \quad (3.2)$$

where $\epsilon y[\psi(y)]$ means “the least y for which $\psi(y)$ is true” and $\psi(y)$ and $\phi(x, y)$ are primitive recursive functions. Without loss of generality, we may suppose that the functions ϕ, ψ take only the values 0, 1. Then, if

[†] Kleene [2] 727.ⁱⁱ This result is really superfluous for our purpose, since the proof that every computable function is general recursive proceeds by showing that these functions are of the form (3.2). (Turing [2], 161).

we define $\rho(x)$ by the equations (3.1) and

$$\begin{aligned}\rho(0) &= \psi(0)(1-\theta(0)), \\ \rho(x+1) &= 1 - (1-\rho(x))\sigma[1+\theta(x)-\psi\{\varpi_2(\theta_1(x))\}]\end{aligned}$$

it will be seen that $f(x)$ vanishes identically if and only if $\rho(x)$ vanishes for infinitely many values of x .

The converse of this result is not quite true. We cannot say that the question about the truth of any number-theoretic theorem is reducible to a question about whether a corresponding computable function vanishes identically; we should have rather to say that it is reducible to the problem of whether a certain machine is circle free and calculates an identically vanishing function. But more is true: every number-theoretic theorem is equivalent to the statement that a corresponding machine is circle free. The behaviour of the machine may be described roughly as follows: the machine is one for the calculation of the primitive recursive function $\theta(x)$ of the number-theoretic problem, except that the results of the calculation are first arranged in a form in which the figures 0 and 1 do not occur, and the machine is then modified so that, whenever it has been found that the function vanishes for some value of the argument, then 0 is printed. The machine is circle free if and only if an infinity of these figures are printed, i.e. if and only if $\theta(x)$ vanishes for infinitely many values of the argument. That, on the other hand, questions of circle freedom may be reduced to questions of the truth of number-theoretic theorems follows from the fact that $\theta(x)$ is primitive recursive when it is defined to have the value 0 if a certain machine prints 0 or 1 in its $(x+1)$ -th complete configuration, and to have the value 1 otherwise.

The conversion calculus provides another normal form for the number-theoretic theorems, and the one which we shall find the most convenient to use. Every number-theoretic theorem is equivalent to a statement of the form “**A(n)** is convertible to 2 for every W.F.F. **n** representing a positive integer”, **A** being a W.F.F. determined by the theorem; the property of **A** here asserted will be described briefly as “**A** is dual”. Conversely such statements are reducible to number theoretic theorems. The first half of this assertion follows from our results for computable functions, or directly in this way. Since $\theta(x-1)+2$ is primitive recursive, it is formally definable, say, by means of a formula **G**. Now there is (Kleene [1], 232) a W.F.F. **P** with the property that, if **T(r)** is convertible to a formula representing a positive integer for each positive integer r , then **P(T, n)** is convertible to s , where s is the n -th positive integer t (if there is one) for which



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

is provable in C . Let \mathfrak{U}_l be $(\exists x_0) \text{Proof}_C[x_0, f^{(m_l)} 0] \supset \mathfrak{F}_l$. Then from (8.8) we find that

$$(\exists x_0) \text{Proof}_C[x_0, f^{(m_1)} 0] \vee \dots \vee (\exists x_0) \text{Proof}_C[x_0, f^{(m_k)} 0] \vee (\exists x_0) \mathfrak{B}[x_0]$$

is provable in C . It follows from a result which we have just proved that either $\mathfrak{B}[f^{(c)} 0]$ is provable for some natural number c , or else $\text{Proof}_C[f^{(n)} 0, f^{(m_l)} 0]$ is provable in C for some natural number n and some l , $1 \leq l \leq k$: but this would mean that \mathfrak{F}_l is provable in C (this is one of the points where we assume the validity of C) and therefore also in C' , contrary to hypothesis. Thus $\mathfrak{B}[f^{(c)} 0]$ must be provable in C' ; but we are also assuming $\sim \mathfrak{B}[f^{(c)} 0]$ to be provable in C' . There is therefore a contradiction in C' . Let us suppose that the axioms $\mathfrak{U}_1', \dots, \mathfrak{U}_{k'}'$, of the form (8.7), when adjoined to C are sufficient to obtain the contradiction and that none of these axioms is that provable in C . Then

$$\sim \mathfrak{U}_1' \vee \sim \mathfrak{U}_2' \vee \dots \vee \sim \mathfrak{U}_{k'}'$$

is provable in C , and if \mathfrak{U}_l' is $(\exists x_0) \text{Proof}_C[x_0, f^{(m_l')} 0] \supset \mathfrak{F}_l'$ then

$$(\exists x_0) \text{Proof}_C[x_0, f^{(m_1')} 0] \vee \dots \vee (\exists x_0) \text{Proof}_C[x_0, f^{(m_{k'})} 0]$$

is provable in C . But, by repetition of a previous argument, this means that \mathfrak{U}_l' is provable for some l , $1 \leq l \leq k'$, contrary to hypothesis. This is the required contradiction.

We may now construct an ordinal logic in the manner described on pp. 184–187. We shall, however, carry out the construction in rather more detail, and with some modifications appropriate to the particular case. Each system C of our set W may be described by means of a W.F.F. M_C which enumerates the G.R.'s of the axioms of C . There is a W.F.F. E such that, if a is the G.R. of some proposition \mathfrak{F} , then $E(M_C, a)$ is convertible to the G.R. of

$$(\exists x_0) \text{Proof}_C[x_0, f^{(a)} 0] \supset \mathfrak{F}.$$

If a is not the G.R. of any proposition in P , then $E(M_C, a)$ is to be convertible to the G.R. of $0 = 0$. From E we obtain a W.F.F. K such that $K(M_C, 2n+1) \text{conv } M_C(n)$, $K(M_C, 2n) \text{conv } E(M_C, n)$. The successor system C' is defined by $K(M_C) \text{conv } M_C'$. Let us choose a formula G such that $G(M_C, A) \text{conv } 2$ if and only if the number-theoretic theorem equivalent to “ A is dual” is provable in C . Then we define Λ_P by

$$\Lambda_P \rightarrow \lambda w a . \Gamma \left(\lambda y . G \left(\text{Ck} \left(\text{Tn}(w, y), \lambda m n . m \left(\varpi(2, n), \varpi(3, n) \right), K, M_P \right) \right), a \right).$$

This is an ordinal logic provided that P is valid.

Another ordinal logic of this type has in effect been introduced by Church†. Superficially this ordinal logic seems to have no more in common with Λ_P than that they both arise by the method which we have described, which uses C-K ordinal formulae. The initial systems are entirely different. However, in the relation between C and C' there is an interesting analogy. In Church's method the step from C to C' is performed by means of subsidiary axioms of which the most important (Church [2], p. 88, 1_m) is almost a direct translation into his symbolism of the rule that we may take any formula of the form (8.4) as an axiom. There are other extra axioms, however, in Church's system, and it is therefore not unlikely that it is in some respects more complete than Λ_P .

There are other types of ordinal logic, apparently quite unrelated to the type that we have so far considered. I have in mind two types of ordinal logic, both of which can be best described directly in terms of ordinal formulae without any reference to C-K ordinal formulae. I shall describe here a specimen Λ_H of one of these types of ordinal logic. Ordinal logics of this kind were first considered by Hilbert (Hilbert [1], 183ff), and have also been used by Tarski (Tarski [1], 395ff); see also Gödel [1]^a, foot-note 48^a.

Suppose that we have selected a particular ordinal formula Ω . We shall construct a modification P_Ω of the system P of Gödel (see foot-note † on p. 187). We shall say that a natural number n is a *type* if it is either even or $2p-1$, where $\Omega(p, p)$ conv 3. The definition of a variable in P is to be modified by the condition that the only admissible subscripts are to be the types in our sense. Elementary expressions are then defined as in P : in particular the definition of an elementary expression of type 0 is unchanged. An elementary formula is defined to be a sequence of symbols of the form $\mathfrak{U}_m \mathfrak{U}_n$, where \mathfrak{U}_m , \mathfrak{U}_n are elementary expressions of types m , n satisfying one of the conditions (a), (b), (c).

- (a) m and n are both even and m exceeds n ,
- (b) m is odd and n is even,
- (c) $m = 2p-1$, $n = 2q-1$, and $\Omega(p, q)$ conv 2.

With these modifications the formal development of P_Ω is the same as that of P . We want, however, to have a method of associating number-theoretic theorems with certain of the formulae of P_Ω . We cannot take over directly the association which we used in P . Suppose that G is a

† In outline Church [1], 279–280. In greater detail Church [2], Chap. X.

formula in P interpretable as a number-theoretic theorem in the way described in the course of constructing Λ_P (p. 187). Then, if every type suffix in G is doubled, we shall obtain a formula in P_Ω which is to be interpreted as the same number-theoretic theorem. By the method of §6 we can now obtain from P_Ω a formula L_Ω which is a logic formula if P_Ω is valid; in fact, given Ω there is a method of obtaining L_Ω , so that there is a formula Λ_H such that $\Lambda_H(\Omega) \text{ conv } L_\Omega$ for each ordinal formula Ω .

Having now familiarized ourselves with ordinal logics by means of these examples we may begin to consider general questions concerning them.

9. Completeness questions.

The purpose of introducing ordinal logics was to avoid as far as possible the effects of Gödel's theorem. It is a consequence of this theorem, suitably modified, that it is impossible to obtain a complete logic formula, or (roughly speaking now) a complete system of logic. We were able, however, from a given system to obtain a more complete one by the adjunction as axioms of formulae, seen intuitively to be correct, but which the Gödel theorem shows are unprovable† in the original system; from this we obtained a yet more complete system by a repetition of the process, and so on. We found that the repetition of the process gave us a new system for each C-K ordinal formula. We should like to know whether this process suffices, or whether the system should be extended in other ways as well. If it were possible to determine about a W.F.F. in normal form whether it was an ordinal formula, we should know for certain that it was necessary to make extensions in other ways. In fact for any ordinal formula Λ it would then be possible to find a single logic formula L such that, if $\Lambda(\Omega, A) \text{ conv } 2$ for some ordinal formula Ω , then $L(A) \text{ conv } 2$. Since L must be incomplete, there must be formulae A for which $\Lambda(\Omega, A)$ is not convertible to 2 for any ordinal formula Ω . However, in view of the fact, proved in §7, that there is no method of determining about a formula in normal form whether it is an ordinal formula, the case does not arise, and there is still a possibility that some ordinal logics may be complete in some sense. There is a quite natural way of defining completeness.

Definition of completeness of an ordinal logic. We say that an ordinal logic Λ is complete if corresponding to each dual formula A there is an ordinal formula Ω_A such that $\Lambda(\Omega_A, A) \text{ conv } 2$.

† In the case of P we adjoined all of the axioms $(\exists x_0) \text{Proof}[x_0, f^{(m)}0] \supset \tilde{\gamma}$, where m is the G.R. of $\tilde{\gamma}$; the Gödel theorem shows that some of them are unprovable in P .



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

B such that $\Lambda(\Omega, \mathbf{B}) \text{ conv } 2$ whenever Ω represents γ , but is not convertible to 2 if Ω represents a smaller ordinal. Let us take first the case $\gamma_0 \geq 2\omega$. Suppose that $\gamma_0 = \omega + \gamma_1$, and that Ω_1 is an ordinal formula representing γ_1 . Let \mathbf{A} be any W.F.F. with a normal form and no free variables, and let Z be the class of those positive integers which are exceeded by all integers n for which $\mathbf{A}(n)$ is not convertible to 2. Let E be the class of integers $2p$ such that $\Omega(p, n) \text{ conv } 2$ for some n belonging to Z . The class E , together with the class Q of all odd integers, is constructively enumerable. It is evident that the class can be enumerated with repetitions, and since it is infinite the required enumeration can be obtained by striking out the repetitions. There is, therefore, a formula En such that $\text{En}(\Omega, \mathbf{A}, r)$ runs through the formulae of the class $E+Q$ without repetitions as r runs through the positive integers. We define

$$\text{Rt} \rightarrow \lambda w a m n . \text{Sum} \left(\text{Dt}, w, \text{En}(w, a, m), \text{En}(w, a, n) \right).$$

Then $\text{Rt}(\Omega_1, \mathbf{A})$ is an ordinal formula which represents γ_0 if \mathbf{A} is dual, but a smaller ordinal otherwise. In fact

$$\text{Rt}(\Omega_1, \mathbf{A}, m, n) \text{ conv } \{\text{Sum}(\text{Dt}, \Omega_1)\} (\text{En}(\Omega_1, \mathbf{A}, m), \text{En}(\Omega_1, \mathbf{A}, n)).$$

Now, if \mathbf{A} is dual, $E+Q$ includes all integers m for which

$$\{\text{Sum}(\text{Dt}, \Omega_1)\} (m, m) \text{ conv } 3.$$

(This depends on the particular form that we have chosen for the formula Sum .) Putting “ $\text{En}(\Omega_1, \mathbf{A}, p) \text{ conv } q$ ” for $M(p, q)$, we see that condition (7.4) is satisfied, so that $\text{Rt}(\Omega_1, \mathbf{A})$ is an ordinal formula representing γ_0 . But, if \mathbf{A} is not dual, the set $E+Q$ consists of all integers m for which

$$\{\text{Sum}(\text{Dt}, \Omega_1)\} (m, r) \text{ conv } 2,$$

where r depends only on \mathbf{A} . In this case $\text{Rt}(\Omega_1, \mathbf{A})$ is an ordinal formula representing the same ordinal as $\text{Inf}(\text{Sum}(\text{Dt}, \Omega_1), r)$, and this is smaller than γ_0 . Now consider \mathbf{K} :

$$\mathbf{K} \rightarrow \lambda a . \Lambda \left(\text{Sum} \left(\text{Rt}(\Omega_1, \mathbf{A}), \mathbf{P} \right), \mathbf{B} \right).$$

If \mathbf{A} is dual, $\mathbf{K}(\mathbf{A})$ is convertible to 2 since $\text{Sum}(\text{Rt}(\Omega_1, \mathbf{A}), \mathbf{P})$ represents γ . But, if \mathbf{A} is not dual, it is not convertible to 2, since $\text{Sum}(\text{Rt}(\Omega_1, \mathbf{A}), \mathbf{P})$ then represents an ordinal smaller than γ . In \mathbf{K} we therefore have a complete logic formula, which is impossible.

Now we take the case $\gamma_0 = \omega$. We introduce a W.F.F. Mg such that if n is the D.N. of a computing machine \mathcal{M} , and if by the m -th complete

configuration of \mathbf{M} the figure 0 has been printed, then $Mg(n, m)$ is convertible to $\lambda pq . Al(4(P, 2p+2q), 3, 4)$ (which is an ordinal formula representing the ordinal 1), but if 0 has not been printed it is convertible to $\lambda pq . p(q, I, 4)$ (which represents 0). Now consider

$$\mathbf{M} \rightarrow \lambda n . \Lambda \left(\text{Sum} \left(\text{Lim} \left(Mg(n) \right), \mathbf{P} \right), \mathbf{B} \right).$$

If the machine never prints 0, then $\text{Lim}(\lambda r . Mg(n, r))$ represents ω and $\text{Sum}(\text{Lim}(Mg(n)), \mathbf{P})$ represents γ . This means that $\mathbf{M}(n)$ is convertible to 2. If, however, \mathbf{M} never prints 0, $\text{Sum}(\text{Lim}(Mg(n)), \mathbf{P})$ represents a finite ordinal and $\mathbf{M}(n)$ is not convertible to 2. In \mathbf{M} we therefore have means of determining about a machine whether it ever prints 0, which is impossible† (Turing [1], § 8). This completes the proof of (A).

