THEORY OF PROVABLE RECURSIVE FUNCTIONS

BY
PATRICK C. FISCHER(1)

1. **Introduction.** The theory of effective computability, which has developed over the past thirty years, concerns two basic classes of binary relations: the *partial recursive functions* (p.r.f.'s) and the *recursive functions*, those p.r.f.'s which are totally defined. Regardless of the particular method of formalization used, the same relations turn out to be p.r.f.'s, and the same total functions turn out to be recursive functions.

One property of the partial recursive functions is that they can be indexed in an effective manner, i.e., one can establish a one-one correspondence between the non-negative integers and instructions for computing p.r.f.'s such that, given an index, one can effectively produce the corresponding instructions for computing the p.r.f. and, given a set of instructions, one can effectively find its index. The class of recursive functions cannot be so indexed; this is one of the basic theorems of recursive function theory.

One might feel that there would be a more constructive aspect to a class of effectively computable total functions which could be indexed in a suitable manner. One subclass of the recursive functions which can be suitably indexed is the class of partial recursive functions which can be proved to be total in a given axiomatic system S(2).

Such functions will be called *provable recursive functions*. Since the theorems of S can be effectively enumerated, one can effectively establish a one-one correspondence between appropriate instructions for computing provable recursive functions and the non-negative integers.

This paper will be concerned with the relationship of the provable recursive functions to the recursive functions. A theory of provable functions, analogous to the theory of recursive functions will be developed with particular emphasis on

Presented to the Society, April 19, 1962, under the title of *Some basic properties of provable recursive functions*, October 27, 1962, under the title of *Proof indices and recursion properties of provable recursive functions*, January 24, 1963, under the title of *Elementary properties of provably recursive sets*, and under the title of *Provably productive and provably creative sets*; received by the editors June 13, 1963.

(1) The results in this paper are contained in a doctoral thesis presented to the Department of Mathematics, Massachusetts Institute of Technology, in 1962 and were obtained while the author held a National Science Foundation Graduate Fellowship.

(2) The class will not necessarily be a subclass of the recursive functions unless S is sound.

the similarities and differences between the new theory and recursive function theory. Suitable analogues for the various concepts of recursive function theory will be exhibited when they exist.

The notion of a p.r.f. which can be proved to be total in Peano arithmetic was considered by Kreisel in 1952 [9]. In 1958, Kreisel showed [10] that the same class of functions can be proved to be total in the intuitionistic arithmetic of Heyting.

In 1956, Rogers considered partial recursive functions which could be proved to be total in a system S, which was permitted to be stronger than Peano arithmetic. He also considered functions which could be proved in S to be one-one recursive functions and functions which could be proved in S to be permutations. These concepts were used in [2] and [3] to obtain several results concerning the degrees of unsolvability associated with reduction of one set to another by functions in each of the three classes, i.e., the p-many-one degrees, the p-one-one-degrees, and the p-isomorphism types.

In 1960, Kent developed a theory of provable permutations and went on to analyze the algebraic structure of the provable permutations considered as a group. As did Rogers, Kent allowed the system S to be stronger than Peano arithmetic. The reader is refered to pp. 61–69 of Kent [1] for additional background material concerning provable functions.

The approach of this paper will be general both in specification of the system S and in development of several areas of theory relating to provable functions. We shall not specify a particular theory S but shall require that it contain properly a conventional axiomatization of elementary number theory (ENT) such as that of Kleene [7, p. 82] and enough of the power of axiomatic set theory to enable formalization of straightforward mathematical argument(3).

Some of the theorems below will contain as part of the hypothesis the statement that S is sound for ENT, i.e., that there is no formula F which is a theorem of S and which is false under the standard interpretation of ENT. By the incompleteness theorem of Gödel, the soundness of S for ENT cannot itself be a theorem of S since it implies the consistency of S. However, if S is strong enough, the theorems with soundness as a hypothesis can still be formulated within S and will be theorems of S as distinguished from theorems about S. Soundness usually is necessary as an additional hypothesis when one uses in a proof a statement of the form "all provable functions are recursive functions."

The treatment of the theory will be informal. We adopt here the viewpoint of Post that the real mathematical content of many results in the theory of recursive functions is contained in informal proofs of the results, and although such

(3) By *elementary number theory* we mean here the theory of number-theoretic predicates expressible in the first-order predicate calculus. Thus, Peano arithmetic (e.g., $Z\mu$ of Hilbert and Bernays) is an axiomatization of ENT but is not itself ENT.

results would be meaningless if they could not be translated into some formal mathematical system, the required translation is a routine, albeit sometimes lengthy, exercise. We thus employ Church's thesis, which states that any function which is intuitively effectively calculable is a recursive function.

The author believes that there should exist no serious difficulties in formalizing this work within Peano arithmetic. Much of the task would merely be adaptation of results of Kreisel [9]. Many of the results in this paper have been formalized within Peano arithmetic by David Ballard.

Since one can prove in set theory that Peano arithmetic is sound for *ENT*, the occurrences of soundness in the hypotheses of some of the theorems could be eliminated when S is Peano arithmetic. The theorems, of course, would then no longer be theorems of S, but would instead be theorems of a more powerful system.

The author is indebted to Hartley Rogers, Jr. for his advice and encouragement and to the referee for his comments and suggestions.

2. Notation.

2.1. *The formal system S.*

Propositional connectives: $\wedge$ (and); $\vee$ (or); $\sim$ (not); $\rightarrow$ (implies).

Quantifiers: $\exists$ (there exists); $\forall$ (for all).

Predicate symbols: $=$ (equals); $\in$ (belongs to).

Function symbols: $+$ (plus); $\cdot$ (times); **s** (successor).

Individual constant: **0**.

Individual variables: u, v, w, x, y, z, with or without numerical subscripts.

In addition, we use parentheses and brackets (,), [,], and define the relation $<$ in terms of $+$ and $=$. We also introduce the symbols **1** for **s(0)**, **2** for **s(s(0))**, **3** for **s(s(s(0)))**, etc. In general, **n** will stand for **s(s(**$\cdots$ **s(0)**$\cdots$**))**, where there are n applications of the successor function.

The above is a minimal description of S. If S is chosen as a relatively strong system, more structure would be used than that explicitly mentioned above.

2.2. *Informal notation.*

Informal variables: u, v, w, x, y, z, with or without numerical subscripts.

Recursive functions (including provable functions and sometimes including primitive recursive functions): $f, g, h, \cdots$.

Partial recursive functions: $\Delta, \theta, \Phi, \cdots$.

Primitive recursive functions: $\alpha, \beta, \gamma, \eta, \psi$.

Sets of non-negative integers: $A, B, C, \cdots$.

Complement of a set A: $\bar{A}$ $(= N - A)$.

Set-theoretic connectives: $\cup$, $\cap$, $\subset$, $\not\subset$, $\in, \notin$.

Characteristic function of a set A: $C_A(x)$, where

$$C_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

$f[A]$: $\{f(x) \mid x \in A\}$.
$f^{-1}[A]$: $\{x \mid f(x) \in A\}$.
$f \to B$: "B is the range of f."
$\mu z[\cdots]$: "the least z such that $\cdots$."
$\equiv$: "if and only if."
$\vdash_S A$: "A is a theorem of S."

The function symbols and predicate symbols of the formal system will also be used as informal symbols. There should be no difficulty in determining the intended use of such symbols as the context will also contain symbols (e.g., variables and constants) which are distinguishable as formal or informal notations.

2.3. *Other notation.*

$\phi_0, \phi_1, \phi_2, \cdots$: the partial recursive functions with Gödel numbers $0, 1, 2, \cdots$, respectively.

$W_0, W_1, W_2, \cdots$: the ranges of the partial recursive functions $\phi_0, \phi_1, \phi_2, \cdots$.

N: the set of all non-negative integers.

$\varnothing$: the empty set.

K: $\{x \mid x \in W_x\}$.

τ, π_1, π_2: primitive recursive functions giving a standard effective one-one correspondence between $N \times N$ and N and satisfying the relationships $\tau(\pi_1(z), \pi_2(z)) = z$; $\pi_1(\tau(x, y)) = x$; $\pi_2(\tau(x, y)) = y$ (cf. functions J, K, L in Davis [6, p. 45]).

It is possible to formalize the intuitive notion of *computational step.* In the Turing formalism (cf. [6]), the number of steps can be just the number of successive instantaneous descriptions in a terminal computation; in Kleene's system [7], it can be the number of lines in the shortest deduction of an end equation. Having chosen an appropriate formalization, let $M(e, x, y, n)$ hold if and only if the eth partial recursive function applied to input x gives output y in not more than n steps. A predicate of Peano arithmetic M(e, x, y, n) which numeral-wise expresses M in S can readily be defined in terms of the T-predicate of Kleene and M can be shown to be primitive recursive.

3. **Definitions.** We proceed to make the following definitions.

