THE JOURNAL OF SYMBOLIC LOGIC
Volume 24, Number 4, Dec. 1959

TWENTY-FOURTH ANNUAL MEETING OF THE ASSOCIATION FOR SYMBOLIC LOGIC

The twenty-fourth annual meeting of the Association for Symbolic Logic was held on Monday, December 28, 1959 at Columbia University in New York, in conjunction with the annual meetings of the American Philosophical Association.

Professor Paul Bernays of Zürich delivered an invited address in the afternoon on *Changes in problems in the foundations of mathematics*. Six twenty-minute contributed papers were delivered at the morning session which was presided over by Professor Hartley Rogers, Jr. Five twenty-minute papers were presented after Professor Bernays's address in the afternoon, with Professor Frederic B. Fitch presiding. The remaining papers were presented by title.

The Council of the Association met at lunch. ALAN ROSS ANDERSON

SOLOMON FEFERMAN. *Some completeness results for recursive progressions of theories (ordinal logics).*

This is a continuation of the work reported in this JOURNAL, vol. 23 (1958) pp. 105–106. All the theories T considered here are assumed to be axiomatic systems formalized in first or higher order calculi and adequate to the development of Peano's arithmetic. x will denote a first order variable below and f a second order variable, if any are to be used. We assume there is a formula $N(x)$ in T which is intended to express that x is a natural number. Further, it is taken that a notion of *validity* is defined for sentences of T according to which $\bigwedge_x(N(x) \rightarrow \phi(x))$ will be valid if and only if $\phi(\bar{n})$ is valid for each n. The notion of ordinal logic as defined in the previous reports is directly extended to such theories; we give it here the new designation *recursive progression of theories*.

We consider, in particular, recursive progressions based on the following *succession principle*. Let $\tau(x)$ be an RE-formula expressing that x is an axiom of T. Let $Sc^{(\tau)}(\mathrm{T})$ be the theory whose axioms are T, together with all sentences which express in T: *if for each n, $\vdash_{\mathrm{T}} \phi(\bar{n})$ then $\bigwedge_x(N(x) \rightarrow \phi(x))$*; here τ is needed to formalize the notion of provability from T. If all sentences of T are valid then so are those of $Sc^{(\tau)}(\mathrm{T})$. Let T_1 be an arbitrary valid theory, τ_1 an RE-formula which represents the axioms of T_1. A recursive progression of RE-formulas $\tau_d(d \in O)$ and associated theories T_d is constructed such that if $2^d \in O$ then $\mathrm{T}_{2^d} = Sc^{(\tau_d)}(\mathrm{T}_d)$, and if $3 \cdot 5^d \in O$ then $\mathrm{T}_{3 \cdot 5^d} = \mathbf{U}(\mathrm{T}_b : b <_O 3 \cdot 5^d)$.

It is possible to reduce the study of this progression to the work of Shoenfield on a *recursive* or *restricted ω-rule* (to appear in ***Bull. Acad. Sci. Polon.***). Denote by $Rs^{(\omega)}(\mathrm{T})$ the set of theorems obtainable from T by arbitrarily many applications of this rule. Shoenfield has shown that $Rs^{(\omega)}(\mathrm{T})$ contains all true sentences of number theory; further, if T is adequate to second order arithmetic, it contains all true sentences of the form $\bigvee_f \bigwedge_x[N(x) \wedge \phi(\bar{f}(x))]$. We have been able to show the following, where '$\equiv$' abbreviates 'has the same theorems as'. THEOREM 1. $\mathbf{U}(\mathrm{T}_d : d \in O) \equiv Rs^{(\omega)}(\mathrm{T}_1)$. THEOREM 2. *There is a path K through O which is recursive in O and such that* $\mathbf{U}(\mathrm{T}_d : d \in K) \equiv \mathbf{U}(\mathrm{T}_d : d \in O)$. THEOREM 3. *In case the language of* T *is first-order and* T_1 *is Peano's arithmetic (together with* $\bigwedge_x N(x)$*) then there is a hyperarithmetic path K within O such that* $\mathbf{U}(\mathrm{T}_d : d \in K) \equiv \mathbf{U}(\mathrm{T}_d : d \in O)$. In other words, the set of all true sentences of number theory is a constructive limit of recursively axiomatizable theories proceeding by the given succession principle.

It is natural to consider, besides progressions of the above type, those which are *autonomous* in the sense that only those theories T_d are taken in for which d can be proven to be in O within some theory $T_{d'}$ where $d' <_O d$. However, the totality of theorems of an autonomous progression is recursively enumerable; hence the above results depend in an essential way upon non-autonomy. (*Received October 30, 1959*).

FREDERIC B. FITCH. *A computer program for basic logic.*

A program for the IBM 704 has been devised which deals with the writer's system of "basic logic" in the following way: If any provable (or disprovable) formula is presented to the machine, it will report that the formula *is* provable (or disprovable) unless memory storage becomes exhausted in the process of testing the formula for provability. Furthermore, the actual proof (or disproof) of the formula can be reconstructed if desired, and in a certain sense this will be the simplest proof (or disproof) possible. If any unprovable formula that is not disprovable is presented to the machine, it will continue to run until all of memory storage is used up. The system of basic logic used here is extended to include negation, a "delay" operator D, and a multiple disjunction operator P, in addition to the usual operators **v** (disjunction), & (conjunction), ε (class membership, sometimes called T), **o** (product of operators, sometimes called B), E (non-emptiness or existence operator), and the combinatory operators W, C, I Z, the last of which can be used to represent the feedback aspects of sequential circuits. In fact, any sequential circuit (within limits of size) can be represented in this basic logic and so can be simulated by this program. Truth-tables can also be easily simulated, since the decision procedure for two-valued logic is incorporated in the program. Various problems in Boolean algebra can also be handled. It is clear that the program can be further elaborated so as to be able to handle the lower functional calculus in a somewhat similar way. (*Received October 28, 1959*.)

MAKOTO ITOH. *On a sequential Boolean lattice.*

We introduce into a boolean lattice B a monadic operator $\mathfrak{a}$ which satisfies the following axioms:

$$
\begin{array}{rll}
\text{I.} & \mathfrak{a}(a \vee b) = \mathfrak{a}a \vee \mathfrak{a}b & \\
\text{II.} & \mathfrak{a}(a \wedge b) = \mathfrak{a}a \wedge \mathfrak{a}b & \\
\text{III.} & \mathfrak{a}\neg a = \neg\mathfrak{a}a & (\neg a \text{ denotes the complement of } a) \\
\text{I}'. & \mathfrak{a}\bigvee_{\alpha \in M} a_\alpha = \bigvee_{\alpha \in M} \mathfrak{a}a_\alpha & (\text{M is any set}) \\
\text{II}'. & \mathfrak{a}\bigwedge_{\alpha \in M} a_\alpha = \bigwedge_{\alpha \in M} \mathfrak{a}a_\alpha & \\
\text{IV.} & \mathfrak{a}e_0 = 0 & (0 \text{ is the minimal zero element of B}) \\
\text{V.} & \mathfrak{a}e_\lambda = e_{\lambda-1}, \ (\lambda \geqq 1) &
\end{array}
$$

where $(e_0, e_1, \ldots)$ are the atomic elements of B.

We shall call such an operator $\mathfrak{a}$ a "sequential operator" and the B a "sequential boolean lattice".