Proof of (B). It is sufficient to prove that, if \mathbf{C} represents an ordinal γ , $\omega^2 \leq \gamma < \alpha$, then the extent of $\Lambda(H(\mathbf{C}))$ is included in the set-theoretic sum of the extents of $\Lambda(H(\mathbf{G}))$, where \mathbf{G} represents an ordinal less than γ . We obtain a contradiction from the assumption that there is a formula \mathbf{B} which is in the extent of $\Lambda(H(\mathbf{G}))$ if \mathbf{G} represents γ , but not if it represents any smaller ordinal. The ordinal γ is of the form $\delta + \omega^2 + \xi$, where $\xi < \omega^2$. Let \mathbf{D} be a C-K ordinal formula representing δ and $\lambda aufx . Q(u, f, A(u, f, x))$ one representing $\alpha + \xi$ whenever A represents α .

We now define a formula Hg . Suppose that \mathbf{A} is a W.F.F. in normal form and without free variables; consider the process of carrying out conversions on $\mathbf{A}(1)$ until it is brought into the form 2, then converting $\mathbf{A}(2)$ to 2, then $\mathbf{A}(3)$, and so on. Suppose that at the r -th step of this process we are doing the n_r -th step in the conversion of $\mathbf{A}(m_r)$. Thus, for instance, if \mathbf{A} is not convertible to 2, m_r can never exceed 3. Then $Hg(\mathbf{A}, r)$ is to be convertible to $\lambda f . f(m_r, n_r)$ for each positive integer r . Put

$$Sq \rightarrow \lambda dm n . n \left(\text{Suc}, m \left(\lambda aufx . u \left(\lambda y . y \left(\text{Suc}, a(u, f, x) \right) \right), d(u, f, x) \right) \right),$$

$$\mathbf{M} \rightarrow \lambda aufx . Q(u, f, u \left(\lambda y . Hg(a, y, Sq(\mathbf{D})) \right)),$$

$$\mathbf{K}_1 \rightarrow \lambda a . \Lambda \left(\mathbf{M}(a), \mathbf{B} \right),$$

† This part of the argument can equally well be based on the impossibility of determining about two W.F.F. whether they are interconvertible. (Church [3], 363.)ⁱ

then I say that \mathbf{K}_1 is a complete logic formula. $Sq(\mathbf{D}, \mathbf{m}, \mathbf{n})$ is a C-K ordinal formula representing $\delta + m\omega + n$, and therefore $Hg(A, r, Sq(\mathbf{D}))$ represents an ordinal ζ_r which increases steadily with increasing r , and tends to the limit $\delta + \omega^2$ if A is dual. Further

$$Hg(A, r, Sq(\mathbf{D})) < Hg(A, S(r), Sq(\mathbf{D}))$$

for each positive integer r . Therefore $\lambda ufx.u(\lambda y.Hg(A, y, Sq(\mathbf{D})))$ is a C-K ordinal formula and represents the limit of the sequence $\zeta_1, \zeta_2, \zeta_3, \dots$. This is $\delta + \omega^2$ if A is dual, but a smaller ordinal otherwise. Likewise $M(A)$ represents γ if A is dual, but is a smaller ordinal otherwise. The formula B therefore belongs to the extent of $\Lambda(H(M(A)))$ if and only if A is dual, and this implies that \mathbf{K}_1 is a complete logic formula, as was asserted. But this is impossible and we have the required contradiction.

As a corollary to (A) we see that Λ_H is incomplete and in fact that the extent of $\Lambda_H(Dt)$ contains the extent of $\Lambda_H(\Omega)$ for any ordinal formula Ω . This result, suggested to me first by the solution of question (b), may also be obtained more directly. In fact, if a number-theoretic theorem can be proved in any particular P_Ω , it can also be proved in $P_{\lambda mn.m(n, I, 4)}$. The formulae describing number-theoretic theorems in P do not involve more than a finite number of types, type 3 being the highest necessary. The formulae describing the number-theoretic theorems in any P_Ω will be obtained by doubling the type subscripts. Now suppose that we have a proof of a number-theoretic theorem G in P_Ω and that the types occurring in the proof are among 0, 2, 4, 6, t_1, t_2, t_3, \dots . We may suppose that they have been arranged with all the even types preceding all the odd types, the even types in order of magnitude and the type $2m-1$ preceding $2n-1$ if $\Omega(m, n) \text{ conv } 2$. Now let each t_r be replaced by $10+2r$ throughout the proof of G . We thus obtain a proof of G in $P_{\lambda mn.(n, I, 4)}$.

As with problem (a), the solution of problem (b) does not require the use of high ordinals [e.g. if we make the assumption that the extent of $\Lambda(\Omega)$ is a steadily increasing function of the ordinal represented by Ω we do not have to consider ordinals higher than $\omega+2$]. However, if we restrict what we are to call ordinal formulae in some way, we shall have corresponding modified problems (a) and (b); the solutions will presumably be essentially the same, but will involve higher ordinals. Suppose, for example, that Prod is a W.F.F. with the property that $Prod(\Omega_1, \Omega_2)$ is an ordinal formula representing $a_1 a_2$ when Ω_1, Ω_2 are ordinal formulae representing a_1, a_2 respectively, and suppose that we call a W.F.F. a 1-ordinal



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

12. Gentzen type ordinal logics.

In proving the consistency of a certain system of formal logic Gentzen (Gentzen [1]) has made use of the principle of transfinite induction for ordinals less than ϵ_0 , and has suggested that it is to be expected that transfinite induction carried sufficiently far would suffice to solve all problems of consistency. Another suggestion of basing systems of logic on transfinite induction has been made by Zermelo (Zermelo [1]). In this section I propose to show how this method of proof may be put into the form of a formal (non-constructive) logic, and afterwards to obtain from it an ordinal logic.

We can express the Gentzen method of proof formally in this way. Let us take the system P and adjoin to it an axiom \mathfrak{U}_Ω with the intuitive meaning that the W.F.F. Ω is an ordinal formula, whenever we feel certain that Ω is an ordinal formula. This is a non-constructive system of logic which may easily be put into the form of an ordinal logic. By the method of § 6 we make correspond to the system of logic consisting of P with the axiom \mathfrak{U}_Ω adjoined a logic formula L_Ω : L_Ω is an effectively calculable function of Ω , and there is therefore a formula Λ_G^1 such that $\Lambda_G^1(\Omega) \text{ conv } L_\Omega$ for each formula Ω . Λ_G^1 is certainly not an ordinal logic unless P is valid, and therefore consistent. This formalization of Gentzen's idea would therefore not be applicable for the problem with which Gentzen himself was concerned, for he was proving the consistency of a system weaker than P . However, there are other ways in which the Gentzen method of proof can be formalized. I shall explain one, beginning by describing a certain logical calculus.

The symbols of the calculus are $f, x, ^1, _1, 0, S, R, \Gamma, \Delta, E, |, \odot, !, (,), =$, and the comma “,”. For clarity we shall use various sizes of brackets ‘(,)’ in the following. We use capital German letters to stand for variable or undetermined sequences of these symbols.

It is to be understood that the relations that we are about to define hold only when compelled to do so by the conditions that we lay down. The conditions should be taken together as a simultaneous inductive definition of all the relations involved.

Suffixes.

$_1$ is a suffix. If \mathfrak{S} is a suffix then \mathfrak{S}_1 is a suffix.

Indices.

1 is an index. If \mathfrak{I} is an index then \mathfrak{I}^1 is an index.

Numerical variables.

If \mathfrak{S} is a suffix then $x\mathfrak{S}$ is a numerical variable.

(a) The provable equations include all the axioms. The axioms are of the form of equations in which the symbols Γ , Δ , E , $|$, \odot , ! do not appear.

(b) If G is an expression of index \mathfrak{I}^{11} and (\mathfrak{U}) is an argument of index \mathfrak{I} , then

$$(\Gamma G)(\mathfrak{U}x_1, x_{11},) = G(\mathfrak{U}x_{11}, x_1,)$$

is a provable equation.

(c) If G is an expression of index \mathfrak{I}^1 , and (\mathfrak{U}) is an argument of index \mathfrak{I} , then

$$(\Delta G)(\mathfrak{U}x_1,) = G(, x_1 \mathfrak{U})$$

is a provable equation.

(d) If G is an expression of index \mathfrak{I} , and (\mathfrak{U}) is an argument of index \mathfrak{I} , then

$$(E G)(\mathfrak{U}x_1,) = G(\mathfrak{U})$$

is a provable equation.

(e) If G is an expression of index \mathfrak{I} and H is one of index \mathfrak{I}^1 , and (\mathfrak{U}) is an argument of index \mathfrak{I} , then

$$(G | H)(\mathfrak{U}) = H(\mathfrak{U}G(\mathfrak{U}),)$$

is a provable equation.

(f) If N is an expression of index 1 , then $N(,) = N$ is a provable equation.

(g) If G is an expression of index \mathfrak{I} and R one of index \mathfrak{I}^{111} , and (\mathfrak{U}) an argument of index \mathfrak{I}^1 , then

$$(G \odot R)(\mathfrak{U}0,) = G(\mathfrak{U})$$

and $(G \odot R)(\mathfrak{U}S(, x_1,),) = R(\mathfrak{U}x_1, S(, x_1,), (G \odot R)(\mathfrak{U}x_1,),)$

are provable equations. If in addition H is an expression of index \mathfrak{I}^1 and

$$R(, G(\mathfrak{U}S(, x_1,),), x_1,) = 0$$

is provable, then

$$(G! R! H)(\mathfrak{U}0,) = G(\mathfrak{U})$$

and

$$(G! R! H)(\mathfrak{U}S(, x_1,),)$$

$$= R\left((\mathfrak{U}H(\mathfrak{U}S(, x_1,),), S(, x_1,), (G! R! H)(\mathfrak{U}H(\mathfrak{U}S(, x_1,),),),) \right)$$

are provable.

(h) If $\mathfrak{L} = \mathfrak{L}'$ and $\mathfrak{U} = \mathfrak{U}'$ are provable, where $\mathfrak{L}, \mathfrak{L}', \mathfrak{U}$ and \mathfrak{U}' are terms, then $\mathfrak{U}' = \mathfrak{U}$ and the result of substituting \mathfrak{U}' for \mathfrak{U} at any particular occurrence in $\mathfrak{L} = \mathfrak{L}'$ are provable equations.

(i) The result of substituting any term for a particular numerical variable throughout a provable equation is provable.

(j) Suppose that $\mathfrak{G}, \mathfrak{G}'$ are expressions of index \mathfrak{I}^1 , that (\mathfrak{A}) is an argument of index \mathfrak{J} not containing the numerical variable \mathfrak{X} and that $\mathfrak{G}(\mathfrak{A}0,) = \mathfrak{G}'(\mathfrak{A}0,)$ is provable. Also suppose that, if we add

$$\mathfrak{G}(\mathfrak{A}\mathfrak{X},) = \mathfrak{G}'(\mathfrak{A}\mathfrak{X},)$$

to the axioms and restrict (i) so that it can never be applied to the numerical variable \mathfrak{X} , then

$$\mathfrak{G}(\mathfrak{A}S(\mathfrak{A}\mathfrak{X},),) = \mathfrak{G}'(\mathfrak{A}S(\mathfrak{A}\mathfrak{X},),)$$

becomes a provable equation; in the hypothetical proof of this equation this rule (j) itself may be used provided that a different variable is chosen to take the part of \mathfrak{X} .

Under these conditions $\mathfrak{G}(\mathfrak{A}\mathfrak{X},) = \mathfrak{G}'(\mathfrak{A}\mathfrak{X},)$ is a provable equation.

(k) Suppose that $\mathfrak{G}, \mathfrak{G}', \mathfrak{H}$ are expressions of index \mathfrak{I}^1 , that (\mathfrak{A}) is an argument of index \mathfrak{J} not containing the numerical variable \mathfrak{X} and that

$$\mathfrak{G}(\mathfrak{A}0,) = \mathfrak{G}'(\mathfrak{A}0,) \quad \text{and} \quad R\left(\mathfrak{H}(\mathfrak{A}S(\mathfrak{A}\mathfrak{X},),), S(\mathfrak{A}\mathfrak{X},),\right) = 0$$

are provable equations. Suppose also that, if we add

$$\mathfrak{G}(\mathfrak{A}\mathfrak{H}(\mathfrak{A}S(\mathfrak{A}\mathfrak{X},),)) = \mathfrak{G}'(\mathfrak{A}\mathfrak{H}(\mathfrak{A}S(\mathfrak{A}\mathfrak{X},),))$$

to the axioms, and again restrict (i) so that it does not apply to \mathfrak{X} , then

$$\mathfrak{G}(\mathfrak{A}\mathfrak{X},) = \mathfrak{G}'(\mathfrak{A}\mathfrak{X},) \tag{12.1}$$

becomes a provable equation; in the hypothetical proof of (12.1) the rule (k) may be used if a different variable takes the part of \mathfrak{X} .

Under these conditions (12.1) is a provable equation.

We have now completed the definition of a provable equation relative to a given set of axioms. Next we shall show how to obtain an ordinal logic from this calculus. The first step is to set up a correspondence between some of the equations and number-theoretic theorems, in other words to show how they can be interpreted as number-theoretic theorems.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

II. Amongst the symbols of L must be one, \sim , which is interpreted as "not." That is, if A expresses in L a certain sentence, then $\sim A$ expresses in L the contradictory of that sentence.

III. For each positive integer, there must be a particular formula in L which denotes that integer. Also, amongst the symbols of L must be some, called variables, whose mode of interpretation is as follows. If a formula A of L expresses a sentence S and if A contains symbols called variables, v_1, v_2, \dots, v_s , then S contains variables.³ Moreover, if B is the formula got from A by replacing various of the v_i 's of A by other symbols, then the sentence which B expresses is got from S by making corresponding replacements for the variables of S . In particular, if the formula G of L with the symbol v , called a variable, expresses in L the sentence " x has the property Q ," with the variable x corresponding to v , and if F is got from G by replacing all the v 's of G by the formula denoting the number n , then F expresses in L the sentence " n has the property Q ."

IV. Also there must be a process whereby certain of the propositions of L are specified as "provable." The definition of "provable" is always supposed to be made without referring to the meanings of the formulas. However it was always hoped that the set of provable propositions of L would coincide with the set of propositions of L which express true sentences. Gödel's Theorems tell us that such cannot be the case. For Gödel's First Theorem states:

For suitable L , there are undecidable propositions in L ; that is, propositions F such that neither F nor $\sim F$ is provable.

As F and $\sim F$ express contradictory sentences, one of them must express a true sentence. So there will be a proposition of L which expresses a true sentence, but nevertheless is not provable. This still leaves open the possibility that all provable propositions of L may express true sentences. As the notion of "truth of a sentence" is vague, it is usual to deal with weaker but more precise notions. For instance, L is said to be "simply consistent" if there is no proposition F such that both F and $\sim F$ are provable. Clearly, if L is not simply consistent, then some provable proposition of L must express a false sentence. However, some provable propositions of L may express false sentences even if L is simply consistent. Tarski⁴ showed this by constructing a logic L which was simply consistent but in which one could prove the propositions expressing each sentence of the following infinite set (with Q properly chosen):

Not all positive integers have property Q .

1 has property Q .

2 has property Q .

3 has property Q .

.....

³ I am purposely overlooking the complications due to the use of "apparent variables" as being irrelevant to the present discussion.