DEFINITION 3.1. A partial recursive function $f(x)$ will be called a *provable function* (p-function) if there is some Gödel number e of $f(x)$ such that $\vdash_S \mathbf{P}_1(\mathbf{e})$, where

$$\mathbf{P}_1(\mathrm{w}) \equiv (\forall \mathrm{x})(\exists \mathrm{y})(\exists \mathrm{n})\,\mathbf{M}(\mathrm{w}, \mathrm{x}, \mathrm{y}, \mathrm{n}).$$

DEFINITION 3.2. A p.r.f. $f(x)$ will be called a *provably-one-one* (p-1-1) *p-function* if there is some Gödel number e of $f(x)$ such that $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_2(\mathbf{e})$, where

$$\mathbf{P}_2(\mathrm{w}) \equiv (\forall \mathrm{x}_1)(\forall \mathrm{x}_2)(\forall \mathrm{y}_1)(\forall \mathrm{y}_2)[[(\exists \mathrm{n})\mathbf{M}(\mathrm{w}, \mathrm{x}_1, \mathrm{y}_1, \mathrm{n}) \wedge (\exists \mathrm{n})\mathbf{M}(\mathrm{w}, \mathrm{x}_2, \mathrm{y}_2, \mathrm{n}) \wedge \mathrm{x}_1 \neq \mathrm{x}_2] \to \mathrm{y}_1 \neq \mathrm{y}_2].$$

DEFINITION 3.3. A p.r.f. $f(x)$ will be called a *provably-increasing* (p-increasing) *p-function* if there is some Gödel number e of $f(x)$ such that $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_3(\mathbf{e})$, where

$$\mathbf{P}_3(w) \equiv (\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)[[(\exists n)\mathbf{M}(w, x_1, y_1, n) \wedge (\exists n)\mathbf{M}(w, x_2, y_2, n) \wedge x_1 < x_2] \rightarrow y_1 < y_2].$$

DEFINITION 3.4. A p.r.f. $f(x)$ will be called a *provably-nondecreasing* (p-nondecreasing) *p-function* if there is some Gödel number e of $f(x)$ such tha $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_4(\mathbf{e})$, where

$$\mathbf{P}_4(w) \equiv (\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)[[(\exists n)\mathbf{M}(w, x_1, y_1, n) \wedge (\exists n)\mathbf{M}(w, x_2, y_2, n) \wedge x_1 \leqq x_2] \rightarrow y_1 \leqq y_2].$$

DEFINITION 3.5. A p.r.f. $f(x)$ will be called a *provably-onto* (p-onto) *p-function* if there is a Gödel number e of $f(x)$ such that $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_5(\mathbf{e})$, where

$$\mathbf{P}_5(w) \equiv (\forall y)(\exists x)(\exists n)\mathbf{M}(w, x, y, n).$$

DEFINITION 3.6. A p.r.f. $f(x)$ will be called a *provably-infinite* (p-infinite) *p-function* if there is a Gödel number e of $f(x)$ such that $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_6(\mathbf{e})$, where

$$\mathbf{P}_6(w) \equiv (\forall x)(\exists y)(\exists z)(\exists n)[(y > x \wedge \mathbf{M}(w, z, y, n)].$$

DEFINITION 3.7. A p.r.f. $f(x)$ will be called a *provable permutation* (p-permutation) if there is a Gödel number e of $f(x)$ such that $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_2(\mathbf{e}) \wedge \mathbf{P}_5(\mathbf{e})$.

Clearly, by Church's thesis, the set T_1 of Gödel numbers (of partial recursive functions) satisfying the requirement of Definition 3.1 is a recursively enumerable set since the theorems of S can be effectively enumerated. Thus there are primitive recursive functions which enumerate this set (with repetitions allowed) and we will choose one of these and denote it by $\Psi(x)$. (This gives an effective listing of the provable functions: $\phi_{\Psi(0)}, \phi_{\Psi(1)}, \phi_{\Psi(2)}, \cdots$.)

In a similar manner we can define sets T_2 through T_7 to be sets of Gödel numbers satisfying Definitions 3.2 through 3.7, respectively, and can choose primitive recursive functions $\Psi_2(x)$ through $\Psi_7(x)$, respectively, to enumerate these sets. Thus, we have the following primitive recursive enumerating functions:

$\Psi_2(x)$: for provably-one-one provable functions.
$\Psi_3(x)$: for provably-increasing provable functions.
$\Psi_4(x)$: for provably-nondecreasing provable functions.
$\Psi_5(x)$: for provably-onto provable functions.
$\Psi_6(x)$: for provably-infinite provable functions.
$\Psi_7(x)$: for provable permutations.

4. Elementary properties of provable functions. In this section we state some elementary properties of p-functions, the proofs of which are mostly trivial in

S and, in the event S is Peano arithmetic, consequences of results of Kreisel [9, Vol. 17, pp. 43–49].

PROPERTY 4.1. *If $f_1(x), f_2(x), \cdots, f_k(x)$ are p-functions and $g(x)$ is primitive recursive in $f_1, f_2, \cdots, f_k$, then $g(x)$ is a p-function.*

PROPERTY 4.2. *If $f(x)$ and $g(x)$ are both p-functions, then their composition $h(x) = f(g(x))$ is a p-function.*

PROPERTY 4.3. *If $g(x, y)$ and $h(z)$ are p-functions, e is a Gödel number for h and if*

$$\vdash_S (\forall x)(\exists y)[y > x \wedge (\exists n)\mathbf{M}(\mathbf{e}, y, \mathbf{1}, n)]$$

then if $f(x)$ is defined as follows:

$$f(0) = \mu z[h(z) = 1],$$

$$f(x) = \mu z[z > g(x, f(x-1)) \wedge h(z) = 1],$$

then $f(x)$ is a p-function.

PROPERTY 4.4. *If $f(x)$ is a p-permutation (p-onto p-function, p-1-1 p-function, then the function $f'(x)$ defined by:*

$$f'(x) = \mu z[f(z) = x]$$

is a p-permutation (p-1-1 p-function, p-1-1 p-onto p.r.f.)([4]).

Thus the p-permutations form a group (cf. [1], [3]).

PROPERTY 4.5. *If $f(x)$ is a p-increasing p-function, then $f(x)$ is a p-1-1 p-function; if $f(x)$ is a p-1-1 p-function, then $f(x)$ is a p-infinite p-function.*

5. **Properties of provable functions.** Before investigating some of the relationships among the properties of functions contained in Definitions 3.1–3.7, it will be shown that for each of the definitions in §3, there are recursive functions satisfying the antecedent of the definition but not satisfying the provability requirement. The proofs all proceed via diagonal methods.

THEOREM 5.1. *If S is sound for ENT, then there is a recursive function $f(x)$ which is not a p-function.*

Proof. Let $f(x) = \phi_{\Psi(x)}(x) + 1$. If S is sound, then clearly, from Definition 3.1, all members of T_1 are Gödel numbers of recursive functions. Thus, $f(x)$ is totally defined and is a recursive function. However, if $f(x)$ were a p-function, then there would exist some number n such that $f(x) = \phi_{\Psi(n)}(x)$. But then

$$f(n) = \phi_{\Psi(n)}(n) = \phi_{\Psi(n)}(n) + 1,$$

a contradiction.

(4) ϕ_e is a p-1-1 p-onto p.r.f. if $\vdash_S \mathbf{P}_2(\mathbf{e}) \wedge \mathbf{P}_5(\mathbf{e})$.

The above proof yields an "incompleteness theorem" for p-functions, since if we could prove in S that $\phi_{\Psi(x)}(x)$ is defined for all x, then we could prove, using the defining equations for f, that $f(x)$ is totally defined. But then $f(x)$ could be shown to be a p-function, which is impossible from above. Thus we have:

COROLLARY 5.2. *If S is sound for ENT, then the formula*

$$(\forall x)(\exists y)(\exists n)\,M(\Psi(x),x,y,n)$$

is not a theorem of S.

The incompleteness is actually ω-incompleteness since for each x:

$$\vdash_S (\exists y)(\exists n)\,M(\Psi(x),x,y,n).$$

Theorem 5.1 and parts (i) and (vi) of Theorem 5.4 below were proved by Rogers [3, p. 92] in a different manner in 1956. It is observed there that the class of all recursive functions is not recursively enumerable in the following sense:

DEFINITION 5.3. A class $\mathscr{C}$ of partial recursive functions is called a *recursively enumerable class* if there is a recursively enumerable set A such that

$$\phi \in \mathscr{C} \equiv (\exists x)[\phi = \phi_x \wedge x \in A].$$

Since the p-functions are a recursively enumerable class (where the set A is the range of $\Psi(x)$), and since (by soundness of S) all p-functions are recursive functions, there must exist at least one recursive function which is not a p-function. Similar arguments apply to p-1-1 functions and to p-permutations.