Any sequential circuit or sequential machine can be represented with "sequential equations" in such a lattice.

We shall derive here the fundamental normal forms for sequential equations and also give the general method how to solve them. (*Received September 1, 1959*.)

JOHN MYHILL. *Recursive equivalence and recursive isomorphism.*

Lower-case Greek letters denote sets of non-negative integers. α is recursively equivalent (recursively isomorphic) to β if there exists a one-one partial recursive function defined at least on α (a recursive permutation) mapping α and β. Recursive equivalence is denoted by $\simeq$, isomorphism by $\cong$.

We write $\alpha \mid_0 \beta$ if there is a recursively enumerable (r.e.) set which includes α and is disjoint from β; $\alpha \mid_1 \beta (\alpha \mid_2 \beta)$ if there are disjoint r.e. (recursive) sets one of which includes α while the other includes β. It is clear that $\alpha \mid_2 \beta \to \alpha \mid_1 \beta \to \alpha \mid_0 \beta$ and that the converse does not hold. For $i = 0, 1, 2$ let $\alpha \leqq_i \beta$ mean that $\alpha \simeq \gamma$ for some $\gamma \subset \beta$ for which $\gamma \mid_i \beta - \gamma$. Clearly $\alpha \leqq_2 \beta \to \alpha \leqq_1 \beta \to \alpha \leqq_0 \beta$. *Theorem I.* If α, β are complements of r.e. sets, then $\alpha \leqq_2 \beta \leftrightarrow \alpha \leqq_1 \beta$; in fact $\alpha \leqq_1 \beta$ implies that α is *isomorphic* to some $\gamma \subset \beta$ for which $\gamma \mid_2 \beta - \gamma$. This suggests *Problem A.* Does $\alpha \leqq_2 \beta \leftrightarrow \alpha \leqq_1 \beta$ hold for arbitrary α, β? *Problem B.* Does $\alpha \leqq_1 \beta \leftrightarrow \alpha \leqq_0 \beta$ hold for α, β complements of r.e. sets? If so, does it hold for arbitrary α, β? *Theorem II.* For $i = 0, 1, 2$ let $\alpha \leqq_i^* \beta$ mean $\alpha \leqq_i \beta$ and $\alpha' \leqq_i \beta'$ (α' = complement of α). The relations $\alpha \leqq_0^* \beta$, $\alpha \leqq_1^* \beta$, $\alpha \leqq_2^* \beta$ are reducibility relations; indeed $\alpha \leqq_0^* \beta$ is ordinary one-one reducibility. Theorems I–II yield *Corollary III.* For α, β r.e., $\alpha \leqq_1^* \beta \leftrightarrow \alpha \leqq_2^* \beta$ (we do not know if this relation is stronger than one-one reducibility); and *Corollary IV.* Every infinite r.e. set is the union of a recursive set and a creative set. An affirmative answer to Problems A and B is suggested by *Theorem V.* For $i = 0, 1, 2$ denote by $\alpha \equiv_i \beta$ the relation ($\alpha \leqq_i^* \beta$ and $\beta \leqq_i^* \alpha$). Then $\alpha \equiv_0 \beta \leftrightarrow \alpha \equiv_1 \beta \leftrightarrow \alpha \equiv_2 \beta \leftrightarrow \alpha \cong \beta$. [This research was supported by National Science Foundation Grant G3466, and by a grant from the Institute for Advanced Study.] (*Received August 26, 1959.*)

HILARY PUTNAM. *An unsolvable problem in number theory.*

Since every non-negative integer is the sum of four squares, there are positive integers $y_1, \ldots, y_n$, such that $P(y_1, \ldots, y_n, x) = 0$ if and only if there are rational integers $y_{i1}, \ldots, y_{i4}$ $(i = 1, 2, \ldots, n)$, x_1, x_2, x_3, x_4 such that

$$\text{I.} \begin{cases} x = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1 \\ P(y_{11}^2 + y_{12}^2 + y_{13}^2 + y_{14}^2 + 1, \ldots, y_{n1}^2 + y_{n2}^2 + y_{n3}^2 + y_{n4}^2 + 1, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1) = 0. \end{cases}$$

But since when x is positive and P is a polynomial with integral coefficients, I. is equivalent to the single equation:

$x = (1 - P^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1)$, where "P" abbreviates

$P(y_{11}^2 + y_{12}^2 + y_{13}^2 + y_{14}^2 + 1, \ldots, y_{n1}^2 + y_{n2}^2 + y_{n3}^2 + y_{n4}^2 + 1,$

$x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1)$ and the variables range over rational integers, it follows that *every diophantine set of positive integers is identical with the set of positive integers represented by some polynomial.*

Using this characterization of the diophantine sets, and employing the fact that there is no algorithm for telling whether or not a diophantine set is the set of *all* positive integers (this can be proved using an argument which is in essence due to Myhill) we obtain: *There is no algorithm for telling, given a polynomial, whether or not it represents every positive integer.*

Using the result, which Davis and I have obtained (cf. our abstract in the *Notices* of the American Mathematical Society for the October 1959 meeting) that *if* (A) for every n there are n primes in arithmetic progression, and (B) Julia Robinson's hypothesis that there exists a diophantine predicate of "roughly exponential" rate of growth is correct, *then* every recursively enumerable predicate is diophantine, it follows that (A) and (B) imply that every recursively enumerable set is identical with the set of positive integers represented by some polynomial. Similarly it can be shown (using another result which is stated in the same abstract) that (A) by itself implies that every recursively enumerable set of positive integers is identical with the set of positive integers represented by some "exponential polynomial" — i.e., a polynomial which may contain variable exponents (e.g., $x^n + y^n - z^n$). It may be remarked that the truth or falsity of (A) is one of the major open questions in present day number theory. (*Received September 27, 1959.*)

RAYMOND M. SUMLLYAN. *Creative sets.*

We consider the Post enumeration $\omega_1, \omega_2, \ldots, \omega_i, \ldots$ of all r.e. sets. We let N be the set of natural numbers and $\varnothing$ be the empty set. We call a number set α *weakly productive* if there is a recursive function $f(x)$ such that for every number i: (i) if ω_i is empty then $f(i) \in \alpha$; (ii) if ω_i is a *unit* set contained in α then $f(i) \notin \omega_i$. We show the following conditions equivalent: (i) α is weakly productive; (ii) there is a recursive function $g(x)$ such that for every number i, if $\omega_i = \varnothing$ then $g(i) \in \alpha$ and if $\omega_i = \mathrm{N}$ then $g(i) \notin \alpha$; (iii) α is productive; (iv) the complement $\tilde{\alpha}$ of α is universal (i.e., every r.e. set is 1-1 reducible to $\tilde{\alpha}$).