⁴ Alfred Tarski, *Einige Betrachtungen über die Begriffe der ω -Widerspruchsfreiheit und der ω -Vollständigkeit*, *Monatshefte für Mathematik und Physik*, vol. 40 (1933), pp. 97-112.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

telling whether or not a formula with no free variables is provable. Hence it is a corollary of Theorem III (stated below) that there is no *Entscheidungsverfahren* for P_ϵ .

THEOREM III. *If P_ϵ is got by adding various axioms and rules of procedure to P , and if P_ϵ is simply consistent, then there is no generally applicable effective process for determining whether or not a formula with no free variables is provable.*

Proof. Assume that P_ϵ is simply consistent and that there is a generally applicable effective process for determining whether or not a formula with no free variables is provable. Let us define $\phi(n)$ by the rule: $\phi(n)$ shall be 0 if n is the number of a provable formula with no free variables, and 1 otherwise. Then $\phi(n)$ is effectively calculable and we shall follow Church in assuming that this necessitates that $\phi(n)$ be general recursive. Then the class of numbers of provable formulas with no free variables and the class of numbers which are not numbers of provable formulas with no free variables are both recursively enumerable. Also both are non-null. Let $\beta(m)$ and $\gamma(m)$ be primitive recursive functions which enumerate them respectively. Then there is a primitive recursive formula $\theta(m)$ such that $\theta(2n) = \beta(n)$ and $\theta(2n+1) = \gamma(n)$. Then $\theta(m)$ enumerates all numbers in such a way that the numbers occurring in the even places are numbers of provable formulas with no free variables and the numbers occurring at the odd places are not numbers of provable formulas with no free variables. Now put $x B_\epsilon y$ for $\theta(x) = y$ & $x/2$, $Bew_\epsilon(y)$ for $(Ex)[x B_\epsilon y]$, $x Pr_\epsilon y$ for $x B_\epsilon y$ & $\overline{(Ez)}[z \leq x \& \theta(z) = y \& \overline{z/2}]$, and $Prov_\epsilon(y)$ for $(Ex)[x Pr_\epsilon y]$. Then $Bew_\epsilon(y) \sim Prov_\epsilon(y)$. Now let b be the number of the formalization of $Prov_\epsilon(a)$. By a proof like that in the proof of Thm. II, it follows that $Prov_\epsilon(a) \rightarrow Prov_\epsilon(b)$ and $(Ez)[\theta(z) = a \& \overline{z/2}] \rightarrow Prov_\epsilon(Neg(b))$. But if $\overline{Prov_\epsilon(a)}$, then $(Em)[\gamma(m) = a]$, and therefore $\theta(2(em[\gamma(m) = a]) + 1) = a$. Hence $Prov_\epsilon(a) \rightarrow Prov_\epsilon(Neg(b))$. By use of this and $Prov_\epsilon(a) \rightarrow Prov_\epsilon(b)$, one can derive a contradiction by proceeding as on p. 188ⁱ of Gödel, but with $x Pr_\epsilon y$ and $Prov_\epsilon(y)$ in place of $x B_\epsilon y$ and $Bew_\epsilon(y)$ respectively.

With slight modifications the proof above becomes a proof of:

THEOREM IV. *If P_ϵ is got by adding various axioms and rules of procedure to P , and if P_ϵ is simply consistent, then the class of numbers of provable formulas and the class of numbers of unprovable formulas are not both recursively enumerable.*

From this theorem and Theorem III follow:

THEOREM V. *If P is simply consistent, then:*

- The class of unprovable formulas is not recursively enumerable.*
- The class of undecidable formulas is not recursively enumerable.*
- The class of provable formulas is recursively enumerable but not general recursive.*
- The class of decidable formulas is recursively enumerable but not general recursive.*

I wish to thank S. C. Kleene for reading an earlier draft of this paper and suggesting improvements.

GENERAL RECURSIVE FUNCTIONS OF NATURAL NUMBERS

In this paper, Gödel's technique of arithmetization is applied to the general definition of recursive function given in Gödel's lectures, this anthology, pp. 69–71. This leads to yet another proof that there are unsolvable problems.

Errata and addenda supplied by the author for this anthology appear on p. 253 following this paper.

Stephen C. Kleene

GENERAL RECURSIVE FUNCTIONS OF NATURAL NUMBERS¹

Reprinted from MATHEMATISCHE ANNALEN Band 112, Heft 5 (1936) pp. 727-742, with the kind permission of Springer-Verlag.

The substitution

$$1) \quad \varphi(x_1, \dots, x_n) = \theta(\chi_1(x_1, \dots, x_n), \dots, \chi_m(x_1, \dots, x_n)),$$

and the ordinary recursion with respect to one variable

$$(2) \quad \varphi(0, x_1, \dots, x_n) = \psi(x_1, \dots, x_n)$$

$$\varphi(y + 1, x_1, \dots, x_n) = \chi(y, \varphi(y, x_1, \dots, x_n), x_1, \dots, x_n),$$

where $\theta, \chi_1, \dots, \chi_m, \psi, \chi$ are given functions of natural numbers, are examples of the definition of a function φ by equations which provide a step by step process for computing the value $\varphi(k_1, \dots, k_n)$ for any given set k_1, \dots, k_n of natural numbers. It is known that there are other definitions of this sort, e. g. certain recursions with respect to two or more variables simultaneously, which cannot be reduced to a succession of substitutions and ordinary recursions²). Hence, a characterization of the notion of recursive definition in general, which would include all these cases, is desirable. A definition of general recursive function of natural numbers was suggested by Herbrand to Gödel, and was used by Gödel with an important modification in a series of lectures at Princeton in 1934. In this paper we offer several observations on general recursive functions, using essentially Gödel's form of the definition.

The definition will be stated in § 1. It consists in specifying the form of the equations and the nature of the steps admissible in the computation of the values, and in requiring that for each given set of arguments the computation yield a unique number as value. The operations on symbols which occur in the computation have a similarity to ordinary recursive operations on numbers. This similarity will be utilized, by the Gödel method of representing formulas by numbers, to prove that every (general) recursive function is expressible in the form $\psi(e y [\varrho(x_1, \dots, x_n, y) = 0])$ where ψ and ϱ are ordinary or „primitive“

¹⁾ Presented to the American Mathematical Society, September 1935.

²⁾ W. Ackermann, Zum Hilbertschen Aufbau der reellen Zahlen, Math. Annalen 99 (1928), S. 118—133; Rózsa Péter, Konstruktion nichtrekursiver Funktionen, Math. Annalen 111 (1935), S. 42—60.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

$R_0''(i, x, y)$, $R_1''(i, x, y)$, $R_2''(i, x, y)$ correspond to the operations R'_{3i} , R'_{3i+1} , R'_{3i+2} , resp.

$$21. \quad R'(n, x, y) = \varepsilon z \left[z \leq R_0''\left(\left[\frac{n}{3}\right], x, y\right) + R_1''\left(\left[\frac{n+1}{3}\right], x, y\right) + R_2''\left(\left[\frac{n+2}{3}\right], x, y\right) \& \left\{ \begin{array}{l} n \mid 3 \& z = R_0''\left(\left[\frac{n}{3}\right], x, y\right) \\ n+2 \mid 3 \& z = R_1''\left(\left[\frac{n+1}{3}\right], x, y\right) \\ n+1 \mid 3 \& z = R_2''\left(\left[\frac{n+2}{3}\right], x, y\right) \end{array} \right\} \right].$$

$R'(n, x, y)$ corresponds to the operation R'_n .

$$22. \quad Z(0) = R(1), \\ Z(n+1) = R(3) * E(Z(n)).$$

$Z(n)$ corresponds to the numeral $S(\dots n \text{ times } \dots S(0))$.

$$23. \quad \text{Eval}_p(n, y, x_1, \dots, x_p) \equiv (Ex) \{ x \leq y \& y = R([Pr(n+7)]^2) * E(Z(x_1) * R(7) * \dots * R(7) * Z(x_p)) * R(5) * Z(x) \} \text{ (for a fixed number } p).$$

y corresponds to an expression of the form $\varrho_n(x_1, \dots, x_p) = x$, where x is a numeral.

$$24. \quad \text{Val}(y) = \varepsilon x \{ x \leq y \& (Em) [m \leq y \& y = m * Z(x)] \}.$$

If y corresponds to an expression of the form $a = x$ where x is a numeral, then $\text{Val}(y) = x$.

Supposing the function $\varphi(n, x, y)$ given, we define a series of functions as follows:

$$\psi(0, x, y) = x,$$

$$\psi(n+1, x, y) = \varphi(n, x, y).$$

$$\lambda(0, z) = l(z),$$

$$\lambda(k+1, z) = [k+1] \cdot \lambda(k, z)^2.$$

$$\tau(0, z) = z,$$

$$\tau(k+1, z) = \prod_{n=0}^{\lambda(k+1, z)-1} [Pr(n+1)] \exp \left\{ \psi \left(\left[\frac{n}{\lambda(k, z)^2} \right], \left[[1 Gl Dy (\text{Rem}(n, \lambda(k, z)^2))] + 1 \right] Gl \tau(k, z), \left[[2 Gl Dy (\text{Rem}(n, \lambda(k, z)^2))] + 1 \right] Gl \tau(k, z) \right) \right\}.$$

$$\mu(n, z) = \varepsilon t [t \leq n \& n < \sum_{i=0}^t \lambda(i, z)].$$

$$\nu(n, z) = \left[\sum_{i=0}^{\mu(n, z)} \lambda(i, z) \right] - n.$$

$$\theta(z, m) = \nu(m, z) Gl \tau(\mu(m, z), z).$$

Then if z or $\tau(0, z)$ is the Gödel number for the sequence S_0 of the $\lambda(0, z)$ numbers z_1, \dots, z_t ($z_1, \dots, z_t > 0$), $\tau(k+1, z)$ is the Gödel number

for the sequence S_{k+1} of the $\lambda(k+1, z)$ numbers $\psi(n, x, y)$, for $n = 0, \dots, k$ and x and y ranging over S_k , in a certain order. Since $\psi(0, x, y) = x$, S_k includes all numbers in S_j for $0 \leq j \leq k$. When $l(z) > 0$, $\mu(n, z)$ and $\nu(n, z)$ as $n = 0, 1, 2, \dots$ take successively the pairs of values $0\lambda(0, z), 0\lambda(0, z) - 1, \dots, 01; 1\lambda(1, z), 1\lambda(1, z) - 1, \dots, 11; \dots$. Hence $\theta(z, m)$ for $m = 0, 1, 2, \dots$ are the members of S_k ($k = 0, 1, 2, \dots$). But these are (with repetitions) the numbers obtainable from z_1, \dots, z_l by zero or more applications of the operations $\varphi(0, x, y), \varphi(1, x, y), \dots$. Since $\theta(z, m)$ was defined in a manner which shows that it can be obtained from $\varphi(n, x, y)$ and known primitive recursive functions by substitutions and primitive recursions, we have proved:

I. Given a function $\varphi(n, x, y)$, there is a function $\theta(z, m)$, primitive recursive in $\varphi(n, x, y)$ ¹¹, such that, whenever $z = p_1^{z_1} \dots p_l^{z_l} (z_1, \dots, z_l > 0)$, then $\theta(z, 0), \theta(z, 1), \dots$ is an enumeration (with repetitions) of the least class $C(x)$ such that $C(z_1), \dots, C(z_l)$ and $(n, x, y) [C(x) \& C(y) \rightarrow C(\varphi(n, x, y))]$.

We note here the following two theorems for later use:

II. Given a class $A(x)$, a relation $x, y B z$, and a number k which belongs to the least class $C(x)$ such that $(x) [A(x) \rightarrow C(x)]$ and $(x, y, z) [C(x) \& C(y) \& x, y B z \rightarrow C(z)]$, there is a function $\eta(m)$, primitive recursive in $A(x)$ and $x, y B z$, such that $\eta(0), \eta(1), \dots$ is an enumeration (with repetitions) of $C(x)$.

$\eta(m)$ is the function $\theta(R(k), m)$ when $\theta(z, m)$ is chosen as in I taking for $\varphi(n, x, y)$ the function $\varepsilon z [z \leqq n + k \& \{ \{ n | 2 \& [(A[(\frac{n}{2})] \& z = [\frac{n}{2}]) \vee (A[(\frac{n}{2})] \& z = k)] \} \vee \{ n + 1 | 2 \& [(x, y B [\frac{n+1}{2}] \& z = [\frac{n+1}{2}]) \vee (x, y B [\frac{n+1}{2}] \& z = k)] \} \}]$ ¹².

If a member k of a class $R(x)$ is given, the class is enumerated (allowing repetitions) by the function $\varepsilon y [y \leqq m + k \& \{ (R(m) \& y = m) \vee (\overline{R(m)} \& y = k) \}]$, which is primitive recursive in the class. Similarly:

¹¹) We call a function φ primitive recursive in other functions ψ_i , if φ becomes primitive recursive under the supposition that ψ_i are primitive recursive.

$\prod_{n=0}^{\psi(x, y)} \chi(x, z, n)$ and $\sum_{n=0}^{\psi(x, y)} \chi(x, z, n)$ are primitive recursive in $\psi(x, y)$ and $\chi(x, z, n)$.

Here we use x, y, z as abbreviations for $x_1, \dots, x_n, y_1, \dots, y_m, z_1, \dots, z_l$, resp., and we shall continue to do so when convenient.

¹²) If $k = 0$, replace " $\lambda(0, z) = l(z)$ " by " $\lambda(0, z) = 1$ " in the definition of $\theta(z, m)$.

III. Given a relation $R(x, y)$ and a number k such that $(Ey) R(k, y)$, there is a function $\gamma(m)$, primitive recursive in $R(x, y)$, such that $\gamma(0), \gamma(1), \dots$ is an enumeration (allowing repetitions) of the class $(Ey) R(x, y)$.

$$\gamma(m) = \varepsilon y [y \leq [1 \text{ Glm}] + k \& \{(R(1 \text{ Glm}, 2 \text{ Glm}) \& y = 1 \text{ Glm}) \\ \vee \overline{(R(1 \text{ Glm}, 2 \text{ Glm}) \& y = k)}\}].$$

By applying I, taking for $\varphi(n, x, y)$ the function $R'(n, x, y)$ (21), we obtain a primitive recursive function:

25. $H(z, m)$.

If z corresponds to a system of equations $Z, H(z, 0), H(z, 1), \dots$ is an enumeration (with repetitions) of the numbers corresponding to equations Y such that $Z \vdash_{0, 1, 2, \dots} Y$.

Now let $\varphi(\mathfrak{x})$ be a recursive function in the sense of Def. 2a or Def. 2b. Then there is a system E of equations defining φ recursively under Def. 2b; suppose that ϱ_a stands for φ in E . The system E has a Gödel number e . Using 23 and 25, if $R(\mathfrak{x}, y) \equiv \text{Eval}_{r_a}(a, H(e, y), \mathfrak{x})$, then, by Def. 2b, $(\mathfrak{x})(Ey) R(\mathfrak{x}, y)$. Furthermore, using 24, if $\psi(y) = \text{Val}(H(e, y))$, then $\varphi(\mathfrak{x}) = \psi(\varepsilon y [R(\mathfrak{x}, y)])$. We have now proved:

IV. Every function recursive in the sense of Def. 2a (or Def. 2b) is expressible in the form $\psi(\varepsilon y [R(\mathfrak{x}, y)])$, where $\psi(y)$ is a primitive recursive function and $R(\mathfrak{x}, y)$ a primitive recursive relation and $(\mathfrak{x})(Ey) R(\mathfrak{x}, y)$.