THEOREM 5.4. *If S is sound for ENT, then:*

(i) *There is a one-one recursive function $f_2(x)$ which is not a p-1-1 p-function.*

(ii) *There is an increasing recursive function $f_3(x)$ which is not a p-increasing p-function.*

(iii) *There is a nondecreasing recursive function $f_4(x)$ which is not a p-nondecreasing p-function.*

(iv) *There is a recursive function $f_5(x)$ such that $f_5 \to N$, which is not a p-onto p-function.*

(v) *There is a recursive function $f_6(x)$ with infinite range which is not a p-infinite p-function.*

(vi) *There is a recursive permutation $f_7(x)$ which is not a p-permutation.*

Proof. For $k = 2,3,4$, we define $f_k(x)$ as follows:

$$f_k(0) = \mu z\,[z \neq \phi_{\Psi_k(0)}(0)],$$

$$f_k(x) = \mu z\,[z \neq \phi_{\Psi_k(x)}(x) \wedge z > f(x-1)].$$

The soundness of S implies that $\phi_{\Psi_k(x)}$ is totally defined for all x. This fact plus an analysis of the informal defining equations for f_k shows that f_k is recursive

and strictly increasing. However, f_k cannot be the appropriate kind of p-function, else for some number n we would have $f_k(x) = \phi_{\Psi_k(n)}(x)$, which would lead to a contradiction as in Theorem 5.1.

For k= 5, 6, 7, we define f_k as follows:

$$f_k(0) = \mu z\,[z \neq \phi_{\Psi_k(0)}(x)],$$

$$f_k(x) = \mu z\,[z \text{ is different from } f_k(0), f_k(1), \cdots, f_k(x-1); \text{ and if } x \text{ is even, } z \neq \phi_{\Psi_k(x/2)}(x)].$$

An argument paralleling that above shows that f_k is a one-one recursive function. Also, every $n \in N$ appears in the range of f_k and, in fact, we will have $n = f_k(m)$ for some $m \leqq 2n$ since the smallest number not already in the range of f_k is included each time f_k is applied to an even number. Since f_k is one-one and onto, it is a recursive permutation, but f_k differs from each $\phi_{\Psi_k(x)}$ in at least one point.

Theorem 5.4 could have been proved by using $\Psi(x)$ in each of the above constructions since Definitions 3.2–3.7 all contain as a requirement that the function under consideration be a p-function. Since the diagonalizations with $\Psi(x)$ would yield functions which had the desired properties but which were not p-functions, the functions in question could not then be p-1-1 p-functions, p-onto p-functions, etc. This raises the question: Is the possibility of proving that a partial recursive function is total independent of the possibility of proving, say, that the same p.r.f. is one-one, or do relations exist between the two possibilities? Also, what happens if proofs of "ontoness" and "functionhood" are given for different Gödel numbers of the same p.r.f.? These questions will be discussed in the remainder of this section and in §6.

The first question we deal with is whether there are p-functions which are one-one but not p-1-1 p-functions, p-functions which are onto but not p-onto p-functions, etc. This question is answered below by Theorems 5.5 and 5.6.

THEOREM 5.5. *Let $f(x)$ be a p-function.*

(i) *If f is one-one, then f is a* p-1-1 *p-function.*

(ii) *If f is increasing, then f is a p-increasing p-function.*

(iii) *If f is nondecreasing, then f is a p-nondecreasing p-function.*

Proof. Let e be a Gödel number of $f(x)$ such that $\vdash_S \mathrm{P}_1(\mathbf{e})$.

(i) We define a function $g(x)$ as follows:

$$g(0) = \phi_e(0),$$

$$g(x) = \begin{cases} \phi_e(x), \text{ if } \phi_e(x) \text{ is different from } g(0), g(1), \cdots, g(x-1); \\ \mu z[z \text{ is different from } g(0), g(1), \cdots, g(x-1)], \text{ otherwise.} \end{cases}$$

The Gödel number e' for $g(x)$ depends effectively upon the Gödel number e used for computing $f(x)$. From the form of the instructions for g it is clear that,

since $\vdash_S P_1(\mathbf{e}), P_1(\mathbf{e}')$ can be derived in S via elementary quantificational methods. Also, the instructions for $g(x)$ force it to be one-one and this fact is easily provable in S. Therefore, we have $\vdash_S P_1(\mathbf{e}') \wedge P_2(\mathbf{e}')$, and $g(x)$ is a p-1-1 p-function. Now, we observe that if $f(x)$ is one-one that the second clause in the definition of $g(x)$ will never operate and g will be the same function as f. But then e' will be a Gödel number of f and $f(x)$ will be a p-1-1 p-function.

(ii) We define $g(x)$ as follows:

$$g(0) = \phi_e(0),$$

$$g(x) = \begin{cases} \phi_e(x) & \text{if } \phi_e(x) > g(x-1), \\ g(x-1)+1 & \text{otherwise.} \end{cases}$$

The argument proceeds as before.

(iii) We define $g(x)$ as follows:

$$g(0) = \phi_e(0),$$

$$g(x) = \begin{cases} \phi_e(x) & \text{if } \phi_e(x) \geqq g(x-1), \\ g(x-1) & \text{otherwise.} \end{cases}$$

Again the argument proceeds as in (i).

Thus a p-function cannot be one-one without being a p-1-1 function, similarly for increasing and nondecreasing p-functions.

THEOREM 5.6. *If S is sound for ENT, then*:

(i) *There is a p-function which is a recursive permutation (and thus a p-1-1 p-function, by Theorem 5.5) but not a p-permutation.*

(ii) *There is a p-function with range N which is not a p-onto p-function.*

(iii) *There is a p-function which has infinite range but which is not a p-infinite p-function.*

Proof. (i) This result is originally due to Kreisel [11]. A direct proof appears in Kent [1, pp. 73–76]. We will assume, for the moment, that we can construct an infinite recursive set B, the characteristic function C_B of which is a p-function, such that B cannot be proved to be infinite within S. (See definitions 8.1 and 8.2.) This assumption will be proved as Corollary 8.8. We define $f(x)$ as follows:

$$f(x) = \begin{cases} x+1 & \text{if } C_B(x) = 0, \\ \mu z\,[z \text{ is different from } f(0), f(1), \cdots, f(x-1)], & \\ & \text{if } C_B(x) \neq 0. \end{cases}$$

From the definition of $f(x)$ we can see that, if the members of B, in increasing order, are $b_0, b_1, b_2, \cdots$, then f has the following cycle structure:

$$f = (0, 1, 2, \cdots, b_0)(b_0 + 1, b_0 + 2, \cdots, b_1) \cdots (b_k + 1, b_k + 2, \cdots, b_{k+1}) \cdots .$$

From the definition of $f(x)$ and the fact that $C_B(x)$ is a p-function it is clear that f is a p-1-1 p-function. Furthermore, it is easy to show *in* S that B is an infinite set if and only if f is a permutation. Since B is infinite we know that f is a permutation. However, if f were a p-permutation, then B would be p-infinite, contradicting the assumed construction.

(ii) The p-function f above clearly has range N. If e is a Gödel number of f, then from (i) we have $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_2(\mathbf{e})$ but not $\vdash_S \mathbf{P}_1(\mathbf{e}) \wedge \mathbf{P}_2(\mathbf{e}) \wedge \mathbf{P}_5(\mathbf{e})$. Thus we have not $\vdash_S \mathbf{P}_5(\mathbf{e})$ and f is not p-onto.

(iii) Let

$$f'(x) = \begin{cases} 0 & \text{if } C_B(x) = 0, \\ x & \text{if } C_B(x) \neq 0. \end{cases}$$

Clearly $f'(x)$ is a p-function with infinite range. Furthermore, it is trivial in S that $f'(x)$ will have infinite range if and only if B is infinite. Therefore f' cannot be a p-infinite p-function.

If we modify Definitions 3.2 through 3.7 by deleting the requirement $\mathbf{P}_1(\mathbf{e})$ from the expression in each of the definitions, we obtain the notions of a *p-1-1 partial recursive function*, a *p-increasing p.r.f.*, a *p-nondecreasing p.r.f.*, a *p-onto p.r.f.*, a *p-infinite p.r.f.*, and a *p-1-1, p-onto p.r.f.* We can then note the existence of primitive recursive functions $\Psi'_2(x)$ through $\Psi_5(x)$, respectively, which enumerate the above classes of partial recursive functions.

Although a p-1-1 p.r.f. may not be totally defined, it will be one-one over its domain (if S is sound for ENT). Similar properties hold for the other notions above.

The following two corollaries show that the results of Theorems 5.5 and 5.6 hold for partial recursive functions as well as for p-functions.

COROLLARY 5.7. (i) *If $\theta(x)$ is a one-one p.r.f., then θ is a p-1-1 p.r.f.*
(ii) *If $\theta(x)$ is an increasing p.r.f., then θ is a p-increasing p.r.f.*
(iii) *If $\theta(x)$ is a nondecreasing p.r.f., then θ is a p-nondecreasing p.r.f.*

Proof. We sketch the proof, using the general method of Theorem 5.5. If e is a Gödel number of θ, we define a p.r.f. $\Delta(x)$ which will diverge whenever $\theta(x)$ does. In addition, if $\theta(x)$ converges in such a manner that $\Delta(x)$ would not be one-one (or increasing, or nondecreasing, as the case may be), $\Delta(x)$ will also diverge at that particular point. The last part of the instructions for Δ will permit Δ to be proved one-one (or increasing, or nondecreasing) in S. Since θ actually is one-one, etc., we can observe that the instructions for Δ are merely another way for computing θ so that θ is a p-1-1 (or p-increasing, or p-nondecreasing) p.r.f.