Let us say that a collection Σ of r.e. sets is uniformly (many-one) reducible to α if there is recursive function $f(x, y)$ such that for every number i for which $\omega_i \in \Sigma$, the function f_i (defined by the condition $f_i(x) = f(i, x)$) is a many-one reduction of ω_i to α. We show that a sufficient condition for α to be universal is that the collection of *recursive* sets is uniformly reducible to α. From this it readily follows that a sufficient condition for an axiomatizable theory (T) to be creative is that all *recursive* sets be *uniformly* representable in (T) — i.e., that there is a recursive function $\phi(x)$ such that for every *recursive* set ω_i, $\phi(i)$ is the Gödel number of a formula of (T) which represents ω_i. (*Received November 4, 1959.*)

RAYMOND M. SMULLYAN. *Effective inseparability.*

Our terminology follows that of the above abstract. It was first shown by Muchnik, and independently by Smullyan, that every effectively inseparable pair of r.e. sets is doubly universal. Stronger results along these lines are as follows: Call a pair (α, β) *doubly productive* if there is a recursive function $f(x, y)$ such that for any two respective subsets ω_i, ω_j of α, β which are disjoint from each other, $f(i, j) \in (\alpha \cap \beta) - (\omega_i \cup \omega_j)$. If α, β are disjoint and r.e. then $(\tilde{\alpha}, \tilde{\beta})$ is doubly productive iff (α, β) is effectively inseparable (if α, β are not assumed r.e. then the effective inseparability of (α, β) is only *implied* by the double productivity of $(\tilde{\alpha}, \tilde{\beta})$). We say that (α, β) is *weakly doubly productive* if there is a recursive function $f(x, y)$ such that for any numbers i, j such that ω_i, ω_j are disjoint sets with at most one element between them, the following condition holds: (i) if ω_i is a unit set contained in α then $f(i, j) \notin \omega_i$; (ii) if ω_j is a unit set contained in β then $f(i, j) \notin \omega_j$; (iii) if ω_i, ω_j are both empty then $f(i, j) \in \alpha \cap \beta$. The following conditions are shown equivalent: (i) $(\tilde{\alpha}, \tilde{\beta})$ is weakly doubly productive; (ii) $(\tilde{\alpha}, \tilde{\beta})$ is doubly productive; (iii) (α, β) is doubly universal — i.e., for every disjoint pair (ω_i, ω_j) there is a recursive 1-1 function $f(x)$ such that $\omega_i = f^{-1}(\alpha)$ and $\omega_j = f^{-1}(\beta)$; (iv) there is a recursive function $g(x)$ such that for any numbers i, j for which (ω_i, ω_j) is one of the 3 pairs $(\mathrm{N}, \varnothing)$, $(\varnothing, \mathrm{N})$, $(\varnothing, \varnothing)$, $g(i, j)$ is respectively in α, in β, outside α and β. We say that a collection Σ of ordered pairs (ω_i, ω_j) of r.e. sets is *uniformly* reducible to (α, β) iff there is a recursive function $g(x, y, z)$ such that for every pair (ω_i, ω_j) in Σ, the function $g_{i,j}$ (defined by the condition $g_{i,j}(x) = g(i, j, x)$) is simultaneously a reduction of ω_i to α and ω_j to β. We show that a sufficient condition for (α, β) to be doubly universal is that the collection of all disjoint pairs of recursive sets — or even the collection consisting of only the 3 pairs $(\mathrm{N}, \varnothing)$, $(\varnothing, \mathrm{N})$, $(\varnothing, \varnothing)$ — is uniformly reducible to (α, β). (*Received November 4, 1959.*)

RAYMOND M. SMULLYAN. *Further results on effective inseparability.*

We generalize the notion of effective inseparability to pairs of sets not necessarily disjoint. A pair (α, β) is called E.I. (effectively inseparable) iff there is a recursive function $g(x, y)$ such that for every pair ω_i, ω_j of respective supersets of α, β whose intersection is $\alpha \cap \beta$, $g(i, j) \notin \omega_i \cup \omega_j$. It remains true that if $(\tilde{\alpha}, \tilde{\beta})$ is doubly productive then (α, β) is E.I., and if (α, β) is E.I. and α. β are r.e, then $(\tilde{\alpha}, \tilde{\beta})$ is doubly productive. Hence a r.e. pair (α, β) of sets (not necessarily disjoint) is E.I. iff it is doubly universal. We then *strengthen* the notion of E.I. as follows: we say that (α, β) is E.I.$^+$ iff there is a recursive function $g(x, y)$ such that for any numbers i, j such that ω_i, ω_j are respectively supersets of α, β whose intersection is included in the symmetric difference of α and β ,$g(i, j) \notin \omega_i \cup \omega_j$. It is shown that no disjoint pair (α, β) can possibly be E.I.$^+$; hence there exists a pair of r.e. sets which is E.I. but not E.I.$^+$. Up to recursive isomorphism there is only I pair of r.e. sets which is E.I.$^+$ Also a pair (α, β) of r.e. sets is E.I.$^+$ iff it is doubly univeral for *all* pairs ω_i, ω_j, whether disjoint or not — i.e., iff for every ω_i, ω_j (whether disjoint or not) ω_i and ω_j are respectively 1-1 reducible to α, β under a common function. Finally we show that if we let Σ be the collection of all pairs (ω_i, ω_j) of *recursive* sets — or even the collection of such pairs (ω_i, ω_j) such that $\omega_i = \omega_j$ or $\omega_i = \tilde{\omega}_j$ — or even the collection consisting of the 4 pairs (N, ∅), (∅, N), (∅, ∅), (N, N) — then a sufficient condition for (α, β) to be doubly universal for *all* r.e. pairs is that Σ is uniformly reducible to (α, β). (*Received November 4, 1959.*)

NUEL D. BELNAP, JR. *Tautological entailments.*

If B is a propositional variable or the negate thereof, then B is an *atom*. An atom is a *primitive conjunction* {*disjunction*}, and if A and B are primitive conjunctions {disjunctions} then so is $A \wedge B$ {$A \vee B$}. $A \rightarrow B$ is a *primitive entailment* iff A {B} is a primitive conjunction {disjunction}. $A \rightarrow B$ is a *first degree entailment* iff A and B are both written solely in terms of propositional variables, $\wedge$, $\vee$, and $^-$ (other truth-functional connectives being treated as defined by these).

A primitive entailment $A_1 \wedge \ldots \wedge A_m \rightarrow B_1 \vee \ldots \vee B_n$ is an *explicitly tautological entailment* iff some atom A_i is the same as some atom B_j. A first degree entailment $A \rightarrow B$ is a *tautological entailment* iff $A \rightarrow B$ is reducible by the following replacement-rules to a formula $A_1 \vee \ldots \vee A_m \rightarrow B_1 \wedge \ldots \wedge B_n$, where every $A_i \rightarrow B_j$ is an explicitly tautological entailment. *Replacement-rules*: (1) $A \wedge B = B \wedge A$; $A \vee B = B \vee A$; (2) $A \wedge (B \wedge C) = (A \wedge B) \wedge C$; $A \vee (B \vee C) = (A \vee B) \vee C$; (3) $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$; $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$; (4) $\overline{A \wedge B} = \bar{A} \vee \bar{B}$; $\overline{A \vee B} = \bar{A} \wedge \bar{B}$; (5) $\bar{\bar{A}} = A$. Tautological entailmenthood is effectively decidable.

Theorem: A first degree entailment $A \rightarrow B$ is a theorem of the system E of entailment (XXIII 457) iff $A \rightarrow B$ is a tautological entailment.

It is suggested that "tautological entailmenthood" is a plausible definition of "validity" for first degree entailments, in which case the theorem amounts to a proof of the soundness and completeness of that fragment of E consisting of first degree entailments.