Thus the extension of general over primitive recursive functions consists only in that to substitutions and primitive recursions is added the operation of seeking indefinitely through the series of natural numbers for one satisfying a primitive recursive relation.

By Gödel S. 180ⁱ IV, $\varepsilon y [R(\mathfrak{x}, y)]$ is primitive recursive in $R(\mathfrak{x}, y)$ and any function $\chi(\mathfrak{x})$ which bounds y . Hence, in a certain sense, the length of the computation algorithm of a recursive function which is not also primitive recursive grows faster with the arguments than the value of any primitive recursive function¹³⁾.

Given a relation $R(\mathfrak{x})$, the function $\varrho(\mathfrak{x})$ which is 0 or 1, according as $R(\mathfrak{x})$ holds or not, may be called the representing function of $R(\mathfrak{x})$. As with primitive recursions, we say that $R(\mathfrak{x})$ is recursive, if its representing function is recursive (under Def. 2a)¹⁴⁾.

¹³⁾ Besides the method, for demonstrating that a function is not primitive recursive (or not definable by given additional means, such as recursions with respect to n variables simultaneously), which consists in finding a lower bound for the values, we have the method, for demonstrating relationships of the opposite kind, which consists in finding an upper bound for the number of steps in the computation algorithm.

¹⁴⁾ This is equivalent to saying that there is a recursive function $\varrho'(\mathfrak{x})$ such that $R(\mathfrak{x}) \sim [\varrho'(\mathfrak{x}) = 0]$, since then $\varrho(\mathfrak{x}) = 1 - (1 - \varrho'(\mathfrak{x}))$.

ⁱ15,16



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

For, to every proposition of the form $(\exists)(E \eta) R(\bar{x}, \eta)$, there is an equivalent proposition of the form $(x)(E y) R(x, y)$ obtained by utilizing the recursive enumerability of n -tuples of natural numbers, or introducing fictive variables²⁴); and the Gödel number e of the system E of equations which defines $\varepsilon y[R(x, y)]$ in the proof of V on the supposition that $(x)(E y) R(x, y)$ satisfies the present theorem. Similarly, $(E \eta) R(\eta)$ has an equivalent $(E y) R(y)$, and for e we may take the Gödel number of the equations defining $\varepsilon y[R(y) \& x = x]$ on the supposition that $(E y) R(y)$ ²⁵.

My thanks are due to Prof. Paul Bernays for the suggestion of improvements in the presentation.

²⁴) E. g. $(x_1, x_2, x_3) R(x_1, x_2, x_3) \equiv (x)(E y)[R(1Gl x, 2Gl x, 3Gl x) \& y = y]$.

²⁵) XV, XVI, and XVII are similar, respectively, to results obtained in a different connection by Prof. Alonzo Church (An unsolvable problem of elementary number theory, see Bull. Amer. Math. Soc. Abstract 41—5—205), Dr. J. B. Rosser (unpublished), and the present writer (A theory of positive integers in formal logic, Part II, Amer. Jour. Math. 57 No. 2, pp. 230 ff.).

RECURSIVE PREDICATES AND QUANTIFIERS

Although this paper does not develop a specific formalism, the arguments really refer to one. The reader is advised to think of the formalism referred to by the author as that of his earlier paper, this anthology, 236-253. In this paper, the results of the earlier paper are reobtained in strengthened form and in a simplified way. But there is also much new ground covered. Recursiveness is extended to relative recursiveness and the classification of arithmetic predicates in the now classical "Kleene hierarchy" according to their quantificational prefix is introduced. Gödel's incompleteness theorem is discussed from a general and revealing point of view. Some of this discussion overlaps Post's paper, this anthology, pp. 304-337. For the reader who compares the two, it may help to note that what Post calls a recursively enumerable set is just a set which can be defined by a predicate of the form $(Ex)R(a,x)$ where $R(a,x)$ is a recursive predicate. It should also be noted that the author uses the term "elementary predicate" for "arithmetic predicate".

The correction below and the addendum on p. 287 were supplied by the author for this anthology:

Correction: Omit §15, because the result claimed from Kleene [5] on which that section depends is false. The error in the supposed proof in [5] was indicated in the bibliographical reference to [5] (=Kleene 1944) on p. 527 of Kleene's Introduction to Metamathematics (1952). A full discussion and corrected result are given in S. C. Kleene, "On the forms of the predicates in the theory of constructive ordinals (second paper)", Amer. J. Math., vol. 77 (1955), pp. 405-428.

Stephen C. Kleene

RECURSIVE PREDICATES AND QUANTIFIERS¹

This paper contains a general theorem on the quantification of recursive predicates, with applications to the foundations of mathematics. The theorem (Theorem II) is a slight extension of previous results on Herbrand-Gödel general recursive functions⁽²⁾, while the applications include theorems of Church (Theorem VII)⁽³⁾ and Gödel (Theorem VIII)⁽⁴⁾ and other incompleteness theorems. It is thought that in this treatment the relationship of the results stands out more clearly than before.

The general theorem asserts that to each of an enumeration of predicate forms, there is a predicate not expressible in that form. The predicates considered belong to elementary number theory.

The possibility that this theorem may apply appears whenever it is proposed to find a necessary and sufficient condition of a certain kind for some given property of natural numbers; in other words, to find a predicate of a given kind equivalent to a given predicate. If the specifications on the predicate which is being sought amount to its having one of the forms listed in the theorem, then for some selection of the given property a necessary and sufficient condition of the desired kind cannot exist.

In particular, it is recognized that to find a complete algorithmic theory for a predicate $P(a)$ amounts to expressing the predicate as a recursive predicate. By one of the cases of the theorem, this is impossible for a certain $P(a)$, which gives us Church's theorem.

Again, when we recognize that to give a complete formal deductive theory (symbolic logic) for a predicate $P(a)$ amounts to finding an equivalent predicate of the form $(\exists x)R(a, x)$ where $R(a, x)$ is recursive, we have immediately Gödel's theorem, as another case of the general theorem.

Still another application is made, when we consider the nature of a constructive existence proof. It appears that there is a proposition provable classically for which no constructive proof is possible (Theorem X).

The endeavor has been made to include a fairly complete exposition of definitions and results, including relevant portions of previous theory, so that

^c American Mathematical Society, 1943, All Rights Reserved. Reprinted by permission from the TRANSACTIONS, Volume 53, No. 1, pages 41-73.

⁽¹⁾ A part of the work reported in this paper was supported by the Institute for Advanced Study and the Alumni Research Foundation of the University of Wisconsin.

⁽²⁾ Gödel [2, §9] (see the bibliography at the end of the paper).

⁽³⁾ Church [1].

⁽⁴⁾ Gödel [1, Theorem VI].



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

For the interpretation of the propositions we have required, as minimum, only the notions of effectively calculable predicates and of the quantifiers used constructively. It seems that lesser presuppositions, if one is to allow any mathematical infinite, are hardly conceivable.

Beyond that the system should fulfil the structural characteristic expressed in Thesis II, and should yield results correct under this modicum of interpretation, we have need of no reference whatsoever to its detailed constitution.

In particular, the nature of the intuitive evidence for the deductive processes which are formalized in the system plays no role.

Let us imagine an omniscient number theorist, whom we should expect, through his ability to see infinitely many facts at once, to be able to frame much stronger systems than any we could devise. Any correct system which he could reveal to us, telling us how it works without telling us why, would be equally subject to the Gödel incompleteness.

It is impossible to confine the intuitive mathematics of elementary propositions about integers to the extent that all the true theorems will follow from explicitly stated axioms by explicitly stated rules of inference, simply because the complexity of the predicates soon exceeds the limited form representing the concept of provability in a stated formal system.

We selected as the objective in constructing a formal deductive system that what constitutes proof should be made explicit in the sense that a proposed proof could be effectively checked, and either declared formally correct or declared formally incorrect.

Let us for the moment entertain a weaker conception of a formal system, under which, if we should happen to discover a correct proof of a proposition or be presented with one, then we could check it and recognize its formal correctness, but if we should have before us an alleged proof which is not correct, then we might not be able definitely to locate the formal fallacy. In other words, under this conception a system possesses a process for checking, which terminates in the affirmative case, but need not in the negative. Then the concept of provability would have the form $(Ex)P^+(a, x)$ where P^+ is the positive completion of a partial recursive predicate $P(a, x)$. By Theorem VI, $P^+(a, x)$ is expressible in the form $(Ey)R(a, x, y)$ where R is general recursive. Then the provability concept has the form $(Ex)(Ey)R(a, x, y)$, or by contraction of quantifiers $(Ex)R(a, (x)_1, (x)_2)$. This is of the form $(Ex)R(a, x)$ where R is general recursive. Thus the concept of provability has the usual form, and Gödel's theorem applies as before. If we take a new concept of proof based on $R(a, x)$, that is, if we redesignate the steps in the checking process as the formal proof steps, the concept of proof assumes the usual form.

We gave no attention, when we formulated the objectives both of an algorithmic and of a formal deductive theory, to the nature of the evidence for the correctness of the theory, or to various other practical considerations,

simply because the crude structural objectives suffice to entail the corresponding incompleteness theorems. In this connection, it may be of some interest to give the corresponding definitions, although these may not take into account all the desiderata, for the case of incomplete theories of the two sorts. We shall state these for predicates of n variables a_1, \dots, a_n , as we could also have done for the case of the complete theories.

To give an *algorithmic theory* (not necessarily complete) for a predicate $P(a_1, \dots, a_n)$ is to give a general recursive function $\pi(a_1, \dots, a_n)$, taking only 0, 1, and 2 as values, such that

$$(36) \quad \begin{cases} \pi(a_1, \dots, a_n) = 0 \rightarrow P(a_1, \dots, a_n) \\ \pi(a_1, \dots, a_n) = 1 \rightarrow \overline{P}(a_1, \dots, a_n). \end{cases}$$

The algorithm always terminates, but if $\pi(a_1, \dots, a_n)$ has the value 2 we can draw no conclusion about $P(a_1, \dots, a_n)$.

To give a *formal deductive theory* (not necessarily complete) for a predicate $P(a_1, \dots, a_n)$ is to give a general recursive predicate $R(a_1, \dots, a_n, x)$ such that

$$(37) \quad (\exists x)R(a_1, \dots, a_n, x) \rightarrow P(a_1, \dots, a_n).$$

In words, to give a formal deductive theory for a predicate $P(a_1, \dots, a_n)$ is to find a sufficient condition for it of the form $(\exists x)R(a_1, \dots, a_n, x)$ where R is general recursive. Here, according to circumstances, the sufficiency may be established from a wider context, or it may be a matter of postulation (hypothesis), or of conviction (belief).

From the present standpoint, the setting up of this sufficient condition is the essential accomplishment in the establishment of a so-called metatheory (in the constructive sense) for the body of propositions taken as the values of a predicate. We note that this may be accomplished without necessarily going through the process of setting up a formal object language, from which R is obtainable by subsequent arithmetization, although as remarked above, we can always set up the object language, if we have the R by some other means.

In the view of the present writer, the interesting variations of formal technique recently considered by Curry have the above as their common feature with formalization of the more usual sort⁽³⁰⁾. This is stated in our terminology, Curry's use of the terms "meta" and "recursive" being different. He gives examples of "formal systems," in connection with which he introduces some predicates by what he calls "recursive definitions," but what we should prefer to call "inductive definitions." This important type of definition, under suitable precise delimitation so that the individual clauses are constructive, can be shown to lead always to predicates expressible in the form $(\exists x)R(a_1, \dots, a_n, x)$ where R is recursive in our sense. Indeed, this fact

⁽³⁰⁾ Curry [1].



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

be refuted intuitionistically, for a certain A . Hitherto the intuitionistic refutations of laws of the classical predicate calculus have depended on the interpretation of the quantifiers in intuitionistic set theory⁽⁴⁰⁾.

The result of Theorem X, with another proposition as example, can be reached as follows. Consider the proposition,

$$(x)(Ey) \{ [(Ex)T_1(x, x, z) \& y = 0] \vee [(z)\bar{T}_1(x, x, z) \& y = 1] \}.$$

This holds classically, by application of the law of the excluded middle in the form

$$(x) \{ (Ex)A(x, z) \vee (z)\bar{A}(x, z) \},$$

or the form

$$(x)(A(x) \vee \bar{A}(x)),$$

from which the other follows by substituting $(Ex)A(x, z)$ for $A(x)$. But it is not recursively fulfillable, since it can be fulfilled only by the representing function of the predicate $(Ex)T_1(x, x, z)$, which, as we saw in the proof of Theorem II, is non-recursive.

17. Non-elementary predicates. The elementary predicates are enumerable. By Cantor's methods, there are therefore non-elementary number-theoretic predicates. However let us ask what form of definition would suffice to give such a predicate. Under classical interpretations, the enumeration of predicate forms given in Theorem II for n variables suffices for the expression of every elementary predicate of n variables. By defining relations of the form shown in the next theorem, we can introduce a predicate $M(a, k)$ so that it depends for different values of k on different numbers of alternating quantifiers. On the basis of Theorem II, it is possible to do this in such a way that the predicate will be expressible in none of the forms of Theorem II.

THEOREM XI. *Classically, there is a non-elementary predicate $M(a, k)$ definable by relations of the form*

$$\begin{cases} M(a, 0) \equiv R(a) \\ M(a, 2k + 1) \equiv (Ex)M(\phi(a, x), 2k) \\ M(a, 2k + 2) \equiv (x)M(\phi(a, x), 2k + 1) \end{cases}$$

where R and ϕ are primitive recursive.

We are dealing here with essentially the same fact which Hilbert-Bernays discover by setting up a truth definition for their formal system (Z) ⁽⁴¹⁾.

The system (Z) has as primitive terms only ' $,$ ', ' $+$ ', ' \cdot ', ' $=$ ' and the logical operations. The predicates expressible in these terms are elementary. Con-

⁽⁴⁰⁾ Heyting [1, p. 65].

⁽⁴¹⁾ Hilbert and Bernays [1, pp. 328-340].

FINITE COMBINATORY PROCESSES. FORMULATION I.

This paper gives an analysis of the computing process substantially identical to that given by Turing (this anthology, p. 116–154). Although this work is independent of Turing's, it is not independent of Church's, referring as it does to Church's paper, this anthology, pp. 89–107.

Note that what Turing refers to as internal configuration of a machine occurs in Post's treatment as instructions to be carried out by a human computer.

Emil L. Post

FINITE COMBINATORY PROCESSES. FORMULATION I.

The present formulation should prove significant in the development of symbolic logic along the lines of Gödel's theorem on the incompleteness of symbolic logics¹ and Church's results concerning absolutely unsolvable problems.²

We have in mind a *general problem* consisting of a class of *specific problems*. A solution of the general problem will then be one which furnishes an answer to each specific problem.

In the following formulation of such a solution two concepts are involved: that of a *symbol space* in which the work leading from problem to answer is to be carried out,³ and a fixed unalterable *set of directions* which will both direct operations in the symbol space and determine the order in which those directions are to be applied.

In the present formulation the symbol space is to consist of a two way infinite sequence of spaces or boxes, i.e., ordinally similar to the series of integers $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$. The problem solver or worker is to move and work in this symbol space, being capable of being in, and operating in but one box at a time. And apart from the presence of the worker, a box is to admit of but two possible conditions, i.e., being empty or unmarked, and having a single mark in it, say a vertical stroke.

One box is to be singled out and called the starting point. We now further assume that a specific problem is to be given in symbolic form by a finite number of boxes being marked with a stroke. Likewise the answer is to be given in symbolic form by such a configuration of marked boxes. To be specific, the answer is to be the configuration of marked boxes left at the conclusion of the solving process.