COROLLARY 5.8. *If S is sound for ENT, then*:

(i) *There is a p.r.f. which is a one-one onto p.r.f. but not a p-1-1, p-onto p.r.f.*

(ii) *There is a p.r.f. with range N which is not a p-onto p.r.f.*

(iii) *There is a p.r.f. which has infinite range but which is not a p-infinite p.r.f.*

Proof. The corollary is an immediate consequence of Theorem 5.6.

We can now obtain a slight strengthening of Theorem 5.4.

THEOREM 5.9. *If S is sound for ENT, then*:

(i) *There is a one-one recursive function which is a p-1-1 p.r.f. but not a p-1-1 p-function.*

(ii) *There is an increasing recursive function which is a p-increasing p.r.f. but not a p-increasing p-function.*

(iii) *There is a nondecreasing recursive function which is a p-nondecreasing p.r.f. but not a p-nondecreasing p-function.*

(iv) *There is a recursive function with range N which is a p-onto p.r.f. but not a p-onto p-function.*

(v) *There is a recursive function with infinite range which is a p-infinite p.r.f. but not a p-infinite p-function.*

(vi) *There is a recursive permutation which is a p-1-1, p-onto p.r.f. but not a p-permutation.*

Proof. Parts (i), (ii) and (iii) follow from Theorem 5.4 and Corollary 5.7.

(iv) Define $g(x)$ as follows:

$$g(x) = \begin{cases} \dfrac{x-1}{2} & \text{if } x \text{ is odd,} \\ \phi_{\Psi(x/2)}(x) + 1 & \text{if } x \text{ is even.} \end{cases}$$

Clearly, g is a recursive function and g is p-onto (also p-infinite). However, g differs from each p-function so that g cannot be a p-function, much less a p-onto or a p-infinite p-function.

(v) Immediate from part (iv).

(vi) The inverse function of $f_7(x)$ in Theorem 5.4(vi) is the desired recursive permutation. By Property 4.4, since f_7 is a p-1-1 p-function, its inverse will be a p-1-1, p-onto p.r.f. The inverse cannot be a p-permutation, however, for then f_7 would be also.

6. **Gödel numbers of provable functions.** Now that the existence of p-functions which are onto but which are not p-onto p-functions has been shown, one might wonder whether the failure of such a function $f(x)$ to be a p-onto p-function arises from inability to prove that f has N as its range, or merely from inability

to prove "ontoness" for the same Gödel number of $f(x)$ for which it is shown that f is total. In other words, if $f(x)$ has a Gödel number e for which $\vdash_S P_1(\mathbf{e})$ and another Gödel number e', $e \neq e'$, for which $\vdash_S P_5(\mathbf{e}')$, must f be a p-onto p-function? That this question is not trivial is shown by Theorem 6.1 and Corollary 6.2.

THEOREM 6.1. *If S is sound for ENT, every p-function $f(x)$ has at least one Gödel number e' such that not $\vdash_S P_1(\mathbf{e}')$.*

Proof. Given $f(x)$, we define $g(x)$ as follows:

$$g(x) = \begin{cases} f(x) & \text{if } \phi_{\Psi(x)}(x) \text{ converges.} \\ & \text{diverges otherwise.} \end{cases}$$

We take e' to be the Gödel number of $g(x)$ determined by the above instructions for computing $g(x)$. Since S is sound, $\phi_{\Psi(x)}(x)$ always converges, so e' is also a Gödel number for $f(x)$. However, if $\vdash_S P_1(\mathbf{e}')$, then clearly $\vdash_S (\forall x)(\exists y)(\exists n)\, M(\Psi(x), x, y, n)$ which contradicts Corollary 5.2.

COROLLARY 6.2. *If S is sound for ENT, then for each p-function $f(x)$ there exist a pair $\{e, e'\}$ of Gödel numbers for f such that it cannot be proved in S that ϕ_e and $\phi_{e'}$ are the same function, i.e.,*

$$\text{not } \vdash_S (\forall x)[(\forall y_1)(\forall y_2)[[(\exists n)\, M(\mathbf{e}, x, y_1, n) \wedge (\exists n)\, M(\mathbf{e}', x, y_2, n)] \rightarrow y_1 = y_2]$$
$$\wedge\ [(\exists y)(\exists n)\, M(\mathbf{e}, x, y, n) \leftrightarrow (\exists y)(\exists n)\, M(\mathbf{e}', x, y, n)]].$$

Proof. We take e to be a Gödel number of $f(x)$ such that $\vdash_S P_1(\mathbf{e})$ and determine e' as in Theorem 6.1. Clearly, if the statement above is a theorem of S, then $\vdash_S P_1(\mathbf{e}')$, which contradicts Theorem 6.1.

THEOREM 6.3. *If e and e' are Gödel numbers of the same recursive function $f(x)$ with range N such that $\vdash_S P_1(\mathbf{e})$ and $\vdash_S P_5(\mathbf{e}')$, then there is another Gödel number e'' of $f(x)$, which depends effectively on e and e', such that $\vdash_S P_1(\mathbf{e}'') \wedge P_5(\mathbf{e}'')$. That is to say, f is a p-onto p-function.*

Proof. We define a function $g(x)$ by enumerating its ordered pairs $\langle x, g(x)\rangle$ as follows.

Step 0: *A.* $g(0) = \phi_e(0)$.

B. Find an x_0 such that $\phi_{e'}(x_0) = 0$. Set $g(x_0) = 0$ (i.e., list the ordered pair $\langle x_0, 0\rangle$) unless $x_0 = 0$ and $g(x_0)$ has already been defined to be different from 0. In this case, set $g(1) = 0$.

Step 1: *A.* $g(1) = \phi_e(1)$ unless $g(1)$ was defined in Step 0, part *B*.

B. Find an x_1 such that $\phi_{e'}(x_1) = 1$. Set $g(x_1) = 1$ unless $g(x_1)$ has previously been defined to be different from 1. In this case, set $g(y_1) = 1$, where y_1 is the smallest number for which $g(x)$ has not already been defined.

Continuing, we obtain at the nth step:

Step n: *A*. $g(n) = \phi_e(n)$ unless $g(n)$ has been already defined at a previous step.

B. Find an x_n such that $\phi_{e'}(x_n) = n$. Set $g(x_n) = n$ unless $g(x_n)$ has previously been defined to be different from n. In this case, set $g(y_n) = n$, where y_n is the smallest number for which $g(x)$ has not previously been defined.

The above instructions for computing $g(x)$ yield a Gödel number e'' for g, which depends effectively on e and e'. First we observe that the procedure with Gödel number e'' will not run into trouble at part *A* of any step since ϕ_e is totally defined, nor will it diverge at part *B* of any step since $\phi_{e'}$ has range N. Furthermore, since $P_1(\mathbf{e})$ and $P_5(\mathbf{e}')$ are theorems of S, it can be shown in S that, for any n, the procedure will reach and carry out the instructions of step n. With this fact in hand, it is easy to show in S that $P_1(\mathbf{e}'')$ since if g has not been defined for some argument k by the kth step, it will be defined in step k, part *A*. Also, we can deduce $P_5(\mathbf{e}'')$ in S by formalizing the argument that if a number k has not appeared in the range of g by the kth step, k will be defined as the output of $g(x)$, for some x, in step k, part *B*. Thus we have $\vdash_S P_1(\mathbf{e}'') \wedge P_5(\mathbf{e}'')$. Now we note that whenever g is defined for an argument z, either $g(z) = \phi_e(z)$ or $g(z) = \phi_{e'}(z)$ or there must have been conflict at an earlier step between $\phi_e(z)$ and $\phi_{e'}(z)$. Since $f(x) = \phi_e(x) = \phi_{e'}(x)$, no conflicts will actually occur and $g(x) = f(x)$. Thus e'' is another Gödel number for $f(x)$, and f is a p-onto p-function.

COROLLARY 6.4. *If e and e' are Gödel numbers of the same infinite recursive function $f(x)$ such that $\vdash_S P_1(\mathbf{e})$ and $\vdash_S P_6(\mathbf{e}')$, then there is another Gödel number e'' of $f(x)$, which depends effectively on e and e', such that $\vdash_S P_1(\mathbf{e}'') \wedge P_6(\mathbf{e}'')$. That is to say, f is a p-infinite p-function.*

Proof. We modify the proof of Theorem 6.3 by changing part *B* of each step so that the nth step will read: "Find an x_n such that $\phi_{e'}(x_n) > n$. Set $g(x_n) = \phi_{e'}(x_n)$ unless $g(x_n)$ has previously been defined to be different from $\phi_{e'}(x_n)$. In this case set $g(y_n) = n + 1$, where y_n is the smallest number for which $g(x)$ has not previously, been defined." Again, the process can be guaranteed to reach step n, for any n, and $P_1(\mathbf{e}'')$ and $P_6(\mathbf{e}'')$ can both be deduced in S.

COROLLARY 6.5. *If e and e' are Gödel numbers of the same recursive permutation $f(x)$ such that $\vdash_S P_1(\mathbf{e})$ and $\vdash_S P_5(\mathbf{e}')$ then there is another Gödel number e'' of $f(x)$, which depends effectively on e and e', such that*

$$\vdash_S P_1(\mathbf{e}'') \wedge P_2(\mathbf{e}'') \wedge P_5(\mathbf{e}'').$$

That is to say, f is a p-permutation.