It is also possible to generate the set of tautological entailments via a Gentzen *Sequenzen-kalkül*: to the usual machinery for $\wedge$ and $\vee$, add rules for negated negation, negated conjunction, and negated disjunction in antecedent and consequent. (*Received November 1, 1959.*)

H. KYBURG. *Probability and randomness, I.*

A set of statements $\mathscr{S}$ is called a rational set, if it satisfies the following axioms:

S-1. If S $\in \mathscr{S}$, then (the denial of S) nS $\notin \mathscr{S}$.

S-2. If S $\in \mathscr{S}$, and the conditional whose antecedent is S and whose consequent is T is logically true, then T $\in \mathscr{S}$.

S-3. $\mathscr{S}$ is not empty.

S-4. If there is a statistical statement about the sets x and y in $\mathscr{S}$, then there is a strongest statistical statement about these sets in $\mathscr{S}$.

Randomness is characterized by six axioms:
R-1. If x is a random member of y with respect to z, relative to $\mathscr{S}$, $\mathscr{S}$ is a rational set of statements.
R-2. If x is a random member of y with respect to z, relative to $\mathscr{S}$, '$x \epsilon y$' belongs to $\mathscr{S}$.
R-3. If x is a random member of y with respect to z, relative to $\mathscr{S}$, and x' is a random member of y' with respect to z', relative to $\mathscr{S}$, and '$x \epsilon z$' is connected by a biconditional chain to '$x' \epsilon z'$', then the strongest statement about y and z is just as strong as the strongest statement about y' and z'.
R-4. If x is a random member of y with respect to z, relative to $\mathscr{S}$, then x is a random member of y with respect to z, relative to $\mathscr{S}$, then x is a random member of y with respect to $\bar{z}$, relative to $\mathscr{S}$.
R-5. If x is a random member of y with respect to z, relative to $\mathscr{S}$, and x' is a random member of y' with respect to z', relative to $\mathscr{S}$, then $(x; x')$ is a random member of the cartesian product $y \times y'$, with respect to the cartesian product $z \times z'$, relative to $\mathscr{S}$.
R-6. If x is a random member of y with respect to z, relative to $\mathscr{S}$, and x' is a random member of y' with respect to z', relative to $\mathscr{S}$, then $(x; x')$ is a random member of $y \times y'$, with respect to $\hat{x}\hat{y}(x \epsilon z \vee y \epsilon z')$, relative to $\mathscr{S}$.

Probability is defined thus: The probability of a statement S, relative to the set of statements $\mathscr{S}$ (which may represent a set of true or hypothetically true statements, or a rational corpus, or simply a set of statements) is the pair of numbers $(p; q)$, if S is connected biconditionally to a statement of the form '$x \epsilon z$'; if x is a random member of y, with respect to z, relative to $\mathscr{S}$, for some y; and if the strongest statistical statement in $\mathscr{S}$ about y and z asserts that the proportion of y's that are z's falls in the closed interval $[p, q]$.

Theorems analogous to the conventional rules for manipulating probabilities are proved on the basis of the above axioms; but I argue that there are sufficient grounds for rejecting axioms R-5 and R-6 as representing an intuitively acceptable notion of randomness. (*Received October 30, 1959.*)

H. Kyburg. *Probability and randomness, II.*

This is a specification of the preceding system, in which it is possible to define randomness explicitly, and in which all of the usual probability relationships are forthcoming. But it is too narrow to serve as a general explication for probability, even though it is broader than the usual frequency interpretation.

$\mathscr{S}$A is a *rational set of statements about the set A*. The following axioms hold for $\mathscr{S}$A.

(S-1) If S ϵ $\mathscr{S}$A, then its negation, nS, does not belong to $\mathscr{S}$A.
(S-2) If S ϵ $\mathscr{S}$A, and the conditional whose antecedent is S and whose consequent is T, S cd T, belongs to $\mathscr{S}$A, then T ϵ $\mathscr{S}$A.
(S-3) $\mathscr{S}$A is not empty.

I define the set of *interesting subsets of A* thus:

D-4: "$x \epsilon$ IA" for " '$x \subset$ A' ϵ $\mathscr{S}$A. '%(A, x, $(p; p)$)' ϵ $\mathscr{S}$A for some p. x is not the unit class of some member of A."
(S-5) If $x_1 \epsilon$ IA and $x_2 \epsilon$ IA and ..., then $x_1 \cup x_2 \cup \ldots \epsilon$ IA, and $\bar{x}_1 \cap$ A ϵ IA.
(S-6) If '%(A, y, (0; 0))' ϵ $\mathscr{S}$A, then $\sim(\exists x)$('$x \epsilon y$' ϵ $\mathscr{S}$A).
(S-7) If $z \epsilon$ IA and $z' \epsilon$ IA and '$x \epsilon z$' $\mathscr{S}$A-B'$x' \epsilon z'$, then either '$x \epsilon z$' ϵ $\mathscr{S}$A, or '$x = x'$' and '$z = z'$' both belong to $\mathscr{S}$A.
(S-8) $(\exists y)(z)(y \epsilon$ IA."$x \epsilon y$" ϵ $\mathscr{S}$A.$z \epsilon$ IA."$x \epsilon z$" ϵ $\mathscr{S}$A.$\supset$"$y \subset z$" ϵ $\mathscr{S}$A).

Randomness is defined as follows: relative to the set of statements $\mathscr{S}$A, x is a random member of y with respect to membership in z, when either '$x \epsilon y$' ϵ $\mathscr{S}$A and '$y \subset z$' ϵ $\mathscr{S}$A, or '$x \epsilon y$' ϵ $\mathscr{S}$A, y and z are both interesting subsets of A, and for every new triplet x', y', and z', such that "$x' \epsilon z'$" is connected by a biconditional chain to "$x \epsilon z$" and y' and z' are interesting subsets of A, and "$x' \epsilon y'$" is a member of $\mathscr{S}$A, either the proportion of y' that belongs to z' is just the same as the proportion of y that belongs to z, or else "$y \subset y'$" $\epsilon\ \mathscr{S}$A. In symbols:

D-5: "$x\mathscr{S}$A-Ran(y, z)" for " '$x \epsilon y'$' $\epsilon\ \mathscr{S}$A . '$y \subset z'$' $\epsilon\ \mathscr{S}$A $\vee$ '$y \subset \bar{z}'$' $\epsilon\ \mathscr{S}$A: $\vee$:
'$x \epsilon y'$' $\epsilon\ \mathscr{S}$A . $y \epsilon$ IA . $z \epsilon$ IA . $(x')(y')(z')$("$x' \epsilon z'$"$\mathscr{S}$A-B"$x \epsilon z$" .
$z' \epsilon$ IA . $x' \epsilon$ IA . "$x' \epsilon y'$" $\epsilon\ \mathscr{S}$A. $\supset$:'%$(y', z', (p; p))$' $\epsilon\ \mathscr{S}$A $\equiv$
'%$(y, z, (p; p))$' $\epsilon\ \mathscr{S}$A .$\vee$ "$y \subset y'$" $\epsilon\ \mathscr{S}$A).

Probability is defined in the manner of the previous system. Conditional probabilities are introduced in the obvious way: the probability of S, given T, relative to the set of statements about A, $\mathscr{S}$A, is simply the probability of S relative to the set of statements $\mathscr{S}$A supplemented by T, together with all of its consequences in $\mathscr{S}$A. On this basis the whole conventional probability calculus can be derived for statements of the form $x \epsilon y$, where y is one of the interesting subsets of A, and where x is, in any given context, always the same object.