The worker is assumed to be capable of performing the following primitive acts:⁴

- (a) *Marking the box he is in (assumed empty),*
- (b) *Erasing the mark in the box he is in (assumed marked),*
- (c) *Moving to the box on his right,*
- (d) *Moving to the box on his left,*
- (e) *Determining whether the box he is in, is or is not marked.*

The set of directions which, be it noted, is the same for all specific problems and thus corresponds to the general problem, is to be of the following form. It is to be headed:

Start at the starting point and follow direction 1.

Received October 7, 1936. The reader should compare an article by A. M. Turing, *On computable numbers*,^a shortly forthcoming in the *Proceedings of the London Mathematical Society*. The present article, however, although bearing a later date, was written entirely independently of Turing's. *Editor.*

¹ Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, *Monatshefte für Mathematik und Physik*, vol. 38 (1931), pp. 173–198.^a

² Alonzo Church, *An unsolvable problem of elementary number theory*, *American Journal of Mathematics*, vol. 58 (1936), pp. 345–363.^a

³ Symbol space, and time.

⁴ As well as otherwise following the directions described below.

It is then to consist of a finite number of directions to be numbered 1, 2, 3, . . . n. The i th direction is then to have one of the following forms:

(A) Perform operation O_i [$O_i = (a), (b), (c)$, or (d)] and then follow direction j_i ,

(B) Perform operation (e) and according as the answer is yes or no correspondingly follow direction j_i' or j_i'' ,

(C) Stop.

Clearly but one direction need be of type C. Note also that the state of the symbol space directly affects the process only through directions of type B.

A set of directions will be said to be *applicable* to a given general problem if in its application to each specific problem it never orders operation (a) when the box the worker is in is marked, or (b) when it is unmarked.⁵ A set of directions applicable to a general problem sets up a deterministic process when applied to each specific problem. This process will terminate when and only when it comes to the direction of type (C). The set of directions will then be said to set up a *finite 1-process* in connection with the general problem if it is applicable to the problem and *if the process it determines terminates for each specific problem*. A finite 1-process associated with a general problem will be said to be a *1-solution* of the problem if the answer it thus yields for each specific problem is always correct.

We do not concern ourselves here with how the configuration of marked boxes corresponding to a specific problem, and that corresponding to its answer, symbolize the meaningful problem and answer. In fact the above assumes the specific problem to be given in symbolized form by an outside agency and, presumably, the symbolic answer likewise to be received. A more self-contained development ensues as follows. The general problem clearly consists of at most an enumerable infinity of specific problems. We need not consider the finite case. Imagine then a one-to-one correspondence set up between the class of positive integers and the class of specific problems. We can, rather arbitrarily, represent the positive integer n by marking the first n boxes to the right of the starting point. The general problem will then be said to be *1-given* if a finite 1-process is set up which, when applied to the class of positive integers as thus symbolized, yields in one-to-one fashion the class of specific problems constituting the general problem. It is convenient further to assume that when the general problem is thus 1-given each specific process at its termination leaves the worker at the starting point. If then a general problem is 1-given and 1-solved, with some obvious changes we can combine the two sets of directions to yield a finite 1-process which gives the answer to each specific problem when the latter is merely given by its number in symbolic form.

With some modification the above formulation is also applicable to symbolic logics. We do not now have a class of specific problems but a single initial finite marking of the symbol space to symbolize the primitive formal assertions of the logic. On the other hand, there will now be no direction of type (C). Consequently, assuming applicability, a deterministic process will be set up which is *unending*. We further assume that in the course of this process certain recognizable symbol groups, i.e., finite sequences of marked and unmarked boxes, will appear which are not further altered in the course of the process. These will be the derived assertions of the logic. Of course the set of directions corresponds to the deductive processes of the logic. The logic may then be said to be *1-generated*.

An alternative procedure, less in keeping, however, with the spirit of symbolic

* While our formulation of the set of directions could easily have been so framed that applicability would immediately be assured it seems undesirable to do so for a variety of reasons.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

verified from the deterministic character of the Turing machine, and from the forms of the above operations, that at most one of these operations is applicable to any string having no more than one occurrence of a q therein, and then in only one way.

The unsolvable problem that is to yield the unsolvability of the problem of Thue would seem to be furnished by the following result of Turing's [7, p. 248]:ⁱⁱ "There can be no machine \mathfrak{G} which, when supplied with the S.D of an arbitrary machine \mathfrak{M} , will determine whether \mathfrak{M} ever prints a given symbol (0 say)." There are, however, difficulties in using this result as given due to peculiarities of Turing's development. (The matter is discussed in the appendix.) We therefore proceed independently of Turing as follows.

We start with the known recursive unsolvability of the decision problem for the class of normal systems on two letters a, b .⁶ It suffices here to think of this problem as consisting of a class of questions, each question Q being symbolized by a string on a given finite set of letters. By methods such as those used by Turing in setting up his universal computing machine [7], we then set up the quadruplets (3) of a fixed Turing machine with certain letters S_1, S_2, \dots, S_m , and internal configurations q_1, q_2, \dots, q_n , and give an effective method for translating each question Q into a Q' of form (2) to serve as the initial state of tape versus machine, the construction being such that the following is true. The answer to question Q is yes, or no, according as the constructed machine, when applied to Q' , does, or does not, in the course of its operation print a certain fixed letter S_p . This letter S_p is not present in the Q' of any Q . Since such methods are fully exploited by Turing in [7], we do not give the details of this construction.⁷

Now, given Q , form the semi-Thue system T' with initial assertion $hQ'h$, and operations (4)–(8) corresponding to this Turing machine. Then, the answer to Q is yes, or no, according as some assertion of T' involves the letter S_p , or no assertion involves that letter. We now modify T' as follows. Delete all operations in T' such that the S_i of the premise, the symbol on the scanned square of the Turing machine, is S_p . Since, when S_p is first printed, it can appear so only as the S_k of (8), and thus would be the S_i of a next operation, the deductive processes of the semi-Thue system will now stop the first time S_p appears in an assertion. We now add operations which, in deterministic fashion, will erase all of this assertion except for the two h 's and the q , while changing this q . For this purpose, we introduce two new "internal configurations"

⁶ See [5, footnote 2]. The specific form of this problem, however, need not be known by the reader for an understanding of the present argument.

⁷ This work was carried through before the definitive study of Turing's paper [7], referred to in the appendix, was made. As a result, some differences of method appear. A minor difference is that where Turing uses the method of "marking" a sequence of symbols [7, p. 235] to distinguish it, we introduce the effect of movable physical markers; two, indeed, suffice. A major difference is that instead of the m -configuration functions of Turing's skeleton tables [7, p. 236], we introduce a symbolism and technique based on the concept of a subset of directions of a given set of directions. Both differences were suggested by [2]. They may, perhaps, better be exploited in a more general setting.ⁱ

ⁱ For page references in this footnote, the reader should subtract 114 from the page given in order to obtain the corresponding page in this anthology.

q_{R+1} and q_{R+2} . We further alter the operations of T' by changing the q_i of each operation (8) for which S_k is S_p , to q_{R+1} , and add the following operations:

$$PS_n q_{R+1} Q \text{ produces } Pq_{R+1} Q, n = 0, 1, \dots, m; n \neq p. \quad (9)$$

$$Phq_{R+1} Q \text{ produces } Phq_{R+2} Q. \quad (10)$$

$$Pq_{R+2} S_n Q \text{ produces } Pq_{R+2} Q, n = 0, 1, \dots, m. \quad (11)$$

Note that as a result of the previous changes, when S_p first appears in an assertion, the q therein is q_{R+1} . Operations (9) then serve to erase the S 's of that assertion to the left of q_{R+1} , (10) then changes q_{R+1} to q_{R+2} , (11) erases the S 's to the right of q_{R+2} . Finally, therefore, the assertion becomes $hq_{R+2}h$, to which no further operation is applicable. Call the resulting semi-Thue system T'' . Clearly, for T'' it is also true that at most one of its operations is applicable to any string having no more than one occurrence of a q therein, and then in only one way. It follows that the answer to Q is yes, or no, according as $hq_{R+2}h$ is, or is not, an assertion in T'' , the operations of T'' operating one by one in deterministic fashion, and, in the former case, terminating in $hq_{R+2}h$.

The proof of the reducibility of our initial unsolvable problem to the problem of Thue essentially becomes the proof of the following two lemmas.⁸ By the *inverse* of an operation of the form PAQ produces PBQ we shall mean the operation PBQ produces PAQ . Let T''' be the semi-Thue system with primitive assertion $hq_{R+2}h$ and operations the inverses of those of T'' . We then have:

LEMMA I. The primitive assertion $hq_{R+2}h$ of T''' is an assertion of T'' when, and only when, the primitive assertion $hQ'h$ of T'' is an assertion of T''' .

Proof. D is a result of applying “ PAQ produces PBQ ” to C when, and only when, C is a result of applying the inverse operation “ PBQ produces PAQ ” to D . For both statements are equivalent to the existence of strings P and Q such that $PAQ = C$, $PBQ = D$. If, then, operations O_1, O_2, \dots, O_n of T'' lead from its primitive assertion $hQ'h$ through assertions C_1, C_2, \dots, C_{n-1} to the assertion $hq_{R+2}h$, the inverses of these operations, all in T''' , will in reverse order lead from $hq_{R+2}h$, the primitive assertion of T''' , through C_{n-1}, \dots, C_2, C_1 to $hQ'h$; and conversely.

As a result of Lemma I, the answer to question Q is yes, or no, according as $hQ'h$ is, or is not, an assertion of T''' . Note that while the initial assertion of T'' depended on Q , T''' is the same for all Q 's. Now let T be the Thue system obtained from the semi-Thue system T''' by adding to the latter the inverse of each of its operations. We then have:

LEMMA II. The class of assertions of T is identical with the class of assertions of T''' .

Proof. Each assertion of T''' is, of course, an assertion of T . For the converse, let operations O_1, O_2, \dots, O_n of T lead from its primitive assertion $hq_{R+2}h$, through assertions C_1, C_2, \dots, C_{n-1} , to an assertion C of T . If n is zero, C is $hq_{R+2}h$, and hence an assertion of T''' . Otherwise, note that the operations of T , being those of T''' and their inverses, are the combined operations of T'''

⁸ These lemmas can be made more general.

start operating on a tape previously marked. From Turing's frequent references to the beginning of the tape, and the way his universal computing machine treats motion left, we gather that, unlike our tape, this tape is a one-way infinite affair going right from an initial square.

Primarily as a matter of practice, Turing makes his machines satisfy the following convention. Starting with the first square, alternate squares are called *F*-squares, the rest, *E*-squares. In its action the machine then never directs motion left when it is scanning the initial square, never orders the erasure, or change, of a symbol on an *F*-square, never orders the printing of a symbol on a blank *F*-square if the previous *F*-square is blank and, in the case of a computing machine, never orders the printing of 0 or 1 on an *E*-square. This convention is very useful in practice. However the actual performance, described below, of the universal computing machine, coupled with Turing's proof of the second of the two theorems referred to above, strongly suggests that Turing makes this convention part of the definition of an arbitrary machine. We shall distinguish between a Turing machine and a Turing convention-machine.

By a uniform method of representation, Turing represents the set of instructions, corresponding to our quadruplets,¹² which determine the behavior of a machine by a single string on seven letters called the standard description (S.D) of the machine. With the letters replaced by numerals, the S.D of a machine is considered the arabic representation of a positive integer called the description number (D.N) of the machine. If our critique is correct, a machine is said to be circle-free if it is a Turing computing convention-machine which prints an infinite number of 0's and 1's.¹³ And the two theorems of Turing's in question are really the following. There is no Turing convention-machine which, when supplied with an arbitrary positive integer n , will determine whether n is the D.N of a Turing computing convention-machine that is circle-free. There is no Turing convention-machine which, when supplied with an arbitrary positive integer n , will determine whether n is the D.N of a Turing computing convention-machine that ever prints a given symbol (0 say).¹⁴

In view of [8], these "no machine" results are no doubt equivalent to the re-

¹² Our quadruplets are quintuplets in the Turing development. That is, where our standard instruction orders either a printing (overprinting) or motion, left or right, Turing's standard instruction always orders a printing and a motion, right, left, or none. Turing's method has certain technical advantages, but complicates theory by introducing an irrelevant "printing" of a symbol each time that symbol is merely passed over.

¹³ "Genuinely prints," that is, a genuine printing being a printing in an empty square. See the previous footnote.

¹⁴ Turing in each case refers to the S.D of a machine being supplied. But the proof of the first theorem, and the second theorem depends on the first, shows that it is really a positive integer n that is supplied. Turing's proof of the second theorem is unusual in that while it uses the unsolvability result of the first theorem, it does not "reduce" [4] the problem of the first theorem to that of the second. In fact, the first problem is almost surely of "higher degree of unsolvability" [4] than the second, in which case it could not be "reduced" to the second. Despite appearances, that second unsolvability proof, like the first, is a *reductio ad absurdum* proof based on the definition of unsolvability, at the conclusion of which, the first result is used.

determine whether n is the D.N of an arbitrary Turing machine that ever prints a given symbol (0 say).¹⁹

These alternative procedures assume that Turing's universal computing machine is retained. However, in view of the above discussion, it seems to the writer that Turing's preoccupation with computable numbers has marred his entire development of the Turing machine. We therefore suggest a redevelopment of the Turing machine based on the formulation given in the body of the present paper. This could easily include computable numbers by defining a computable sequence of 0's and 1's as the *time sequence* of printings of 0's and 1's by an arbitrary Turing machine, provided there are an infinite number of such printings. By adding to Turing's complete configuration a representation of the act last performed, a few changes in Turing's method would yield a universal computing machine which would transform such a time sequence into a space sequence. Turing's convention would be followed as a matter of useful practice in setting up this, and other, particular machines. But it would not infect the theory of arbitrary Turing machines.

REFERENCES

- [1] Alonzo Church, *An unsolvable problem of elementary number theory*, *American journal of mathematics*, vol. 58 (1936), pp. 345–363.^a
- [2] Emil L. Post, *Finite combinatory processes—formulation 1*, this JOURNAL, vol. 1 (1936), pp. 103–105.^a
- [3] Emil L. Post, *Formal reductions of the general combinatorial decision problem*, *American journal of mathematics*, vol. 65 (1943), pp. 197–215.
- [4] Emil L. Post, *Recursively enumerable sets of positive integers and their decision problems*, *Bulletin of the American Mathematical Society*, vol. 50 (1944), pp. 284–316.^a
- [5] Emil L. Post, *A variant of a recursively unsolvable problem*, ibid., vol. 52 (1946), pp. 264–268.
- [6] Axel Thue, *Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln*, *Skrifter utgit av Videnskapselskapet i Kristiania*, I. Matematisk-naturvidenskabelig klasse 1914, no. 10 (1914), 34 pp.
- [7] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, *Proceedings of the London Mathematical Society*, ser. 2 vol. 42 (1937), pp. 230–265.^a
- [8] A. M. Turing, *Computability and λ -definability*, this JOURNAL, vol. 2 (1937), pp. 153–163.

¹⁹ It is here assumed that the suggested extension of [8] includes a proof to the effect that the existence of an arbitrary Turing machine for solving a given problem is equivalent to the existence of a Turing convention-machine for solving that problem.