Proof. Given e and e', we use Theorem 6.3 to obtain a Gödel number e^* of $f(x)$ for which $\vdash_S P_1(\mathbf{e}^*) \wedge P_5(\mathbf{e}^*)$. Now since f is a recursive permutation, it is one-one. Therefore the procedure in Theorem 5.5 (i), when applied to $\phi_{e^*}(x)$ will yield another Gödel number e'' of $f(x)$ for which $\vdash_S P_1(\mathbf{e}'') \wedge P_2(\mathbf{e}'')$. But examination of the instructions for $g(x)$ in Theorem 5.5 (i) shows that it can easily be proved in S that the range of $f(x) = \phi_{e^*}(x)$ is contained in the range of $g(x) = \phi_{e''}(x)$. Thus, from $\vdash_S P_5(\mathbf{e}^*)$ we obtain $\vdash_S P_5(\mathbf{e}'')$, completing the proof.

7. **Proof indices and recursion properties.** One may have already observed that p-functions can be described in three different ways: as sets of ordered pairs, by the instructions for computing the function (that is, by the Gödel number of the function), and by the argument to which $\Psi(x)$ must be applied to give a Gödel number e of the function for which $P_1(\mathbf{e})$. We shall consider the third method of naming p-functions in this section and in part of §10.

DEFINITION 7.1. Let $f(x)$ be a p-function. Then a number k will be called a *proof number* of $f(x)$ if $\Psi(k)$ is a Gödel number of $f(x)$.

In developing a theory of provable recursive functions analogous to the theory of recursive functions, one might hope that a proof number of a p-function might be an analogue of a Gödel number for a partial recursive function. While this hope is not entirely in vain (cf. Theorem 10.2) at least one very important property of Gödel numbers of partial recursive functions, namely the fixed-point property given in the recursion theorem (cf. Kleene [7, p. 352]), fails to carry over to proof indices of p-functions.

Before proving this negative result, we can obtain a slight strengthening of the recursion theorem, which will be used in §§10 and 11.

THEOREM 7.2. *There exists a p-1-1 p-function $n(e)$ such that, for all e, $\phi_{\phi_e(n(e))} = \phi_{n(e)}$.*

Proof. Define a recursive function $g(e)$ such that $\phi_{g(e)} = \phi_{\phi_e(e)}$. Then the desired function $n(e)$ is simply $g(k(e))$, where $k(e)$ is the Gödel number of the composition $\phi_e(g(x))$, using a fixed Gödel number of g. Under a suitable method of Gödel numbering, there will be no difficulty in assuring that g and k are both one-one primitive recursive operations on Gödel numbers of partial recursive functions. Thus, $n(e)$ is a one-one primitive recursive function, therefore a p-1-1 p-function, and we have:

$$\phi_{n(e)} = \phi_{g(k(e))} = \phi_{\phi_{k(e)}(k(e))} = \phi_{\phi_e(g(k(e)))} = \phi_{\phi_e(n(e))}.$$

One might hope that a provable function analogue of Theorem 7.2 might hold, i.e., that for every recursive mapping $g(x)$ of proof numbers of p-functions, there would be a fixed point n, depending effectively on g, such that $\phi_{\Psi(g(n))} = \phi_{\Psi(n)}$. Failing this, one might still hope to obtain such a result if g were required to be

a p-function. However, neither result holds. That the first of the two propositions is false is easily shown.

THEOREM 7.3. *If S is sound for ENT, there exists a recursive function $g(x)$ such that, for every x, $\phi_{\Psi(g(x))} \neq \phi_{\Psi(x)}$.*

Proof. We merely define g as follows

$$g(x) = \mu z\,[\phi_{\Psi(z)}(0) \neq \phi_{\Psi(x)}(0)].$$

The soundness of S plus the fact that all constant functions are p-functions show that $g(x)$ is the desired recursive function.

The use of soundness of S, as a sufficient condition for Theorem 7.3 and for Theorem 7.4 below to hold, is clear. Furthermore, consistency of S is a necessary condition for the two theorems to hold. For if S is inconsistent, all Gödel numbers e of partial recursive functions have proofs in S of $\mathrm{P}_1(\mathbf{e})$. Thus, $\Psi \to N$ and Ψ is a recursive permutation. Then, given a recursive function f, we can apply the recursion theorem to the recursive function $h(x) = \Psi(f(\Psi^{-1}(x)))$ and obtain an n such that $\phi_{\Psi(f(\Psi^{-1}(n)))} = \phi_n$. Then if we let $y = \Psi^{-1}(n)$, we have $\Psi(y) = n$, and

$$\phi_{\Psi(f(y))} = \phi_{\Psi(f(\Psi^{-1}(\Psi(y))))} = \phi_{\Psi(f(\Psi^{-1}(n)))} = \phi_n = \phi_{\Psi(y)}.$$

Thus, Theorems 7.3 and 7.4 do not hold if S is inconsistent.

We now obtain the stronger negative result:

THEOREM 7.4. *If S is sound for ENT, there exists a p-function $f(x)$ such that for every x, $\phi_{\Psi(f(x))} \neq \phi_{\Psi(x)}$*[5].

Proof. First we define a recursive function g which operates on the instructions for computing $\phi_{\Psi(x)}$ in such a manner that for all x and all y:

$$\phi_{g(x)}(y) = \phi_{\Psi(x)}(y) + 1.$$

By soundness of S, $\phi_{\Psi(x)}$ is defined for all y so we have, for all x, $\phi_{g(x)} \neq \phi_{\Psi(x)}$. Now, if we can find a p-function f such that, for all x, $\Psi(f(x)) = g(x)$, then we are done since we will have, for all x,

$$\phi_{\Psi(f(x))} = \phi_{g(x)} \neq \phi_{\Psi(x)}.$$

The construction and justification of f takes place in five steps below; f is actually primitive recursive.

---

(5) The referee has pointed out that the method of proof used for this theorem is not valid when Ψ is an arbitrary primitive recursive enumeration of the p-functions. Thus, Ψ should be chosen so that there exist primitive recursive functions α and η with the properties mentioned in the proof. Such an enumeration of the p-functions can be produced using the standard techniques of arithmetization of S.

(1) We consider a suitable Gödelization of all finite sequences of characters using the alphabet of S, arranged according to the number of characters in each sequence. Clearly, one can effectively establish a one-one correspondence between such sequences of characters and N by listing all 1-character sequences, then all 2-character sequences, then all 3-character sequences, and so on, in such a manner that, given a number n, one can find effectively the sequence corresponding to n. Furthermore, given a sequence, one can effectively find its Gödel number, and if two sequences are of different length, the longer sequence will have the greater Gödel number. Now we assert the existence of a primitive recursive predicate $Q(x)$ such that $Q(x)$ is true if and only if the sequence with Gödel number x is a list of well-formed formulas of S which constitutes a proof in S of an expression of the form $\mathrm{P}_1(\mathbf{e})$, for some e. The actual primitive recursion equations for Q are somewhat tedious to construct but are straightforward in nature.

Given an x for which $Q(x)$, we can effectively "pad" the proof associated with x by adjoining the identity "$0 = 0$" in front of the proof. This yields a sequence of characters of S of greater length, which is, however, still a proof in S of the same expression as before. Because of the effectiveness of the Gödel numbering and the uniform manner in which a proof is modified, there is a primitive recursive function $\rho(x)$, which gives the Gödel number of the expression resulting when "$0 = 0$" is concatenated on the left of the sequence with Gödel number x. From the above discussion we see that for all x, $\rho(x) > x$ and if $Q(x)$, then $Q(\rho(x))$.

(2) We can now define a primitive recursive function $\eta(x)$ which enumerates in strictly increasing order the Gödel numbers x for which $Q(x)$. Let:

$$\eta(0) = a, \text{ where } a = \mu z\,[Q(z)],$$

$$\eta(x) = \begin{cases} \mu z\,[\eta(x-1) < z \leqq \rho(\eta(x-1)) \wedge Q(z)] & \text{if such a } z \text{ exists,} \\ 0 \quad \text{otherwise.} \end{cases}$$

Since $\rho(\eta(x-1))$ is a Gödel number greater than $\eta(x-1)$ for which Q holds, there will always be a z, $\eta(x-1) < z \leqq \rho(\eta(x-1))$, such that $Q(z)$. Thus, every number in the range of η will be the Gödel number of a proof in S of $\mathrm{P}_1(\mathbf{e})$, for some e, and conversely. Clearly, we also have for all x, $x \leqq \eta(x)$ since η is an increasing function.

(3) There is a primitive recursive function $\alpha(y)$ such that, whenever y is the Gödel number of a proof in S of $\mathrm{P}_1(\mathbf{e})$, $\alpha(y) = e$. This function merely extracts the expression for the numeral e from the last line of the proof associated with y. We now have the relationship $\Psi(x) = \alpha(\eta(x))$. (This equation can be made the definition for Ψ.)