In order to deal with statements like '$x_1 \epsilon y_1 . x_2 \epsilon y_2$,' however, we need modify the system only to the extent of considering a rational set of statements about A^2 in lieu of a rational set of statements about A; and in general a rational set of statements about A^n will suffice for most finitary probabilistic considerations. *(Received November 19, 1959.)*

HUGUES LEBLANC. *On requirements for conditional probability functions.*

Let PC be a version of the propositional calculus based on '$\sim$' and '&'. Conditional probability functions can be tacked on to PC in two major ways. Method A: The metalogical phrase 'A is a valid wff of PC' or, for short, '$\vdash A$' is first recursively defined by means of such clauses as A1–A3 in this JOURNAL, vol. 23 (1958) no. 4, p. 422, and Modus Ponens (A4). A metalogical function Pr, defined for every pair of wffs of PC, is next said to constitute a conditional probability function for PC if it meets the following requirements: A5. $0 \leqq \Pr(A, B)$; A6. $\Pr(A, A) = 1$; A7. If $\vdash (A \equiv B)$ and $\vdash (C \equiv D)$, then $\Pr(A, C) = \Pr(B, D)$; A8. If not $\vdash \sim B$, then $\Pr(\sim A, B) = 1 - \Pr(A, B)$; and A9. $\Pr(A \,\&\, B, C) = \Pr(A, B \,\&\, C) \times \Pr(B, C)$. Method B: A metalogical function Pr, defined again for every pair of wffs of PC, is first said to constitute a conditional probability function for PC if it meets the following requirements: B1. $0 \leqq \Pr(A, B)$; B2. $\Pr(A, A) = 1$; B3. If $\Pr(B, D) = \Pr(C, D)$ for every wff D of PC, then $\Pr(A, B) = \Pr(A, C)$; B4. If $\Pr(C, B) \neq 1$ for at least one wff C of PC, then $\Pr(\sim A, B) = 1 - \Pr(A, B)$; B5. $\Pr(A \,\&\, B, C) = \Pr(A, B \,\&\, C) \times \Pr(B, C)$; and B6. $\Pr(A \,\&\, B, C) = \Pr(B \,\&\, A, C)$. The metalogical phrase '$\vdash A$' is next defined as follows: B7 $\vdash A$ if and only if $\Pr(A, \sim A) = 1$. Method A, which may go back to Carnap, ***Logical foundations of probability,*** pp. 295–296, is studied in Leblanc, this JOURNAL, vol. 22, (1957) no. 4, pp. 345–349. Method B is an adaptation of a proposal of Popper, ***The logic of scientific discovery,*** Appendix *v, who showed, essentially, that B1–B7 yield as theorems the propositional analogues of Huntington's fourth set of postulates for Boolean algebra. It is reported here, as an improvement upon Popper's result, that Method A and Method B are equivalent, and, incidentally, that the propositional analogues of Huntington's postulates, though they yield only valid biconditionals of PC as theorems, come to yield all valid wffs of PC as theorems when supplemented with Modus Ponens and the rule: From $(A \,\&\, B) \equiv A$ to infer $A \supset B$. *(Received November 14, 1959.)*

M. L. MINSKY. *A non-writing non-erasing universal Turing machine with two blank tapes.*

We consider Turing machines with single ended tapes and assume that the machines can sense the ends of their tapes. For an arbitrary (one-tape) such machine T we can construct a two-tape machine T* with this property: If the machine T, started at its tape origin with the binary number K written on its tape, stops eventually with the binary number T(K) written on its tape then the machine T*, if started with its first tape at its origin and the second tape at its 2^K-th square, will stop with the second tape at this $2^{T(K)}$-th square.

The machine T* never changes the contents of its tapes which may as well be blank. From this we can easily obtain Theorem 19 of Rabin and Scott (***IBM J. Res. and Dev.,*** vol. 2, no. 3, April 1959) and H. Wang's result (***J. Assoc. Computing Machinery,*** vol. 4, pp. 69 ff.) that all recursive functions are computable on ordinary Turing machines without erasure. It also follows that there exists an ordinary universal Turing machine which never has more than three 1's on an otherwise blank tape. (*Received November 4, 1959.*)

TRENCHARD MORE, Jr. *A normal form theorem for the implicational ordering,* A0.

Modus ponens, $B \Rightarrow C\ .\Rightarrow\!:\ A \Rightarrow .\ B \Rightarrow C$, $A \Rightarrow .\ B \Rightarrow C :\ \Rightarrow\!:\ A \Rightarrow B\ .\Rightarrow .\ A \Rightarrow C$, and $A \Rightarrow A$ define A0a (format a). If A is a formula then A and $\oplus$A are *lines*. If L is a line then *L is a line. Let "$*n$" denote a sequence $** \ldots *$ of n uncircled stars, $n \geqq 0$. Let "$\oplus n$" denote either $*n$ if $n \geqq 0$ or $*n - 1\oplus$ if $n > 0$. For $n \geqq 0$ let "$---n$" denote a finite sequence of zero or more lines that does not contain a line of the form $*m \oplus C$, $0 \leqq m < n$ when $0 < n$. The following rules define A0c: (1) Infer $*n \oplus A$. (2) From $\left\{\begin{array}{c} *n \oplus A \\ ---n+1 \\ *n * B \end{array}\right\}$ infer $*n[A \Rightarrow B]$. (3) From $\left\{\begin{array}{c} \oplus n[A \Rightarrow B] \\ ---n \end{array}\right\}$ and $\left\{\begin{array}{c} *n \oplus m\, A \\ ---n+m \end{array}\right\}$, infer $*n *m\, B$. (4) Infer $*n[A \Rightarrow A]$. No stars prefix a proved formula. The following rules define A0c1: (1) and (2) of A0c. (5) From $\left\{\begin{array}{c} *n[A \Rightarrow B] \\ *n\, A \end{array}\right\}$ infer $*n\, B$. (6) From $\left\{\begin{array}{c} \oplus n\, A \\ ---n \end{array}\right\}$ infer $*n\, A$. (7) From $*n[A \Rightarrow B]$ infer $*n * [A \Rightarrow B]$. Then A0a = A0c1 and A0c1 = A0c in the sense that each system has the same theorems and formulas. Let f_n have as values finite sequences of zero or more lines of the form $*m\, A$, $m \leqq n$. f and g are similar to f_n. $f \subseteq g$ if, disregarding repetition, every line that occurs in f also occurs in g. f and g are *cognate* if $f \subseteq g$ and $g \subseteq f$. $f \Vdash *n\, B$ means that there is a proof in A0c that does not contain a line of the form $*m \oplus C$ $(m < n)$ of $*n\, B$ from the line hypotheses f. $*n\, B$ is a theorem if and only if $n = 0$ and $\Vdash B$. Let "$\rightarrow$" replace "$\Vdash$". The following subproof sequent rules define A0d2:

*axiom $f,\ *n\, A,\ g \rightarrow *n\, A$

*thin $f \rightarrow *n\, C$
$*m\, A,\ f \rightarrow *n\, C$

*cog $f \rightarrow *n\, C$
$g \rightarrow *n\, C$ if f and g are cognate.