RECURSIVELY ENUMERABLE SETS OF POSITIVE INTEGERS AND THEIR DECISION PROBLEMS

This paper initiated the classification theory of recursively enumerable sets. Because of its clear informal style, the early part of this paper can be recommended as an introduction to the theory of recursive functions and to its relation to Gödel's incompleteness theorem. The later part contains ingenious constructions and raises the question which came to be known as Post's problem: Can there be two recursively enumerable but non-recursive sets such that the first is recursive relative to the second (i.e. using the second as an "oracle") but not vice versa? This question was answered much later in the affirmative by Richard Friedberg (*Proceedings of the National Academy of Sciences (U. S. A.)*, vol. 43(1957), pp. 236–238) and independently by A. A. Muchnik (*Doklady Akademii Nauk S. S. R.*, n.s. vol. 108(1956), pp. 194–197).

Emil Post

RECURSIVELY ENUMERABLE SETS OF POSITIVE INTEGERS AND THEIR DECISION PROBLEMS

Introduction. Recent developments of symbolic logic have considerable importance for mathematics both with respect to its philosophy and practice. That mathematicians generally are oblivious to the importance of this work of Gödel, Church, Turing, Kleene, Rosser and others as it affects the subject of their own interest is in part due to the forbidding, diverse and alien formalisms in which this work is embodied. Yet, without such formalism, this pioneering work would lose most of its cogency. But apart from the question of importance, these formalisms bring to mathematics a new and precise mathematical concept, that of the general recursive function of Herbrand-Gödel-Kleene, or its proved equivalents in the developments of Church and Turing.¹ It is the purpose of this lecture to demonstrate by example that this concept admits of development into a mathematical theory much as the group concept has been developed into a theory of groups. Moreover, that stripped of its formalism, such a theory admits of an intuitive development which can be followed, if not indeed pursued, by a mathematician, layman though he be in this formal field. It is this intuitive development of a very limited portion of a sub-theory of the hoped for general theory that we present in this lecture. We must emphasize that, with a few exceptions explicitly so noted, we have obtained formal proofs of all the consequently mathematical theorems here developed informally. Yet the real mathematics involved must lie in the informal development. For in every instance the informal "proof" was first obtained; and once gotten, transforming it into the formal proof turned out to be a routine chore.²

We shall not here reproduce the formal definition of *recursive function of positive integers*. A simple example of such a function is an

© American Mathematical Society, 1944, All Rights Reserved. Reprinted by permission from the BULLETIN, Volume 50, pages 284-316.

¹ For "general recursive function" see [9] ([8] a prerequisite), [12] and [11]; for Church's " λ -defineability," [1] and [6]; for Turing's "computability," [24] and the writer's related [18]. To this may be added the writer's method of "canonical systems and normal sets" [19]. See pp. 39-42 and bibliography of [6] for a survey of the literature and further references. Numbers in brackets refer to the bibliography at the end of the paper.

² Our present formal proofs, while complete, will require drastic systematization and condensation prior to publication.

arbitrary polynomial $P(x_1, x_2, \dots, x_n)$, with say non-negative integral coefficients, and not identically zero. If the x 's are assigned arbitrary positive integral values expressed, for example, in the arabic notation, the algorithms for addition and multiplication in that notation enable us to calculate the corresponding positive integral value of the polynomial. That is, $P(x_1, x_2, \dots, x_n)$ is an *effectively calculable function of positive integers*. The importance of the technical concept recursive function derives from the overwhelming evidence that it is coextensive with the intuitive concept effectively calculable function.³

A set of positive integers is said to be *recursively enumerable* if there is a recursive function $f(x)$ of one positive integral variable whose values, for positive integral values of x , constitute the given set. The sequence $f(1), f(2), f(3), \dots$ is then said to be a *recursive enumeration* of the set. The corresponding intuitive concept is that of an *effectively enumerable* set of positive integers. To prepare us in part for our intuitive approach, consider the following three examples of recursively enumerable sets of positive integers.

- (a): $1^2, 2^2, 3^2, \dots$
- (b): $1, 2, 2^{1+2}, 2^{1+2+2^{1+2}}, \dots$
- (c): $1^2, 2^2, 3^2, \dots$
 $1^3, 2^3, 3^3, \dots$
 $1^4, 2^4, 3^4, \dots$
 $\vdots \quad \vdots \quad \vdots \quad \ddots$
 $\vdots \quad \vdots \quad \vdots \quad \ddots$

In the first example, the set is given by a recursive enumeration thereof via the recursive function x^2 . In the second example, the set is generated in a linear sequence, each new element being effectively obtained from the elements previously generated, in this case by raising 2 to the power the sum of the preceding elements. The set is effectively enumerable, since the n th element of the sequence can be found, given n , by regenerating the sequence through its first n elements. In the third example, we rather imagine the positive integers $1, 2, 3, \dots$ generated in their natural order, and, as each positive integer n is generated, a corresponding process set up which generates n^2, n^3, n^4, \dots , all these to be in the set. Actually, the standard method for proving that an enumerable set of enumerable sets is enumerable yields an effective enumeration of the set.

³ See Kleene [13, footnote 2]. In the present paper, "recursive function" means "general recursive function."

Several more examples would have to be given to convey the writer's concept of a *generated set*, in the present instance of positive integers. Suffice it to say that each element of the set is at some time written down, and earmarked as belonging to the set, as a result of predetermined effective processes. It is understood that once an element is placed in the set, it stays there. The writer elsewhere has referred to a generalization which may be restated *every generated set of positive integers is recursively enumerable*.⁴ For comparison purposes this may be resolved into the two statements: every generated set is effectively enumerable, every effectively enumerable set of positive integers is recursively enumerable. The first of these statements is applicable to generated sets of arbitrary symbolic expressions; their converses are immediately seen to be true. We shall find the above concept and generalization very useful in our intuitive development. But while we shall frequently say, explicitly or implicitly, "set so and so of positive integers is a generated, and hence recursively enumerable set," as far as the present enterprise is concerned that is merely to mean "the set has intuitively been shown to be a generated set; it can indeed be proved to be recursively enumerable." Likewise for other identifications of informal concepts with corresponding mathematically defined formal concepts.

At a few points in our informal development we have to lean upon the formal development. The latter is actually yet another formalism, due to the writer [19] but proved completely equivalent to that of general recursive function. It will suffice to give the equivalent of "recursively enumerable set of positive integers" in this development.

A positive integer n is represented in the most primitive fashion by a succession $11 \dots 1$ of n strokes. For working purposes, we introduce the letter b , and consider "strings" of 1's and b 's such as $11b1bb1$. An operation on such strings such as " $b1bP$ produces $P1bb1$ " we term a normal operation. This particular normal operation is applicable only to strings starting with $b1b$, and the derived string is then obtained from the given string by first removing the initial $b1b$, and then tacking on $1bb1$ at the end. Thus $b1bb$ becomes $b1bb1$. " gP produces Pg' " is the form of an arbitrary normal operation. A system in normal form, or normal system, is given by an initial string A of 1's and b 's, and a finite set of normal operations " $g_i P$ produces Pg'_i ," $i = 1, 2, \dots, \mu$. The derived strings of the system are A and all strings obtainable from A by repeated applications of the μ normal

⁴ See [19, p. 201 and footnote 18]. In this connection note Kleene's use of the word "Thesis" in [14, p. 60].⁵ We still feel that, ultimately, "Law" will best describe the situation [18].

operations. Each normal system uniquely defines a set, possibly null, of positive integers, namely the integers represented by those derived strings which are strings of 1's only. It can then be proved that every recursively enumerable set of positive integers is the set of positive integers defined by some normal system, and conversely.⁵ We here, as below, arbitrarily extend the concept recursively enumerable set to include the null set.

By the *basis* B of a normal system, and of the recursively enumerable set of positive integers it defines, we mean the string of letters and symbols here represented by

$$A; g_1 P \text{ produces } Pg'_1, \dots, g_\mu P \text{ produces } Pg'_\mu.$$

When meaningfully interpreted, B determines the normal system, and recursively enumerable set of positive integers, in question. Each basis is but a finite sequence of the symbols 1, b , P , the comma, semi-colon and the letters of the word "produces." The set of bases is therefore enumerably infinite, and can indeed be effectively generated in a sequence of distinct elements

$$O: \quad B_1, B_2, B_3, \dots.$$

Since each B_i defines a unique recursively enumerable set of positive integers and each such set is defined by at least one B_i , O is also an ordering of all recursively enumerable sets of positive integers, though each set will indeed recur an infinite number of times in O . We may then say, in classical terms, that whereas there are 2^{\aleph_0} arbitrary sets of positive integers, there are but \aleph_0 recursively enumerable sets.

By the *decision problem* of a given set of positive integers we mean the problem of effectively determining for an arbitrarily given positive integer whether it is, or is not, in the set. While, in a certain sense, the theory of recursively enumerable sets of positive integers is potentially as wide as the theory of general recursive functions, the decision problems for such sets constitute a very special class of decision problems. Nevertheless they are important, as is shown by the following special and general examples.

One of the problems posed by Hilbert in his Paris address of 1900 [10, problem 10] is the problem of determining for an arbitrary diophantine equation with rational integral coefficients whether it has, or has not, a solution in rational integers. If the variables in a

⁵ We have thus restricted the normal operations and normal systems of [19] because of the following result. If in the initial string and in the normal operations of a normal system with primitive letters 1, $a'_1, \dots, a'_{\mu'}$, each a'_i , $i=1, \dots, \mu'$, is replaced by $b1 \dots 1b$ with i 1's, a normal system with primitive letters 1, b results, defining the same set of strings on 1 only as the original normal system.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

effective calculability, recursive solvability is coextensive with solvability in the intuitive sense. In particular, the decision problem of a recursively enumerable set would be solvable or unsolvable according as the set is, or is not, recursive. More generally than in our two illustrations, through the more precise mechanism of Gödel representations [8], a wide variety of decision and other problems are transformed into problems about positive integers; and whether those problems are, or are not, solvable in the intuitive sense would be equivalent to their being, or not being, recursively solvable in the precise technical sense.

Gödel's classic theorem on the incompleteness and extendibility of symbolic logics [8] in all but wording led him to the recursive unsolvability of a generalization of the above problem of Hilbert [8, 9, 22]. Church explicitly formulated the concept of recursive unsolvability, and arrived at the unsolvability of a number of problems; certainly he proved them recursively unsolvable [1-4]. The above problem of Hilbert begs for an unsolvability proof (see [17]). Like the classic unsolvability proofs, these proofs are of unsolvability by means of given instruments. What is new is that in the present case these instruments, in effect, seem to be the only instruments at man's disposal.

Related to the question of solvability or unsolvability of problems is that of the reducibility or non-reducibility of one problem to another. Thus, if problem P_1 has been reduced to problem P_2 , a solution of P_2 immediately yields a solution of P_1 , while if P_1 is proved to be unsolvable, P_2 must also be unsolvable. For unsolvable problems the concept of reducibility leads to the concept of *degree of unsolvability*, two unsolvable problems being of the same degree of unsolvability if each is reducible to the other, one of lower degree of unsolvability than another if it is reducible to the other, but that other is not reducible to it, of incomparable degrees of unsolvability if neither is reducible to the other. A primary problem in the theory of recursively enumerable sets is the problem of determining the degrees of unsolvability of the unsolvable decision problems thereof. We shall early see that for such problems there is certainly a highest degree of unsolvability. Our whole development largely centers on the single question of whether there is, among these problems, a lower degree of unsolvability than that, or whether they are all of the same degree of unsolvability. Now in his paper on *ordinal logics* [26, section 4], Turing presents as a side issue a formulation which can immediately be restated as the general formulation of the "recursive reducibility" of one problem to another, and proves a result which immediately



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

ν would not be in the set generated by B_ν , that is (1): ν would not be in S_0 . But (B_ν, ν) being of the form (B_n, n) , (2): ν would be in S_0 . Our assumption thus leading to a contradiction, it follows that (B_ν, ν) is not in F . But ν can only be in S_0 by (B_ν, ν) being in F . Hence, ν is not in S_0 . Finally, (B_ν, ν) as proposition says that ν is in S_0 . The proposition (B_ν, ν) is therefore false, that is (B_ν, ν) is in \bar{T} .

For any recursively enumerable subset F of \bar{T} there is then always this couple (B_ν, ν) in \bar{T} , but not in F . On the one hand, then, \bar{T} can never be F . Hence, \bar{T} is not recursively enumerable. By the definitions of this section, and the first theorem of the last, it follows that T , while recursively enumerable, is not recursive. By the decision problem of T we mean the problem of determining for an arbitrarily given member of E whether it is, or is not, in T . But that can be interpreted as the decision problem for the class of recursively enumerable sets of positive integers, that is, the problem of determining for any arbitrarily given recursively enumerable set, that is, arbitrarily given basis B of such a set, and arbitrary positive integer n whether n is, or is not, in the set generated by B . We may therefore say that the decision problem for the class of all recursively enumerable sets of positive integers is recursively unsolvable, and hence, in all probability, unsolvable in the intuitive sense.

On the other hand, since (B_ν, ν) of \bar{T} is not in F , T and F together can never exhaust E . Now T , or any recursively enumerable subset T' of T , in conjunction with F may be called a recursively generated logic relative to the class of enunciations E . For the appearance of (B, n) in T' assures us of the truth of the proposition " n is in the set generated by B ," while its presence in F would guarantee its falseness. We can then say that no recursively generated logic relative to E is complete, since F alone will lead to the (B_ν, ν) which is neither in T' nor in F . That is, (B_ν, ν) is undecidable in this logic. Moreover, if, with a given "basis" for F , the above argument is carried through formally,¹⁴ the recursively enumerable S_0 obtained above will actually be given by a specific basis B which can be constructed by that formal argument. Having found this B , we can then regenerate $O: B_1, B_2, B_3, \dots$, until B is reached, and thus determine the ν such that $B = B_\nu$. That is, given the basis of F , the (B_ν, ν) in \bar{T} and not in F can actually be found. If then we add this (B_ν, ν) to F , a wider recursively enumerable subset F' of \bar{T} results. We may then say that every recursively generated logic relative to E can be extended. Outwardly, these two results, when formally developed, seem to be

¹⁴ Here, the basis of F may be taken to be the basis of the recursively enumerable set of Gödel representations of the members of F . But see the preceding footnote.

Gödel's theorem in miniature. But in view of the generality of the technical concept general recursive function, they implicitly, in all probability, justify the generalization that every symbolic logic is incomplete and extendible relative to the class of propositions constituting E .¹⁵ The conclusion is unescapable that even for such a fixed, well defined body of mathematical propositions, *mathematical thinking is, and must remain, essentially creative*. To the writer's mind, this conclusion must inevitably result in at least a partial reversal of the entire axiomatic trend of the late nineteenth and early twentieth centuries, with a return to meaning and truth as being of the essence of mathematics.

3. The complete set K ; creative sets. Return now to the effective 1-1 correspondence between the set E of distinct (B, n) 's and the set of positive integers obtained via the effective enumeration O' of E . Since T is a recursively enumerable subset of E , the positive integers corresponding to the elements of T constitute a recursively enumerable set of positive integers, K . We shall call K the *complete set*.¹⁶ Since \bar{T} is not recursively enumerable, \bar{K} , which consists of the positive integers corresponding to the elements of \bar{T} , is not recursively enumerable. Now let B be the basis of a recursively enumerable subset α of \bar{K} . The elements of E corresponding to the members of α constitute, then, a recursively enumerable subset F of \bar{T} . Find then the (B_r, ν) of \bar{T} not in F , and, via O' , the positive integer n corresponding to (B_r, ν) . This n will then be an element of \bar{K} not in α .