(4) If we now reconsider the function $g(x)$, we can see that given a proof in S of $\mathrm{P}_1(\Psi(x))$, we can uniformly convert it to a proof of $\mathrm{P}_1(\mathbf{g}(x))$. This can be done

so as to give rise to a primitive recursive function $\beta(y)$ with the property that whenever y is the Gödel number of a proof in S of $P_1(\Psi(x))$, $\beta(y)$ is the Gödel number of a proof in S of $P_1(g(x))$. From this we have $\alpha(\beta(\eta(x))) = g(x)$.

(5) Finally, we define the desired function $f(x)$ as follows:

$$f(x) = \begin{cases} \mu z\,[z \leqq \beta(\eta(x)) \wedge \eta(z) = \beta(\eta(x))] & \text{if such a } z \text{ exists,} \\ 0 & \text{otherwise.} \end{cases}$$

Then f will be primitive recursive because β and η are. Since, from (4), $Q(\beta(\eta(x)))$ holds, we know that $\beta(\eta(x)) = \eta(z) \geqq z$, for some z. Therefore, the first clause of the definition of f will always be satisfied and we have, for each x, $\eta(f(x)) = \beta(\eta(x))$. Applying α to both sides we obtain:

$$\Psi(f(x)) = \alpha(\eta(f(x))) = \alpha(\beta(\eta(x))) = g(x).$$

This completes the proof.

8. **Provably recursive sets.** In this section we study properties of a provable analogue of the notion of a recursive set.

DEFINITION 8.1. A set B (of non-negative integers) will be called *provably recursive* (p-recursive) if the characteristic function C_B of B is a p-function.

DEFINITION 8.2. A p-recursive set B will be called *provably infinite* (p-infinite) if there is a Gödel number e of the characteristic function C_B of B such that

$$\vdash_S (\forall x)(\exists y)(\exists n)[y > x \wedge M(e,y,\mathbf{1},n)] \wedge P_1(e)\,(6).$$

Clearly the sets of Gödel numbers of characteristic functions of p-recursive sets and of p-infinite p-recursive sets are recursively enumerable.

Theorems 8.3 and 8.4 appear in Rogers [3]. We give a different proof for Theorem 8.4.

THEOREM 8.3. (i) *If a set B is finite or co-finite, then B is p-recursive*(7).

(ii) *If A and B are p-recursive sets, then $A \cup B$, $A \cap B$, $A - B$, and $\bar{A}$ are p-recursive sets.*

The proof is trivial.

THEOREM 8.4. *If S is sound for ENT, then there exists a recursive set B which is not p-recursive.*

---

(6) The method of Corollary 6.4 can be used to show that the expression $P_1(e)$ may be dropped from the formal statement without weakening the definition. The class of p-recursive sets is also unchanged if the definition is modified to require also that C_B be provably a characteristic function (cf. Theorem 5.5).

(7) A set B is said to be co-Z for some property Z if $\bar{B}$ has property Z.

Proof. We use a simple diagonalization. Let B be the set such that

$$C_B(x) = \begin{cases} 1 & \text{if } \phi_{\Psi(x)}(x) = 0, \\ 0 & \text{if } \phi_{\Psi(x)}(x) \neq 0. \end{cases}$$

By soundness of S, B is a recursive set, but its characteristic function cannot be a p-function.

THEOREM 8.5. *A set B is a p-infinite p-recursive set if and only if B is the range of a p-increasing p-function.*

Proof. Suppose B is p-infinite p-recursive. Define $f(x)$ as follows:

$$f(0) = \mu z\,[C_B(z) = 1],$$
$$f(x) = \mu z\,[z > f(x-1) \wedge C_B(z) = 1].$$

Since C_B is given as a p-function, f will be a p-increasing p-function by Property 4.3 and Theorem 5.5 (ii). It is clear that $f \to B$.

Now suppose B is the range of a p-increasing p-function $g(x)$. We can define a characteristic function of B as follows:

$$C_B(x) = \begin{cases} 1 & \text{if } (\exists y)\,[y \leqq x \wedge g(y) = x], \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to verify that the definition of C_B does, in fact, yield a characteristic function of B. Since g is a p-function, C_B will be a p-function and B will be p-recursive. Furthermore, by Property 4.5, g is a p-infinite p-function and it also can easily be shown in S that, for all x, $g(x) \geqq x$. From this it follows that one can show in S that for each x in the range of g, $C_B(x) = 1$, so that B is p-infinite p-recursive.

THEOREM 8.6. (i) *If B is a nonempty recursive set, then B is the range of a p-nondecreasing p-function.*

(ii) *If S is sound for ENT and B is the range of a p-nondecreasing p-function, then B is a nonempty recursive set.*

Proof. (i) Suppose that B is nonempty and recursive. Let e be a Gödel number of the characteristic function of B. We define an auxiliary function $g(x)$ as follows:

$$g(0) = \tau(b, b+1), \text{ where } b = \mu z\,[z \in B],$$

$$g(x+1) = \begin{cases} \tau(\pi_2(g(x)), \pi_2(g(x)) + 1) & \text{if } M(e, \pi_2(g(x)), 1, x+1), \\ \tau(\pi_1(g(x)), \pi_2(g(x)) + 1) & \text{if } M(e, \pi_2(g(x)), 0, x+1), \\ g(x)\ (\text{i.e., } \tau(\pi_1(g(x)), \pi_2(g(x)))) & \text{otherwise.} \end{cases}$$

Then we define $f(x) = \pi_1(g(x))$. To see that f is the desired function we must analyze the operation of g. Essentially, $g(x)$ represents the process of taking steps in the computation of $C_B(b + 1)$ until an output is obtained, then $C_B(b + 2)$, then $C_B(b + 3)$, etc. Those arguments for which $C_B(x) = 1$ are identified as members of B. If we regard g as a mapping from $N \times N$ into $N \times N$, the left member of the ordered pair of the argument for g represents the latest number found by the process to be in B and the right member represents the argument to which C_B is currently being applied. From this, one can verify that $f \to B$ and f is nondecreasing. Since f is clearly a p-function, by Theorem 5.5 (iii) f is a p-nondecreasing p-function.

(ii) By soundness of S, B is the range of a nondecreasing recursive function and B is consequently a recursive set.

Theorem 8.5 is the direct analogue of the fact that a set is infinite and recursive if and only if it is the range of an increasing recursive function. A natural analogue of the fact that a nonempty set is recursive if and only if it is the range of a nondecreasing recursive function would be a statement that a nonempty set would be p-recursive if and only if it were the range of a p-nondecreasing p-function. This statement is false since, by Theorem 8.6, a set would be recursive if and only if it were p-recursive, which contradicts Theorem 8.4.

We now fill in the lacuna left in the proof of Theorem 5.6. The following theorem was suggested by a closely-related result of Kent [12], and gives one of the basic incompleteness results for the theory of p-functions and p-recursive sets. The proof is based on a modification of the method Kreisel used in [11].

THEOREM 8.7. *If S is sound for ENT, then there is a p-recursive set A such that:*
(i) *A is infinite and co-infinite.*
(ii) *A is neither p-infinite nor co-p-infinite.*

Proof. First we introduce the primitive recursive predicate:

$$C(x,m,n) \equiv [n < x \wedge (\exists z)[z < x \wedge {}'M(\Psi(m), n, z, x - 1)]].$$

One can see that $C(x, m, n)$ will be true if and only if x is a proper upper bound for the following three numbers: n; the number of steps it takes for the computation of $\phi_{\Psi(m)}(n)$ to give an output; the ouput of the computation of $\phi_{\Psi(m)}(n)$.

Now we construct the following strictly increasing sequence:

$$\begin{aligned} x_0 &= \mu z C(z,0,0), \\ x_1 &= \mu z C(z,0,x_0), \\ x_2 &= \mu z C(z,1,x_1), \\ x_3 &= \mu z C(z,1,x_2), \\ &\vdots \\ x_{2k} &= \mu z C(z,k,x_{2k-1}), \\ x_{2k+1} &= \mu z C(z,k,x_{2k}). \end{aligned}$$

We next define a predicate $Q(x)$ so that:

$$Q(x) \equiv (\exists i)[x = x_i].$$

It is not immediately clear that $Q(x)$ is primitive recursive, but a set of primitive recursion equations can be written without difficulty. Given x, one merely imitates the construction of the above sequence until he encounters an application of C to $\langle x, m_0, n_0\rangle$ for some m_0 and n_0. Then $Q(x) \equiv C(x, m_0, n_0)$. Furthermore, to arrive at this point the predicate C need only be used $x+1$ times since the procedure for constructing the sequence can be carried out so that the leftmost argument of C increases by 1 at each step.