$\rightarrow \Rightarrow$ $f_n,\ *n+1\, A \rightarrow *n+1\, B$
$f_n \rightarrow *n[A \Rightarrow B]$

$\Rightarrow \rightarrow$ $f_m \rightarrow *m\, A;\ *m\, B,\ g \rightarrow *n\, C$
$*i[A \Rightarrow B],\ g \rightarrow *n\, C$ if $f_m \subseteq g$ and $i \leqq m \leqq n$.

*mix $f_m \rightarrow *m\, A;\ g(M) \rightarrow *n\, C$
$f_{m'},\ g(0) \rightarrow *n\, C$ if $*m\, A \in g(M),\ \notin g(0)$, and $m \leqq n$.

Then A0c = A0d2. Let A0d1 contain all the rules of A0d2 except *mix. A0d2 = A0d1 by an argument similar to Theorem 48 of Kleene's ***Introduction to metamathematics,*** 1952. Thus A0a = A0d1, which leads to a decision procedure for A0. (*Received November 14, 1959.*) [This work is supported in part by the United States Navy (Bureau of Ships), and in part by the United State Army (Signal Corps), and the United States Air Force (Office of Scientific Research, Air Research and Development Command), and the United States Navy (Office of Naval Research).]

TRENCHARD MORE, Jr. *Negated implicational lattice A′3.*

Modus ponens (from A ⇒ B and A, infer B), recapitulation (B ⇒ C .⇒: A ⇒. B ⇒ C), A ⇒. B ⇒ C :⇒: A ⇒ B .⇒. A ⇒ C, and A ⇒ A define the affirmative system A0. A0 plus A & B .⇒ A, A & B .⇒ B, and A ⇒ B .⇒: A ⇒ C .⇒ [A ⇒. B & C] define A1. A0 plus A ⇒. A *or* B, B ⇒. A *or* B, and A ⇒ C .⇒: B ⇒ C .⇒ [A *or* B .⇒ C] define A2. A1 ∪ A2 = A3. A0 plus A ⇒ B .⇒ : A ⇒ ⌞B .⇒. A ⇒ C and A ⇒ B .⇒: ⌞A ⇒ B .⇒ B define A′0. A′0 ∪ A3 = A′3. These 12 schemata are independent. We say "lattice" because distributivity (A &. B *or* C :⇒: A & B .*or*. A & C) and modularity (A ⇒ C .⇒ [A *or* B .& C :⇒: A *or*. B & C]) fail in A3, A′3, and U. System U of my abstract this JOURNAL, vol. 23, p. 103, is A′3 plus A ⇒ ⌞⌞A, ⌞⌞A ⇒ A, and A ⇒ B .⇒. ⌞B ⇒ ⌞A. Let □A be A ⇒ A .⇒ A. Then □A ⇒ A, □A ⇒ □□A, A ⇒ B .⇒ □[A ⇒ B], and A ⇒ B .⇒. □A ⇒ □B are theorems of A0. Since A ⇒. B ⇒ B in A0, let A ⇒ ⇑ . Then □A ⇔. ⇑ ⇒ A. Since A & ⌞A .⇒ B in A′1, let ⊙ ⇒ A. Then □⌞A ⇔. A ⇒ ⊙ and □A .⇔. ⌞A ⇒ ⊙. The following are theorems: □B ⇒. A ⇒ B, □A ⇒: A ⇒ B .⇒ B, A ⇒. A ⇒ B :⇒: A ⇒ B, A ⇒ B .⇒: B ⇒ C .⇒. A ⇒ C, A ⇒. B ⇒ C :⇒ : □B ⇒. A ⇒ C of A0; □A ⇒: B ⇒. A & B, A & B .⇒ C :⇒: □A ⇒. B ⇒ C of A1; □A &. B *or* C :⇒: A & B .*or*. A & C, A ⇒ C .⇒ [A *or* B .& □C :⇒: A *or*. B & C] of A3; □A ⇒ ⌞⌞A, □⌞⌞A ⇒ A, A ⇒ B .⇒. □⌞B ⇒ □⌞A, □⌞A ⇒. A ⇒ B, A ⇒ ⌞A .⇒ ⌞A, □A ⇒ □⌞□⌞□A, □⌞□⌞□⌞□A ⇒ □⌞□A, □⌞□⌞□⌞A ⇒ □⌞□A of A′0; ⌞[A & ⌞A] of A′1; A *or* ⌞A, A ⇒ B .⇒. ⌞A *or* B, □⌞A *or* □B .⇒. A ⇒ B of A′2; □A &. ⌞A *or* B :⇒ B, □[A & ⌞B] ⇒ ⌞[⌞A *or* B], □⌞A *or* □B .⇒ ⌞[A & ⌞B] of A′3. None of the 18 formulas obtained from this list by deleting □ can be proved in A′3. The following formulas: A ⇒ □A, ⌞A ⇒ □⌞A, ⌞□A ⇒ □⌞□A, □⌞□⌞□A ⇒ □A, □⌞A ⇒ □⌞B .⇒. □B ⇒ □A, □A ⇒ □B .⇒ □A :⇒ □A, □A *or* ⌞A, A *or* □⌞A, □A *or* □⌞□A, □[⌞A *or* B] ⇒. A ⇒ B, A ⇒ B .⇒. □⌞A *or* □B, and □⌞[A & ⌞B] ⇒. □⌞A *or* □B cannot be proved in A′3. A′3 contains Heyting's intuitionistic calculus as a sublogic of formulas of the form □A, □B, . . ., where Heyting's negation ¬ corresponds to □⌞. A′3 has infinitely many negated modalities because the laws of double negation and contraposition fail. A′3 plus A &. B *or* C :⇒: A & B .*or*. A & C define A′4. Let ◇ be ⌞□⌞. Lewis's S4 = A′4. (*Received November 9, 1959.*)

ALAN ROSS ANDERSON and NUEL D. BELNAP, Jr. *A simple proof of Gödel's completeness theorem.*

F^{1**} has $^-$, $\vee$, $\exists x$, as primitive. A is a *disjunctive part* of A; if $B \vee C$ is a disjunctive part of A, so are B and C. $\phi(A)$ is a wff of which A is a disjunctive part. A is an *atom* of $\phi(A)$ if it is p, $\bar{p}$, $f(x_1, \ldots, x_n)$, $\overline{f(x_1, \ldots, x_n)}$. A is a *molecule* of $\phi(A)$ if it does not have the form $B \vee C$. A is an axiom if there are atoms B and $\bar{B}$ which are disjunctive parts of A. Rules: (1) $\phi(A) \to \phi(\bar{\bar{\bar{A}}})$; (2) $\phi(\bar{A})$, $\phi(\bar{B}) \to \phi(\overline{A \vee B})$; (3) $\phi(Ax) \vee \exists yAy \to \phi(\exists yAy)$; (4) $\phi(\overline{Ax}) \to \phi(\overline{\exists yAy})$; (5) alphabetic change of bound variable. (Usual conditions on variables). Without loss of generality, let A have no variables both bound and free, and let V be the set of variables $v_1, \ldots, v_i, \ldots$ (in alphabetic order) not occurring bound in A. **B** is a *full normal branch* of a deduction tree for A if A is the first member A_1 of **B**, and for each A_i in **B**, (i) if A_i is an axiom, or has no non-atomic molecules, then A_i is the terminus of **B**; (ii) otherwise A_i has the form $\phi(B)$, where B is the leftmost non-atomic molecule, and: if B is $\bar{\bar{C}}$ $\{\overline{C \vee D}$; $\exists yCy$; $\overline{\exists yCy}\}$, then A_{i+1} is $\phi(C)$ {either $\phi(\bar{C})$ or $\phi(\bar{D})$; $\phi(Cv_j) \vee \exists yCy$, where v_j is the first variable in V such that Cv_j does not occur as a disjunctive part of any of $A_1, \ldots, A_i$; $\phi(\overline{Cv_j})$, where v_j is the first variable in V not occurring free in $A_1, \ldots A_i$}.