Actually, we have no general method of telling when a basis B defines a recursively enumerable subset of \bar{K} . Indeed, the above method will yield a unique positive integer n for any basis B of a recursively enumerable set α of positive integers. However, when α is a subset of \bar{K} , n will also be in \bar{K} , but not in α .

Furthermore, even the formal proof of this result merely gives an effective method for finding n , given B . But this method itself can be formalized, so that, as a result, n is given as a "recursive function of B ." This can mean that a recursive function $f(m)$ can be set up such that $n = f(m)$ where $B = B_m$. We now isolate this property of K by setting up the

DEFINITION. *A creative set C is a recursively enumerable set of positive integers for which there exists a recursive function giving a unique*

¹⁵ See Kleene's Theorem XIII in [12] for a mathematically stateable theorem approximating the generality of our informal generalization.

¹⁶ "A complete set" might be better. Just how to abstract from K the property of completeness is not, at the moment, clear. By contrast, see "creative set" below.

positive integer n for each basis B of a recursively enumerable set of positive integers α such that whenever α is a subset of \bar{C} , n is also in \bar{C} , but not in α .

THEOREM. *There exists a creative set; to wit, the complete set K .*

Actually, the class of creative sets is infinite, and very rich indeed as shown by the following easily proved results.¹⁷ If C is a creative set, and E a recursively enumerable set of positive integers, then if E contains \bar{C} , CE is creative, if \bar{C} contains E , $C+E$ is creative. Results of §1 enable us actually to construct creative sets according to the first method by using E 's which are the complements of recursive subsets of C . Results of the rest of this section lead to constructions using the second method.

It is convenient to talk as if the n in the definition of a creative set were determined by the α thereof instead of by the basis B of α . Clearly every creative set C is a recursively enumerable set which is not recursive. For were \bar{C} recursively enumerable, there could be no n in \bar{C} not in the recursively enumerable subset \bar{C} of \bar{C} . The decision problem of each creative set is therefore recursively unsolvable. On the other hand, the complement \bar{C} of any creative set C contains an infinite recursively enumerable set. Recall that every finite set is recursive, and hence recursively enumerable. With, then, α of the definition of creative set as the null set, find the $n=n_1$ of \bar{C} "not in α ." With α the unit set having n_1 as sole member, $n=n_2$ will be in \bar{C} , and distinct from n_1 . With α consisting of n_1 and n_2 , $n=n_3$ will be in \bar{C} , and distinct from n_1 and n_2 , and so on. The set of positive integers n_1, n_2, n_3, \dots is then an infinite generated, and hence recursively enumerable, subset of \bar{C} .

Actually, with this subset of \bar{C} as α , a new element n_ω of \bar{C} is obtained, and so on into the constructive transfinite. But this process is essentially creative. For any mechanical process could only yield n 's forming a generated, and hence recursively enumerable, subset α of \bar{C} , and hence could be transcended by finding that n of \bar{C} not in α .

4. One-one reducibility, to K ; many-one reducibility. Let S_1 and S_2 be any two sets of positive integers. One of the simplest ways in which the decision problem of S_1 would be reduced to the decision problem of S_2 would arise if we had an effective method which would determine for each positive integer n a positive integer m such that n is, or is not, in S_1 according as m is, or is not, in S_2 . For if we could

¹⁷ Of course, all sets abstractly the same as a given creative set, in the sense of §1, are creative. Likewise for our later simple and hyper-simple sets.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Having one simple set, the method of our succeeding §8 can be modified to yield a rich infinite class of simple sets. Clearly, *every simple set S is a recursively enumerable set that is not recursive*. For were S recursive, \bar{S} would be an infinite recursively enumerable subset of \bar{S} . *The decision problem of each simple set is therefore recursively unsolvable*. We thus have obtained two infinite mutually exclusive classes of recursively enumerable sets with recursively unsolvable decision problems, the class of creative sets, and the class of simple sets. They are poles apart in that the complements of creative sets have a creative infinity of infinite recursively enumerable subsets, those of simple sets, not one.

In passing, we may note that every recursively enumerable set of positive integers S with recursively unsolvable decision problem leads to an incompleteness theorem for symbolic logics relative to the class of propositions $n \in S$, n an arbitrary positive integer. Creative sets S are then exactly those recursively enumerable sets of this type each of which admits a universal extendibility theorem as well, simple sets S those for which, given S , each logic can prove the falsity of but a finite number of the infinite set of false propositions $n \in S$.

It is readily seen that no creative set C can be one-one reducible to a simple set S . For under such a reduction, each infinite recursively enumerable subset of \bar{C} , proved above to exist, would be transformed into an infinite recursively enumerable subset of \bar{S} , contradicting the simplicity of S . Simple sets thus offer themselves as *candidates* for recursively enumerable sets with decision problems of lower degree of unsolvability than that of the complete set K . Even for many-one reducibility the situation is no longer immediately obvious; for an infinite recursively enumerable subset of \bar{C} could thus be transformed into a finite subset of \bar{S} , the complement of simple S , without contradiction. However we can actually go much further than that.

6. Reducibility by truth-tables. If S_1 is many-one reducible to S_2 , positive integer n being, or not being, in S_1 may be said to be determined by its correspondent m being, or not being, in S_2 in accordance with the truth-table

(S_2)	m	n	(S_1)
	+	+	
	-	-	

Here, the two signs $+$, $-$ under m represent the two possibilities m is in S_2 , m is not in S_2 , respectively. And by the sign under n in the

same horizontal row as the corresponding sign under m the table in the same language tells whether n correspondingly is (+), or is not (-), in S_1 . The table then says that when m is in S_2 , n is in S_1 , when m is not in S_2 , n is not in S_1 , as required by many-one reducibility. Now there are altogether four ways in which n being, or not being, in S_1 can be made to depend solely on m being, or not being, in S_2 , the signs under n being +, - as above; or +, +; -, -; -, +. If then we have an effective method which for each positive integer n will not only determine a unique corresponding positive integer m , but also one of these four "first order" truth-tables, and if in each case the table is such that for the correct statement of membership or non-membership of m in S_2 , it gives the correct statement of membership or non-membership of n in S_1 , then the decision problem of S_1 will thus be reduced to the decision problem of S_2 . For here also, given n , if we could somehow determine whether m is, or is not, in S_2 , we could thereby determine which row of the corresponding table correctly describes the membership or non-membership of m in S_2 , and from that row correctly determine whether n is, or is not, in S_1 .

More generally, let there be an effective method which for each positive integer n determines a finite sequence of positive integers m_1, m_2, \dots, m_v as well as the m 's depending on n . Let that method correspondingly determine for each n a " v th order" truth-table of the form

(S_2)	m_1	m_2	\dots	m_v	n	(S_1)
+	+	...	+		-	
+	+	...	-		+	
.	
.	
-	-	...	-		-	

Each horizontal row, to the left of the vertical bar, specifies one of the 2^v possible ways in which the v m_i 's may, or may not, be in S_2 , to the right of the bar correspondingly commits itself to one of the statements n is in S_1 , n is not in S_1 . If then for each n that row of the corresponding table which gives the correct statements for the m 's being or not being in S_2 also gives the correct statement regarding the membership or non-membership of n in S_1 , the decision problem of S_1 is again thereby reduced to the decision problem of S_2 .

If such a situation obtains with "effective method" replaced by "recursive method," we shall say that S_1 is *reducible to S_2 by truth-tables*. "Recursive method" here can mean that a suitable Gödel representation of the couple consisting of the sequence $m_1, m_2, \dots,$



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

lows, on the one hand, that for each positive integer n , $k_{\lambda_n} + 1$ is in \bar{H} . On the other hand, $k_{\lambda_{n+1}}$ itself exceeds $k_{\lambda_n} + 1$ so that $k_{\lambda_{n+1}} + 1 > k_{\lambda_n} + 1$. These members of \bar{H} therefore constitute an infinite subset of the consequently infinite \bar{H} . Hence, H is hyper-simple.

Clearly, *every hyper-simple set H is simple*. For an infinite recursively enumerable subset of \bar{H} , as set of unit sequences, would contradict H being hyper-simple. Our construction of §6, in view of §8, gives us, however, *a simple set which is not hyper-simple*. Hyper-simple sets thus constitute a third class of recursively enumerable sets with recursively unsolvable decision problems—a class which is a proper subclass of the class of simple sets.

10. Non-reducibility of creative sets to hyper-simple sets by truth-tables unrestricted. Let creative set C be reducible by truth-tables to a recursively enumerable set of positive integers H . The given reduction will again determine for each positive integer n a finite sequence of positive integers m_1, m_2, \dots, m_v , and a truth-table T of order v such that that row of the table which correctly tells of the m 's whether they are, or are not, in H will correctly tell of n whether it is, or is not, in C . Of course v and T as well as the m 's depend on n , and the set of distinct T 's now entering into our reduction may be infinite, and hence the set of distinct v 's unbounded.

Let l_1, l_2, \dots, l_μ be any given finite sequence of distinct positive integers. A particular hypothesis on the l 's being, or not being, in H may then be symbolized by a sequence of μ signs, each + or -, such as $+ - \dots +$, such that the i th sign is +, or -, according as the hypothesis says that l_i is in H , or \bar{H} , respectively. We shall speak of such a sequence of signs as a *truth-assignment* for the l 's, the i th sign in that sequence as the *sign of l_i* in that truth-assignment. Of the 2^μ possible truth-assignments for the l 's, constituting a set V_1 , one and only one correctly tells of each l_i whether it is, or is not, in H . Every set V of truth-assignments for the l 's is then a subset of V_1 , and will be called a *possible set* of truth-assignments if it includes this *correct* truth-assignment.

Let then V be any given possible set of truth-assignments for the l 's. Let n be a positive integer with corresponding m_1, m_2, \dots, m_v, T yielded by the given reduction of C to H such that *each m not an l is in H*. The correct row of table T must then have the following two properties. First, the sign under each m not an l must be +. Second, the signs under those m 's which are l 's must be the same as the signs of those integers in some one and the same truth-assignment for the l 's in V , in fact, as in the correct truth assignment for the l 's. Any row



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

THEOREM. *For any recursively enumerable set of positive integers S , with infinite \bar{S} , there exists a recursively enumerable set of bases defining finite recursively enumerable sets of positive integers, each set having at least one element in \bar{S} , and at least one set having each of its elements greater than an arbitrarily given positive integer n .*

Briefly, with n given, for each positive integer N , and each positive integer m , place all of the integers $n+1, n+2, \dots, n+m$ in a set α_n if all, or all but the last, are among the first N members of a given recursive enumeration of S . It is readily seen that α_n is a generated, and hence recursively enumerable, set of positive integers. A corresponding basis $B^{(n)}$ can actually be found, and the set of $B^{(n)}$'s, $n=1, 2, 3, \dots$, being a generated set, is therefore recursively enumerable. Moreover, if v_n is the smallest integer in the infinite \bar{S} greater than n , α_n will consist of exactly the integers $n+1, n+2, \dots, v_n$, and hence will be finite, with indeed v_n as the only element in \bar{S} , and with each element greater than n .

As a result we are left completely on the fence as to whether there exists a recursively enumerable set of positive integers of absolutely lower degree of unsolvability than the complete set K , or whether, indeed, all recursively enumerable sets of positive integers with recursively unsolvable decision problems are absolutely of the same degree of unsolvability. On the other hand, if this question can be answered, that answer would seem to be not far off, if not in time, then in the number of special results to be gotten on the way.²⁵

Such then is the portion of "Recursive theory" we have thus far developed. In fixing our gaze in the one direction of answering the lower degree of unsolvability question, we have left unanswered many questions that stud even the short path we have traversed. Moreover, both our special, and the general Turing, definitions of reducibility are applicable to arbitrary decision problems whose questions in symbolic form are recursively enumerable, and indeed to problems with recursively enumerable set of questions whose answers belong to a recursively enumerable set. Thus, only partly leaving the field of decisions problems of recursively enumerable sets, work of Turing [26] suggests the question is the problem of determining of an arbitrary basis B whether it generates a finite, or infinite, set of positive

²⁵ This is a matter of practical concern as well as of theoretical interest. For according as the second or first of the above alternatives holds will the method of reducing new decision problems to problems previously proved unsolvable be, or not be, the general method for proving the unsolvability of decision problem either of recursively enumerable sets of positive integers or of problems equivalent thereto.

integers of absolutely higher degree of unsolvability than K . And if so, what is its relationship to that decision problem of absolutely higher degree of unsolvability than K yielded by Turing's theorem.

Actually, the theory of recursive reducibility can be but one chapter in the theory of recursive unsolvability, and that, but one volume of the theory and applications of general recursive functions. Indeed, if general recursive function is the formal equivalent of effective calculability, its formulation may play a rôle in the history of combinatorial mathematics second only to that of the formulation of the concept of natural number.

BIBLIOGRAPHY

1. Alonzo Church, *An unsolvable problem of elementary number theory*, Amer. J. Math. vol. 58 (1936) pp. 345–363.^a
2. ———, *A note on the Entscheidungsproblem*, Journal of Symbolic Logic vol. 1 (1936) pp. 40–41.^a
3. ———, *Correction to a note on the Entscheidungsproblem*, ibid. pp. 101–102.^a
4. ———, *Combinatory logic as a semi-group*, Preliminary report, Bull. Amer. Math. Soc. abstract 43-5-267.
5. ———, *The constructive second number class*, ibid. vol. 44 (1938) pp. 224–232.
6. ———, *The calculi of lambda-conversion*, Annals of Mathematics Studies, no. 6, Princeton University Press, 1941.
7. C. J. Ducasse, *Symbols, signs, and signals*, Journal of Symbolic Logic vol. 4 (1939) pp. 41–52.
8. Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik vol. 38 (1931) pp. 173–198.^a
9. ———, *On undecidable propositions of formal mathematical systems*, mimeographed lecture notes, The Institute for Advanced Study, 1934.^a
10. David Hilbert, *Mathematical problems*. Lecture delivered before the International Congress of Mathematicians at Paris in 1900. English translation by Mary Winston Newsom, Bull. Amer. Math. Soc. vol. 8 (1901–1902) pp. 437–479.
11. David Hilbert and Paul Bernays, *Grundlagen der Mathematik*, vol. 2, Julius Springer, Berlin, 1939.
12. S. C. Kleene, *General recursive functions of natural numbers*, Math. Ann. vol. 112 (1936) pp. 727–742.^a
13. ———, *On notation for ordinal numbers*, Journal of Symbolic Logic vol. 3 (1938) pp. 150–155.
14. ———, *Recursive predicates and quantifiers*, Trans. Amer. Math. Soc. vol. 53 (1943) pp. 41–73.^a
15. C. I. Lewis, *A survey of symbolic logic*, Berkley, 1918, chap. 6, §3.
16. J. C. C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, Journal of Symbolic Logic vol. 8 (1943) pp. 61–76.
17. Rozsa Péter, *Az axiomatikus módszer korlátai* (The bounds of the axiomatic method), Review of, Journal of Symbolic Logic vol. 6 (1941) pp. 111.
18. Emil L. Post, *Finite combinatory processes—formulation 1*, ibid. vol. 1 (1936) pp. 103–105.^a