Now we define the characteristic function C_A of A as follows:

$$C_A(0) = 1,$$

$$C_A(x) = \begin{cases} 1 - C_A(x-1) & \text{if } Q(x), \\ C_A(x-1) & \text{if } \sim Q(x). \end{cases}$$

Since Q is primitive recursive, so is C_A. Thus A is a p-recursive set. Examination of the defining equations for C_A shows that the sequence of values of $C_A(x)$ is as follows:

$$\begin{array}{rccccccccccccc} x: & 0, & 1, & \cdots, & x_0, & \cdots, & x_1, & \cdots, & x_2, & \cdots, \\ & \updownarrow & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \\ C_A(x): & 1, & 1, & \cdots, 1, & 0, 0, & \cdots, 0, & 1, & 1, \cdots, & 1, 0, & 0, \cdots. \end{array}$$

From this one can see that if the sequence $x_0, x_1, x_2, \cdots$ is infinite, then both A and $\bar{A}$ will be infinite since for each x_i with odd subscript there is at least one member of A and for each x_i with even subscript there is at least one member of $\bar{A}$. Now suppose the last element of the sequence were x_t for some t. Then, for the appropriate k such that $t = 2k$ or $t = 2k + 1$, we would have $\sim C(z, k, x_t)$ for all $z > x_t$. But, by soundness of S, $\phi_{\Psi(x)}(x_t)$ will eventually converge, say in y_0 steps, giving output y_1. Then, if we take $z = \max\{y_0, y_1, x_t\} + 1$, we have $C(z, k, x_t)$, contradicting the above. Thus there are an infinite number of x_i's, and A and $\bar{A}$ are both infinite.

Now suppose A were p-infinite. Then, by Property 4.3 and Definition 8.2, the function $h(x)$ defined by:

$$h(x) = \mu z[z > x \wedge C_A(z) = 1]$$

would be a p-function. Let k be a proof number of $h(x)$. We can see that $h(x_{2k}) = x_{2k+1}$ from the defining equations for h, i.e., that $\phi_{\Psi(k)}(x_{2k}) = x_{2k+1}$. However, x_{2k+1} is defined in the sequence as $\mu z C(z, k, x_{2k})$ and one of the requirements for $C(z, k, x_{2k})$ to be true is that $z > \phi_{\Psi(k)}(x_{2k})$. But then $x_{2k+1} > \phi_{\Psi(k)}(x_{2k}) = x_{2k+1}$, which is impossible.

The proof that $\bar{A}$ is not p-infinite is symmetric with the above. We merely define:

$$h'(x) = \mu z\,[z > x \wedge C_A(z) = 0]$$

and proceed to consider $h'(x_{2k'+1})$, where k' is a proof number for $h'(x)$. This completes the proof of the theorem.

COROLLARY 8.8. *If S is sound for ENT, then there is a p-recursive set B which is infinite, co-infinite, p-infinite, but not co-p-infinite.*

Proof. We define $B = \{y \mid y = 2x \wedge x \in A\}$, where A is the set in Theorem 8.7. Clearly, B and $\bar{B}$ are both infinite. $\bar{B}$ is p-infinite because it contains all of the odd positive integers([8]). B is not p-infinite because it is trivial in S that B is p-infinite if and only if A is p-infinite.

The set $\bar{B}$ is clearly a p-recursive set which is infinite, co-infinite and p-infinite, but does not have a p-infinite complement. Further, we remark that the set of all even non-negative integers is an infinite co-infinite p-recursive set which is p-infinite and has a p-infinite complement. Thus there are infinite co-infinite p-recursive sets exhibiting each of the four possible combinations of provability and nonprovability with respect to the infinite cardinality of the sets and their complements.

9. **Recursively enumerable sets.** The provable analogue of a recursively enumerable set, i.e., the range of a partial recursive function, would be a set which is the range of a p-function. One could call such a set provably enumerable, but in view of the following theorem, the additional terminology is unnecessary.

THEOREM 9.1. *If $B \neq \varnothing$, then B is the range of a p-function if and only if B is recursively enumerable*([9]).

Proof. The result is immediate from the well-known theorem of Kleene that a nonempty set is the range of a primitive recursive function if and only if it is recursively enumerable.

Although one can, given x, y, and n, tell effectively (assuming soundness of S) whether the p-function with proof number n applied to x gives output y (i.e., whether $\phi_{\Psi(n)}(x) = y$), one still cannot tell effectively whether, given x and n, x is in the range of $\phi_{\Psi(n)}$. This follows immediately from the fact that the recursively enumerable, nonrecursive set K is the range of some p-function $f(x)$, by Theorem

([8]) We use the following lemma, the proof of which is immediate: If A and B are p-recursive sets such that A can be proved to be contained in B, then if A is p-infinite, B is p-infinite.

([9]) In fact, if $B \neq \varnothing$, given a Gödel number of B, one can effectively find a Gödel number of the desired p-function and also a number k such that $\phi_{\Psi(k)} \to B$. (See the proof of Theorem 10.2).

9.1. A decision procedure for the range of $f(x)$ would yield a decision procedure for K, which is impossible.

We know that if A is an infinite recursively enumerable set, then A is the range of a one-one recursive function. Theorem 9.1 shows that A is the range of a p-function. However, both properties need not hold simultaneously, i.e., such a set A is not necessarily the range of a one-one p-function, (which, by Theorem 5.5 (i), would be a p-1-1 p-function). This result follows from the next theorem, which is due to Rogers.

THEOREM 9.2. *If S is sound for ENT, there is an infinite recursively enumerable set A which is not the range of any p-1-1 p-function.*

Proof. We set up two lists, List A and List B. First the range of $\phi_{\Psi_2(0)}$ is enumerated until two different numbers have appeared. The first is put into List A and the second into List B. Then the range of $\phi_{\Psi_2(1)}$ is enumerated until two different numbers not occurring in List A or List B have appeared. Again, the first is put into List A and the second into List B. Continuing, at the kth step, the range of $\phi_{\Psi_2(k)}$ is enumerated until two new numbers not already occurring in List A or List B have appeared. This must eventually happen since, by soundness of S, $\phi_{\Psi_2(k)}$ is a one-one recursive function. The first is put into List A and the second into List B. Finally, A is defined as the set of all numbers which eventually get onto List A.

By Church's thesis, A is recursively enumerable. However, each p-1-1 p-function has contributed an element to List B, which is contained in $\bar{A}$, so that A cannot be the range of any p-1-1 p-function.

DEFINITION 9.3. A recursively enumerable set B will be called *provably infinite* if B is the range of a p-infinite p-function.

We show next that a p-infinite recursively enumerable set is a reasonable provable analogue of an infinite recursively enumerable set.

THEOREM 9.4. *A set B is p-infinite and recursively enumerable if and only if B is the range of a p-1-1 p-function.*

Proof. The converse part of the theorem follows immediately from Property 4.5. Now suppose B is the range of a p-infinite p-function $f(x)$. We simply define a function $g(x)$ as follows:

$$g(0) = f(0),$$

$$g(x) = f(y), \text{ where } y = \mu z\,[f(z) \text{ is different from } g(0), g(1), \cdots, g(x-1)].$$

Since f is a p-infinite p-function, it can be shown in S that $(\forall x)(\exists z)[f(z)$ is different from $g(0), g(1), \cdots, g(x-1)]$. Then by Properties 4.1 and 4.3, g is a p-function. It is obvious that g is one-one and therefore a p-1-1 p-function. It is also clear that $g \to B$.

COROLLARY 9.5. *If S is sound for ENT, then there is an infinite recursively enumerable set which is not p-infinite.*

Proof. The set A in Theorem 9.2 is infinite and recursively enumerable but not the range of any p-1-1 p-function. By Theorem 9.4 A cannot be p-infinite.

THEOREM 9.6. *If B is a p-infinite recursively enumerable set, then B contains a p-infinite p-recursive subset A.*

Proof. Let $f(x)$ be a p-infinite p-function such that $f \to B$. We will define a p-increasing p-function $g(x)$ such that the range of g is contained in B. By Theorem 8.5, if we define A as the range of g, then A will be p-infinite p-recursive. Let:

$$g(0) = f(0),$$

$$g(x) = f(y), \text{ where } y = \mu z [\, f(z) > g(x - 1)].$$

Since f is a p-infinite p-function, g will be an increasing (therefore p-increasing) p-function by Property 4.3. Clearly, the range of g is contained in B[10].

10. **Provably productive and provably creative sets.** The following definition is due to Rogers:

DEFINITION 10.1. A set B will be called *provably productive* (p-productive) if B is productive with a productive function which is a p-function.

An alternative definition, which might appear to be a better analogue of the definition of a productive set, would replace Gödel numbers by proof numbers as follows:

DEFINITION 10.1A. A set B will be called *provably productive* if there is a p-function $f(m)$ such that, for all m, whenever $W_{\Psi(m)} \subset B, f(m) \in B - W_{\Psi(m)}$.

THEOREM 10.2. *A set B satisfies Definition* 10.1 *if and only if B satisfies Definition* 10.1A.

Proof. Assume B is productive with a productive p-function g. Then if we define $f(m) = g(\Psi(m))$, f satisfies Definition 10.1A.

Now assume $f(m)$ satisfies Definition 10.1A. First, using the primitive recursive functions $\pi_1^3(x)$, $\pi_2^3(x)$, and $\pi_3^3(x)$, which give an effective one-one correspondence between N and N^3 via

$$x \leftrightarrow \langle \pi_1^3(x), \pi_2^3(x), \pi_3^3(x) \rangle,$$

we define, for each m,

---

[10] The statement that $A \subset B$ is also a theorem of S.

$$k_m(x) = \begin{cases} \pi_2^3(x) & \text{if } M(m, \pi_1^3(x), \pi_2^3(x), \pi_3^3(x)), \\ b & \text{otherwise,} \end{cases}$$

where b is some fixed member of B.