Lemmas. If **B** is a full normal branch for A not terminating in an axiom, then (I) there are no atoms B and $\bar{B}$ both of which are disjunctive parts of **B**; and (II) if

$B \vee C$ $\{\overline{\overline{B}}$; $\overline{B \vee C}$; $\exists y By$; $\overline{\exists y By}\}$ is a disjunctive part of $\mathbf{B}$, then so are B and C $\{B$; either $\overline{B}$ or $\overline{C}$; Bv_i for every v_i in V; Bv_i for some v_i in V$\}$.

Theorem. If $\mathbf{B}$ is a full normal branch for A not terminating in an axiom, then for the following system of values of the free variables of $\mathbf{B}$, every disjunctive part of $\mathbf{B}$ (and in particular A) assumes the value falsehood: to p give f iff p is an atom of $\mathbf{B}$; to v_i give i; to n-ary f give the function taking $(i_1, \ldots, i_n)$ into f iff $f(v_{i_1}, \ldots, v_{i_n})$ is an atom of $\mathbf{B}$.

It follows that F^{1**} is complete. For if every branch for A terminates in an axiom, A is a theorem. If not, the theorem guarantees that A is not valid. (*Received September 1, 1959.*)

J. C. E. DEKKER and J. MYHILL. *The divisibility of isols by powers of primes.*

For notations and terminology see ***Mathematische Zeitschrift,*** vol. 70 (1958), pp. 113–124 and 250–262. Let $\varepsilon = (0, 1, \ldots)$ and let $\bar{\varepsilon}$ be obtained by adjoining the symbol ∞ to ε. The positive primes are arranged according to size in the sequence $\mathbf{p}_0, \mathbf{p}_1, \ldots$. This paper originated with the following *question*: "Does there exist for each function $\mathrm{v}(\mathbf{n})$ from ε into $\bar{\varepsilon}$ an isol X such that (1) if $\mathrm{v}(\mathbf{n}) \neq \infty$, X is divisible by $\mathbf{p}_{\mathbf{n}}^{\mathrm{v}(\mathbf{n})}$, but not by $\mathbf{p}_{\mathbf{n}}^{\mathrm{v}(\mathbf{n})+1}$, and (2) if $\mathrm{v}(\mathbf{n}) = \infty$, X is divisible by $\mathbf{p}_{\mathbf{n}}^{\mathbf{k}}$ for every $\mathbf{k}$ in ε?" The answer to this question is affirmative. This is a corollary of *Theorem* 1. For each function $\mathrm{V}(\mathbf{n})$ from ε into Λ there exists an isol which for every $\mathbf{n}$ in ε is divisible by $\mathbf{p}_{\mathbf{n}}^{\mathrm{V}(\mathbf{n})}$, but not by $\mathbf{p}_{\mathbf{n}}^{\mathrm{V}(\mathbf{n})+1}$.

An isol X is *cosimple* if X = Req (ξ) for some set ξ with a recursively enumerable complement. A sequence $\{\mathrm{V}(\mathbf{n})\}$ of cosimple isols is *recursively enumerable* (r.e.) if $\mathrm{V}(\mathbf{n})$ = Req $(\omega'_{\mathrm{f}(\mathbf{n})})$ for some recursive function $\mathrm{f}(\mathbf{n})$. *Theorem* 2. For each r.e. sequence $\{\mathrm{V}(\mathbf{n})\}$ of cosimple isols there exists a cosimple isol which for every $\mathbf{n}$ in ε is divisible by $\mathbf{p}_{\mathbf{n}}^{\mathrm{V}(\mathbf{n})}$, but not by $\mathbf{p}_{\mathbf{n}}^{\mathrm{V}(\mathbf{n})+1}$.

Side results. For each sequence of isols there exists an isol which is divisible by every isol in that sequence. For each r.e. sequence $\{$Req $(\omega'_{\mathrm{f}(\mathbf{n})})\}$ of cosimple isols there exists a cosimple isol which is divisible by every isol in that sequence; in fact, given the recursive function $\mathrm{f}(\mathbf{n})$, we can effectively find a number k such that Req $(\omega_{\mathbf{k}}')$ satisfies the requirements. (*Received August 11, 1959.*)

RONALD HARROP. *Concerning formulas of the types $A \rightarrow. B \vee C$, $A \rightarrow (Ex)B(x)$, in intuitionistic formal systems.*

By using methods similar to those employed by the present author in the paper '*On disjunctions and existential statements in intuitionistic systems of logic*' (XXIII 345), cited here as DES, some results have been obtained related to those reported by Kreisel in his paper on '*The non-derivability of $\neg(x)A(x) \rightarrow (Ex)\neg A(x)$, A primitive recursive, in intuitionistic formal systems*' (see abstract — this JOURNAL, vol. 23 (1958) p. 456). The suggestion that it might be worth considering the possibility of such application of the ideas of DES was made to the author by Kreisel in correspondence.

Consider intuitionistic elementary number theory $\mathbf{N}$ as defined by Kleene in his ***Introduction to metamathematics.*** Let U be an arbitrary formula of $\mathbf{N}$. Using the terminology of DES, consider the smallest set $\mathscr{S}$ of formulas such that (i) each conjuctand of U is in $\mathscr{S}$, (ii) if $E \rightarrow F$ is in $\mathscr{S}$, then so is F^* for each conjuctand F^* of F, (iii) if G is in $\mathscr{S}$, then so is each conjunctand of a particular case of G. A formula U is said to contain a relevant occurrence of $\vee$ if at least one element of $\mathscr{S}$ has $\vee$ as its main connective and to contain a relevant occurrence of an existential quantifier if at least one element of $\mathscr{S}$ begins with an existential quantifier.

The main results proved are that if U, V, W, $(Ex)Z(x)$ are closed formulas and U has no relevant occurrences of $\vee$ or of existential quantifiers, then

(i) $U \rightarrow. V \vee W$ is provable in $\mathbf{N}$ if and only if at least one of $U \rightarrow V$, $U \rightarrow W$ is provable in $\mathbf{N}$,

(ii) $U \rightarrow (Ex)Z(x)$ is provable in **N** if and only if, for some numeral n, $U \rightarrow Z(n)$ is provable in **N**.