19. ——, *Formal reductions of the general combinatorial decision problem*, Amer. J. Math. vol. 65 (1943) pp. 197–215.
20. J. B. Rosser, *Extensions of some theorems of Gödel and Church*, Journal of Symbolic Logic vol. 1 (1936) pp. 87–91.^a
21. ——, *An informal exposition of proofs of Gödel's theorems and Church's theorem*, ibid. vol. 4 (1939) pp. 53–60.^a
22. Th. Skolem, *Einfacher beweis der unmöglichkeit eines allgemeinen losungsverfahrens für arithmetische probleme*, Review of, Mathematical Reviews vol. 2 (1941) p. 210.
23. Alfred Tarski, *On undecidable statements in enlarged systems of logic and the concept of truth*, Journal of Symbolic Logic vol. 4 (1939) pp. 105–112.
24. A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. (2) vol. 42 (1937) pp. 230–265. ^a
25. ——, *Computability and λ-definability*, Journal of Symbolic Logic vol. 2 (1937) pp. 153–163.
26. ——, *Systems of logic based on ordinals*, Proc. London Math. Soc. (2) vol. 45 (1939) pp. 161–228. ^a

THE CITY COLLEGE,
NEW YORK CITY.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

6. Closing the circle

Apart from the reduction of *10 *Principia Mathematica* to canonical form *B*, our work has consisted of a series of reductions starting with canonical form *A* and ending with systems in normal form. Using $S_1 \rightarrow S_2$ to symbolize S_1 is reducible to S_2 , our definition of reducibility clearly yields the result, if $S_1 \rightarrow S_2$ and $S_2 \rightarrow S_3$ then $S_1 \rightarrow S_3$. If then we can show that systems in normal form are reducible to canonical form *A*, it will follow that all of our canonical forms from first to last are equivalent, that is, for any two of them any system of either is reducible to some system of the other. Stated otherwise, the solution of the finiteness problem for all systems in one canonical form would yield the solution of the finiteness problem for all systems in the other.⁷⁹

We shall perform our reduction in two stages, first to a certain type of system in canonical form *B*, and then just this type of system to canonical form *A*. Corresponding to the primitive letters a_1, a_2, \dots, a_μ of the given system in normal form, we introduce primitive first order functions $a_1(p), a_2(p), \dots, a_\mu(p)$. We cannot quite let an arbitrary enunciation $a_{i_1} a_{i_2} \dots a_{i_n}$ of the given system correspond to $a_{i_1}(p) a_{i_2}(p) \dots a_{i_n}(p)$ in the sense of a formal product of *n* factors. But corresponding to the way in which an ordinary product of *n* elements is secured by a dyadic operation and associative law thereon, we get the desired effect by introducing a primitive second order function $b(p, q)$. The correspondent of $f = a_{i_1} a_{i_2} \dots a_{i_n}$

the new given sequence of assertions. If the given operation is not the last, retain the given assertion as given assertion, and pass to the next operation as given operation. If the given operation is the last, pass from the given assertion to the next assertion, and to the first operation as given operation.

⁷⁹ This idea of closing the circle of reductions by reducing systems in normal form to canonical form *A* does not explicitly appear in the notes. It, however, was probably considered to be one of those things that could obviously be done. While, as a result, the first of the two stages in which this reduction is carried out is "apocryphal," the second of those two stages merely uses a method which in more general form was used in the notes to reduce the canonical form intermediate between *A* and *B* to *A*. In fact, to somewhere preserve this method is our excuse for introducing this section.

As to *10 being merely attached to this circle, the unpublished note referred to in footnote 18, categorically states that a proof of the reducibility of canonical form *A* to *10 "is nearly completed," and as a result even suggests that the solution of the finiteness problem for *10 would yield the solution of the finiteness problem for all of *Principia Mathematica*. An examination of the notes reveals the reduction to have been carried through in three stages: first the reduction to *10 of mathematical systems using *10 as logic, second the reduction to the latter of what were termed "algebraic systems," third the reduction of systems in canonical form *A* to algebraic systems. It is for the second reduction that one half of the necessary two-way proof was postponed. Not having checked the parts of the proof that were given, we cannot guarantee their correctness. In this connection, see footnote 90.

of the given system will then be

$$b(a_{i_1}(p), b(a_{i_2}(p), \dots, b(a_{i_{n-1}}(p), a_{i_n}(p)) \dots)),$$

which we will symbolize by $f(p)$ for purposes of discussion. Of course, when $n = 1$ we simply have $f(p) = a_{i_1}(p)$.

Corresponding to the above mentioned associative law we introduce the operations

$$b(P, b(Q, R)) \text{ produces } b(b(P, Q), R),$$

$$b(b(P, Q), R) \text{ produces } b(P, b(Q, R)),$$

$$b(b(P, Q), b(R, S)) \text{ produces } b(P, b(b(Q, R), S)),$$

which have the effect of enabling us to pass from any mode of inserting b -parentheses in the sequence $a_{i_1}(p), a_{i_2}(p), \dots, a_{i_n}(p)$ to any other mode. All of the resulting forms may then be considered correspondents of f , with $f(p)$ the principal correspondent.

If h symbolizes the one primitive assertion of the given system, our new system will have the primitive assertion $h(p)$. The operations " $g_i P$ produces $P g_i'$ " will be suitably taken care of if we allow for the passage from some correspondent of the hypothesis to some correspondent of the conclusion. Note that for g_i, g_i', P not null, a correspondent of $g_i P$ will be in the form $b(g_i(p), Q)$, of $P g_i'$, $b(Q, g_i'(p))$. We then correspondingly introduce the operation

$$b(g_i(P), Q) \text{ produces } b(Q, g_i'(P)).$$

In fact, since the primitive assertion of the new system involves but the one variable p , all assertions of the system may be considered to be written on the one variable p , since the operation of substitution of canonical form B will merely reproduce these assertions on other variables. In the application of the last given operation, P , in fact, will only be identifiable with that variable p .

To allow for P null in the operation of the given system, the separate operation

$$g_i(P) \text{ produces } g_i'(P)$$

must be added. If either g_i or g_i' is null, we may clearly assume the other not null, while P then certainly can't be null, since the null assertion has been specifically excluded from our systems. When g_i' is null we then need but the one operation

$$b(g_i(P), Q) \text{ produces } Q.$$

When g_i is null we must explicitly insure our conclusion being written on but a single variable. For P of more than one letter, we may write $P = a_j P'$, $j = 1, 2, \dots, \mu$ and correspondingly set up the μ operations

$$b(a_j(P), Q) \text{ produces } b(b(a_j(P), Q), g_i'(P)).$$

For P of one letter we likewise have

$$a_j(P) \text{ produces } b(a_j(P), g_i'(P)), \quad j = 1, 2, \dots, \mu.$$

This completely takes care of the first reduction.

For the second reduction introduce a new primitive first order function $k(p)$ and alter the preceding system as follows. Replace the primitive assertion $h(p)$ by $h(k(p))$, retain the preceding productions, and change the operation of substitution to that of canonical form A . Now it is readily proved by induction that every assertion of the resulting system will be of the form $F(k(P))$ where $F(p)$ does not involve the primitive function k . Furthermore, if $F(k(P)) = F'(k(P'))$, with $F(p)$ and $F'(p)$ not involving k , we see by successively stripping away necessarily identical outmost primitive functions that $F = F'$, $P = P'$, i.e., that such a form is unique.⁸⁰ Again by induction, if $F_1(k(P_1)), F_2(k(P_2)), \dots, F_n(k(P_n))$ are the successive assertions in an arbitrary proof of our system, we find that P_i is either identical with P_{i-1} , or obtainable from it by a substitution. It follows that the only assertions of our system of the form $F(k(p))$ are obtained by deductive processes in which no other substitutions are employed than that of variable for variable. But with substitution thus limited, the new system is simply isomorphic with the old under the replacement $p \leftrightarrow k(p)$, p an arbitrary variable for completeness. It follows that an enunciation $F(p)$ of the previous system is an assertion thereof when and only when $F(k(p))$ is an assertion of the new system, whence our second reduction.

For our original system we then have that $a_{i_1} a_{i_2} \dots a_{i_n}$ is an assertion thereof when and only when

$$b(a_{i_1}(k(p)), b(a_{i_2}(k(p)), \dots b(a_{i_{n-1}}(k(p)), a_{i_n}(k(p))) \dots))$$

is an assertion in the system in canonical form A , as desired.

We have observed in §3 how the seemingly simple problem of “tag” in fact proved intractable for $\mu = 2, \nu > 2$, of bewildering complexity for $\mu > 2, \nu = 2$. In view of our reduction of canonical form A to a form as close to that of “tag” as the normal form, the difficulty of “tag” is no longer surprising.⁸¹ While this suggested that special cases of “tag” might well be worth consideration as major problems in themselves, the following further reduction of the normal form seemed more promising.

We merely state the result. Given any system in normal form on letters a_1, a_2, \dots, a_μ , its assertions will be the assertions, on those letters,

⁸⁰ This is a special aspect of the L.C.M. process referred to early in §3.

⁸¹ In fact, at one point late in the work on “tag,” it seemed that the regularity induced by always removing μ elements from the beginning of a sequence was responsible for the intrusion of number theory in the development, so that it was tentatively suggested that “tag” be generalized to a form which, indeed, is exactly that of the later derived normal form.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.



You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

Index

- absolute definition, 83, 84
- absolutely unsolvable problems, [289](#)
- Ackerman, Wilhelm, 110, 145, 269
- algorithmic theories, 272, [280](#)
- apparent variables, 350
- arithmetic predicates, [254](#)
- arithmetical relations, 29, 30
- arithmetization, [236](#); see also Gödel numbering
- assertions, 339, 345
- axioms of infinity, [74](#), 85

- Baire, R., 264
- Bergson, Henri, 394, 396, 405
- Bernays, Paul, [73](#), [112](#), [143](#), 253
- Borel, E., 264
- Brouwer, L. E. J., 154, 399

- canonical form *A*, 338, 344, 347, 348, 361, [380](#), [382](#), 383
- canonical form *B*, 338, 344, 347, 348, 349, 350, 363, 365, [380](#), 383, 384
- canonical form *C*, 338, 363, 364, 365, 369, 370, 373, 376, 384
- canonical systems, 338
- Cantor, G., 291, 398
- Cantor's diagonal method, 84, 132, 262, 249, 262, 272, 291
- Chinese remainder theorem, [31](#)
- Church, Alonzo, 108, 117, 149, 156, 159, 160, [161](#), 174, [191](#), 219, [230](#), [255](#), 269, 274, [288](#), [289](#), 291, 293, [305](#), [310](#), 312, 338, 340, 343
- Church's theorem, 223, 255, 275, 278
- Church's thesis, 39, 40, 88, 274, 338
- circle-free machines, see Turing machines
- complete algorithmic theory, 273, 275
- complete formal deductive theory, 42, 276
- complete normal system, 390
- complete set, 313
- completeness, 170

computability, 84, 117, 173, 299, 342; see also Turing machines
computable convergence, 142
computable function, 82, 160, 161
computable numbers, 116, 135, 139, 303
computable sequences, 125
computing machines, 117; see also Turing machines
consistency, 268; see also ω -consistency
consistency proof, 35-38, 80
constructive existence proofs, 283
constructive ordinals, 155
continuum hypothesis, 86, 207, 208
convention machines, see Turing machines
creative process, 398
creative set, 316, 317
Curry, H. B., 278, 280

Davis, Martin, 73
decision problem, 308
deducibility problem, 115
definability, 84
 in terms of ordinals, 86
degree of unsolvability, 310, 311, 326
Dekker, J. C. E., 287
demonstrability, 84
diagonal procedure, see Cantor's diagonal method
Diophantine equations, 65, 83, 309

effective calculability, 89, 90, 100, 110, 149, 160, 274, 275, 291,
 305
elementary predicates, 264, 285; see also arithmetic predicates,
 arithmetic relations
engere Funktionenkalkül, 108, 109, 110, 114, 115
Entscheidungsproblem, 108, 109, 110, 112, 114, 117, 145, 152
enumeration theorem, 260
enunciations, 339, 345
Epimenides paradox, 63, 64, 230, 278

Fermat's theorem, last, 165, 207, 395
finite procedure, 39
finiteness problem, 339, 345, 346, 349, 384, 385, 386, 395
first order functional calculus, see engere Funktionenkalkül
formal deductive theories, 275, 280
formalism, 85
formal logic, 209
formal mathematical system, 39, 41
Friedberg, R., 304
functional expressions, 47

general recursiveness, 84, 160, 163, 231, 258, 342
 general recursive functions, 40, 69, 232, 237, 255, 257, 264, 305
 general recursive predicate, 261
 see also recursive functions
generated set, 307, 342
Gentzen, G., 210, 211, 219
Gill, B. P., 361
Gödel, Kurt, 4, 39, 40, 93, 109, 116, 145, 155, 159, 160, 163, 171, 187, 191, 209, 226, 227, 229, 231, 233, 236, 237, 238, 240, 242, 250, 255, 257, 264, 270, 277, 291, 298, 305, 338, 340, 343
Gödel numbering, 13, 93, 94, 96, 103, 104, 105, 160, 244, 249, 252, 271, 272, 276
Gödel's completeness theorem, 108
Gödel's incompleteness theorem, 154, 192, 194, 223, 224, 230, 254, 255, 278, 279, 289, 304, 310, 313
Gödel's theorem, second, 223, 224, 225, 228

Herbrand, Jacques, 40, 75, 76, 77, 78, 79, 80, 160, 163, 229, 237, 240, 255, 257, 264, 305
Heyting, Arend, 75, 77, 79
Hilbert, David, 73, 80, 108, 110, 135, 138, 143, 145, 191, 269, 308, 309, 310
Hilbert's program, 73
Hilbert's problem, tenth, 308
hyper-simple sets, 326, 327, 331

THE UNDECIDABLE

Basic Papers on Undecidable Propositions, Unsolvable Problems
and Computable Functions

Edited by Martin Davis

"A valuable collection both for original source material as well as historical formulations of current problems."

—*The Review of Metaphysics*

"Much more than a mere collection of papers . . . a valuable addition to the literature." —*Mathematics of Computation*

An anthology of fundamental papers on undecidability and unsolvability by major figures in the field, this classic reference is ideally suited as a text for graduate and undergraduate courses in logic, philosophy, and foundations of mathematics. It is also appropriate for self-study.

The text opens with Gödel's landmark 1931 paper demonstrating that systems of logic cannot admit proofs of all true assertions of arithmetic. Subsequent papers by Gödel, Church, Turing, and Post single out the class of recursive functions as computable by finite algorithms. Additional papers by Church, Turing, and Post cover unsolvable problems from the theory of abstract computing machines, mathematical logic, and algebra, and material by Kleene and Post includes initiation of the classification theory of unsolvable problems.

Supplementary items include corrections, emendations, and added commentaries by Gödel, Church, and Kleene for this volume's original publication, along with a helpful commentary by the editor.

Dover (2004) slightly corrected republication of the edition published by Raven Press Books, Ltd., Hewlett, New York, 1965. 416pp. 6 1/2 x 9 1/2. Paperbound.

ALSO AVAILABLE

WHAT IS MATHEMATICAL LOGIC?, J. N. Crossley et al. 82pp. 5 1/2 x 8 1/2. 26404-1

ON FORMALLY UNDECIDABLE PROPOSITIONS OF PRINCIPIA MATHEMATICA AND RELATED SYSTEMS, Kurt Gödel. 80pp. 5 1/2 x 8 1/2. 66980-7

MATHEMATICAL LOGIC, Stephen Cole Kleene. 416pp. 5 1/2 x 8 1/2. 42533-9

For current price information write to Dover Publications, or log on to www.doverpublications.com—and see every Dover book in print.

Free Dover Mathematics and Science Catalog (59065-8) available upon request.

ISBN 0-486-43228-9

UPC



8 00759 43228 8

\$24.95 IN USA
\$37.50 IN CANADA

EAN



9 780486 43228 1