For each m, the function k_m is obviously a p-function. Furthermore, the Gödel number of k_m depends effectively on m. Thus, there is a recursive function $j(m)$ such that, for all m, $\phi_{j(m)} = k_m$. Examination of the definition of k_m shows that k_m has as range all of the outputs of ϕ_m, and b, so that $k_m \to W_m \cup \{b\}$. Thus, for all m, $W_{j(m)} = W_m \cup \{b\}$.

Now we assert the existence of a primitive recursive function $\gamma(m)$ such that, given m, $\gamma(m)$ is the Gödel number of a proof in S of $\mathrm{P}_1(\mathrm{j}(m))$. This can be done because proofs in S that k_m is total can be given in a uniform manner. Using the primitive recursive functions $\alpha(y)$ and $\eta(x)$ of the proof of Theorem 7.4, we note that $\alpha(\gamma(m)) = j(m)$, for all m, and we define a primitive recursive function $g(m)$ as follows:

$$g(m) = \begin{cases} \mu z\,[z \leqq \gamma(m) \wedge \eta(z) = \gamma(m)] & \text{if such a } z \text{ exists,} \\ 0 \quad \text{otherwise.} \end{cases}$$

Arguing as in the proof of Theorem 7.4, we have, for all m,

$$\Psi(g(m)) = \alpha(\eta(g(m))) = \alpha(\gamma(m)) = j(m).$$

Consider the p-function $h(m) = f(g(m))$. For all m, if $W_m \subset B$, then $W_{j(m)} \subset B$, and we have:

$$h(m) = f(g(m)) \in B - W_{\Psi(g(m))} = B - W_{j(m)} \subset B - W_m.$$

Thus h is a productive p-function for B.

DEFINITION 10.3. A set C will be called *provably creative* (p-creative) if C is recursively enumerable and $\bar{C}$ is p-productive.

We remark that the set $K = \{x \mid x \in W_x\}$ is p-creative since its productive function is the identity function. However, Rogers has shown that not all creative sets are p-creative (assuming soundness of S); therefore, not all productive sets are p-productive [3, p. 107].

The remaining results in this section are direct analogues of known facts about productive and creative sets. In each case, the proof follows the "classical" construction and observes that the appropriate functions are, in fact, p-functions. For this reason, although constructions will be given, some of the justifications will be abbreviated. References will be found in [3], [4], [5], and [8].

THEOREM 10.4. *Every p-productive set has a p-increasing productive p-function.*

Proof. Let B be p-productive with productive p-function f. First we define a primitive recursive function $h(x)$ such that, for all x, $W_{h(x)} = W_x \cup \{f(x)\}$. Then we construct $g(x)$ as follows:

$$g(0) = f(0),$$

$$g(x) = \begin{cases} f(h^k(x)), \text{ where } k = \mu z\,[z \leqq g(x-1) + 1 \wedge f(h^z(x)) > g(x-1)] \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if such a } z \text{ exists,} \\ g(x-1) + 1 \quad \text{otherwise.} \end{cases}$$

Clearly, g is increasing and if $W_x \subset B$, then $f(x), f(h(x)), f(h(h(x))), f(h^3(x)), \cdots$ will all be different members of $B - W_x$. Thus for some k, $0 \leqq k \leqq g(x-1) + 1$, $f(h^k(x))$ must be greater than $g(x-1)$ and $g(x)$ will be in $B - W_x$. On the other hand, if $W_x \not\subset B$, $g(x)$ will still be defined, possibly by the second clause in the expression. Since f and h are p-functions, the process defining $g(x)$ can be proved in S to terminate for all x, so that g will be a p-function. By Theorem 5.5, g will be a p-increasing p-function.

COROLLARY 10.5. *Every p-productive set has a p-1-1 productive p-function.*

THEOREM 10.6. *If a set B is p-productive, then B contains a p-infinite recursively enumerable subset A.*

Proof. The set of all Gödel numbers of the empty set (i.e., $\{x \mid W_x = \varnothing\}$) is not recursively enumerable, but it contains a p-infinite recursively enumerable subset D. Let g be a p-infinite p-function with range D and let f be a p-1-1 productive p-function of B. Then $h(x) = f(g(x))$ is a p-infinite p-function, and its range A is contained in B.

THEOREM 10.7. *Every p-1-1 p-function $f(x)$ is a productive p-function for some p-creative set.*

Proof. Let $C = \{f(x) \mid f(x) \in W_x\}$. If $W_x \subset \bar{C}$, then $f(x) \notin W_x$. But then $f(x) \in \bar{C} - W_x$, and C is p-creative with f as a productive p-function.

DEFINITION 10.8. A set B will be called *completely p-productive* if there is a p-function $f(x)$ such that for all x, $f(x) \in (B - W_x) \cup (W_x - B)$.

THEOREM 10.9. *A set is completely p-productive if and only if it is p-productive.*

Proof. The direct part of the theorem is trivial. Now suppose that B is a p-productive set with productive p-function $f(x)$. We can define for each x, a recursive function $g_x(y)$ such that, for all n, $W_{g_x(n)} = W_x \cap \{f(n)\}$. The Gödel number of g_x, as x varies, is given by a p-function $e(x)$. Now by Theorem 7.2 there is a p-function n such that, for all x, $W_{g_{(n(e(x)))}} = W_{n(e(x))}$. Now we define

$h(x) = f(n(e(x)))$. Then h is the desired completely productive p-function for if $h(x) \in W_x$, then $W_{n(e(x))} = \{h(x)\}$ and $h(x) \notin B$; if $h(x) \notin W_x$, then $W_{n(e(x))} = \varnothing$ and $h(x) \in B$.

THEOREM 10.10. *If B is a p-infinite recursively enumerable set, then B can be decomposed into a p-creative set C and a p-productive set P (i.e., $C \cup P = B$, $C \cap P = \varnothing$).*

Proof. By Theorem 9.4 there is a p-1-1 p-function f such that $f \to B$. Then define $C = f[K]$, $P = f[\bar{K}]$. C is recursively enumerable and both $\bar{C}$ and P are p-productive with productive p-function $h(x) = f(g(x))$, where g is a p-function such that, for all x, $W_{g(x)} = f^{-1}[W_x]$.

COROLLARY 10.11. *Every p-productive set B can be decomposed into a p-productive set P and a p-creative set C.*

Proof. Let A be a p-infinite recursively enumerable subset of B (Theorem 10.6). We decompose A into a p-creative set C and a set P' as in Theorem 10.10. Now if $P = B - C$, then P is p-productive with productive p-function $h(x) = f(g(x))$, where f is the productive p-function for B and g is a p-function such that, for all x, $W_{g(x)} = W_x \cup C$.

THEOREM 10.12. *If B is p-productive and A is recursively enumerable, then:*
(i) *If $A \subset B$, then $B - A$ is p-productive.*
(ii) *If $B \subset A$, then $B \cup \bar{A}$ is p-productive.*

Proof. Let f be a productive p-function for B.
(i) If $A \subset B$, the productive p-function for $B - A$ will be $h(x) = f(g(x))$, where g is a p-function such that $W_{g(x)} = W_x \cup A$.
(ii) If $B \subset A$, the productive p-function for $B \cup \bar{A}$ will be $h'(x) = f(g'(x))$, where g' is a p-function such that $W_{g'(x)} = W_x \cap A$.

COROLLARY 10.13. *Every p-productive set B has uncountably many p-productive subsets.*

Proof. By Theorem 10.6 B has a p-infinite recursively enumerable subset A. The construction of Theorem 10.12 (i) shows that for any set D such that $(B - A) \subset D \subset B$, D is p-productive. But there are uncountably many such sets D.

BIBLIOGRAPHY

1. C. F. Kent, *Algebraic structures of some groups of recursive permutations*, Doctoral thesis, Massachusetts Institute of Technology, Cambridge, Mass., 1960.
2. H. Rogers, Jr., *Provable recursive functions*, Bull. Amer. Math. Soc. **63** (1957), 140.
3. ———, *Theory of recursive functions and effective computability*, Vol. I, Mimeographed Notes, Massachusetts Institute of Technology, Cambridge, Mass., 1957.
4. ———, *The present theory of Turing machine computability*, J. Soc. Indust. Appl. Math. **7** (1959), 114–130.

5. ———, *Recursive functions and effective computability*, to be published by McGraw-Hill.

6. M. Davis, *Computability and unsolvability*, McGraw-Hill, New York, 1958.

7. S. C. Kleene, *Introduction to metamathematics*, Van Nostrand, Princeton, N. J., 1952.

8. D. L. Kreider, *Topics in the foundations of mathematics*, Dittoed Course Notes, Massachusetts Institute of Technology, Cambridge, Mass., 1959.

9. G. Kreisel, *On the interpretation of non-finitist proofs*, J. Symbolic Logic **16** (1951), 241–267, ibid. **17** (1952), 43–58.

10. ———, *Mathematical significance of consistency proofs*, J. Symbolic Logic **23** (1958), 155–182.

11. ———, Personal communication to H. Rogers, Jr. (December, 1956).

12. C. F. Kent, Personal communication (November, 1961).

HARVARD UNIVERSITY,
CAMBRIDGE, MASSACHUSETTS