The corresponding result for intuitionistic propositional calculus **P**, namely that $U \rightarrow .\ V \vee W$ is provable in **P** if and only if at least one of $U \rightarrow V$, $U \rightarrow W$ is provable in **P**, leads to several short demonstrations of the unprovability in **P** of formulas which are provable in classical propositional calculus. (*Received October 28, 1959.*)

G. Kreisel. *Reflection principle for subsystems of Heyting's* (first order) *arithmetic* (H).

A formula $T^*(a)$ is a *normal truth definition* (n.t.d.) or, better, a *normal enumeration* of a subsystem H^* of H if the (usual arithmetisation of the) following statements can be proved in H: if $\ulcorner A \urcorner$ is the Gödel number of A, (i) for each propositional connective $\circ$ and variables $\ulcorner A \urcorner$, $\ulcorner B \urcorner$, $T^*(\ulcorner A \circ B \urcorner) \leftrightarrow .\ T^*(\ulcorner A \urcorner) \circ T^*(\ulcorner B \urcorner)$, (ii) for each quantifier (Qx), $T^*[\ulcorner (Qx)A(x) \urcorner] \leftrightarrow (Qx)T^*[\ulcorner A(0^{(x)}) \urcorner]$, (iii) for (each of the finite set of) non-logical axioms A of H^*, $T^*(\ulcorner A \urcorner) \leftrightarrow A$. For instances I of the induction schema in H^*, $T^*(\ulcorner I \urcorner)$ is then provable in H. We define the *complexity* of a formula A *as the sum of the number of connectives and distinct quantifiers* of A. *Theorem. For each* n, *there is an n.t.d. for the system* H_n *consisting of all formulae of complexity* n. Corollary (Reflection principle). For each term $\tau(x)$ of H, $\vdash (x)(Ey)\mathrm{Prov}_n(y, \ulcorner A(0^{(\tau(x))}) \urcorner) \rightarrow (x)A[\tau(x)]$, where $\mathrm{Prov}_n(y, \ulcorner A \urcorner)$ is the (natural) arithmetization of: y is the number of a proof in H_n of A. *Application.* If $\vdash (x)(Ey)A(x, y)$ there is an e such that, for Kleene's T predicate, $\vdash (x)(Ey)T(e, x, y)$ and $\vdash (x)(y)[T(e, x, y) \rightarrow A(x, y)]$. For the proof, we use Harrop's [***Math. Ann.*** vol. 132, (1956), 347–361]: if $\vdash (Ey)A(y)$ and y is the only free variable in $A(y)$, then for some p, also $\vdash A(0^{(p)})$. Analysis of his argument shows (i) the complexity of the proof of $A(0^{(p)})$ given by his method depends uniformly on that of the given proof of $(Ey)A(y)$ and (ii) the metamathematical argument can be formalized in H itself. Now, if $\vdash_n (x)(Ey)A(x, y)$, also $\vdash_n (Ey)A(0^{(x)}, y)$, and by (i) and (ii), for a provably recursive $\tau(x)$ i.e. $\iota_y T(e, x, y)$, also $\vdash_{n'} A[0^{(x)}, 0^{(\tau(x))}]$, and, in fact, $\vdash (x)(Ey)\mathrm{Prov}_{n'}[y, \ulcorner A(0^{(x)}, 0^{(\tau(x))}) \urcorner]$. By the corollary $\vdash (x)A[x, \tau(x)]$, i.e. $(x)A[x, \iota_y T(e, x, y)]$, as required. *Remark.* In [***Fundamenta mathematicae,*** vol. 42, (1955), 101–110)] n.t.d. were given for subsystems Z_n of classical first order arithmetic Z; in particular, for complexity k of A determined by the maximum length of chains of interlocked quantifiers x_{n_i}, $1 \leqq i \leqq k$, of A, where x_{n_i} is in the scope of $x_{n_{i+1}}$, $i < k$. Here the complexity is independent of the number of propositional connectives. This definition seems unsuitable for intuitionistic arithmetic because iterated implications cannot be contracted. (*Received October 25, 1959.*)

G. Kreisel. *Proof by transfinite induction and definition by transfinite induction in quantifier-free systems.*

We consider the usual formulation of primitive recursive arithmetic (successor symbol $'$, function symbols f, $=$) with (a) rules of the elementary calculus with free variables, (b) axioms for successor and equality, (c) the 'defining equations' of primitive recursive form (as axioms) so arranged that the defining equations for the auxiliary function symbols in the definition of f_n occur among $f_1, \ldots, f_{n-1}$, (d) the schema of complete induction applied to formulae in the given notation. It is known that neither definition by induction (c) nor proof by induction (d) is reducible to the other since the theorems of (a), (b), (c) and (a), (b), (d) are incomparable. We extend the notation by adding function symbols φ and ψ, and for a given primitive recursive relation $a \prec b$, with $0^{(n)} \not\prec 0$ for each n, we add the following schemata: (c'_φ) $\varphi_n(0) = \alpha$, $\varphi_n(x') = \chi\{x, \varphi_n[\tau^*(x)]\}$ where $\tau^*(x) = \tau(x)$ if $\tau(x) \prec x'$, $\tau^*(x) = 0$ if $\tau(x) \not\prec x'$ (and so $\tau^*(0) = 0$), (c'_ψ) $\psi_n(m, 0) = \alpha$, $\psi_n(m, x') = \chi[m, x, \psi_n(m, x)]$, and α, χ, τ are built up from $f_i, \varphi_1, \ldots, \varphi_{n-1}, \psi_1, \ldots, \psi_{n-1}$. (d$'$) For each A and τ in this notation, derive $A(n)$ from $A(0)$ and $A[\tau^*(n)] \rightarrow A(n)$. Note that if $\prec$ is a well ordering, (c$'$) expresses *definition by transfinite induction* (t.i) and (d′) *proof* by t.i. *Theorem*: *Each instance of* (*d′*) *is derivable by* (*a*)–(*d*), (*c′*), when (d) is applied to all formulae in the extended notation, i.e. proof by t.i. is *reduced* to definition by t.i. . Given τ, by (c'_ψ) we define the descending sequence $\psi(n, 0) = n$, $\psi(n, x') = \tau^*[\psi(n, x)]$. By (c'_φ) we define the 'length' φ of this sequence, $\varphi(0) = 0$, $\varphi(x') = \varphi[\tau^*(x)]'$, whence $\varphi(x) = 0 \rightarrow x = 0$. By (d), $\psi(n, x) \neq 0 \rightarrow \varphi[\psi(n, x)] + x = \varphi(n)$. Putting $x = \varphi(n)$, $\psi[n, \varphi(n)] = 0 \vee \varphi\{\psi[n, \varphi(n)]\} = 0$, i.e. $\psi[n, \varphi(n)] = 0$, i.e. $\varphi(n)$ is the length of the descending part of $\tau^*(n)$, $\tau^*[\tau^*(n)]$, $\ldots$, etc. Suppose $\mathrm{A}[\tau^*(x)] \rightarrow \mathrm{A}(x)$; then $\mathrm{A}[\psi(n, x')] \rightarrow \mathrm{A}[\psi(n, x)]$ and so $\{\neg\mathrm{A}[\psi(n, 0)] \rightarrow \neg\mathrm{A}[\psi(n, x)]\} \rightarrow \{\neg\mathrm{A}[\psi(n, 0)] \rightarrow \neg\mathrm{A}[\psi(n, x')]\}$, whence, by (d), $\neg\mathrm{A}(n) \rightarrow \neg\mathrm{A}[\psi(n, x)]$. Put $x = \varphi(n)$, and so $\mathrm{A}(0) \rightarrow \mathrm{A}(n)$, as required. *Application*: In the author's quantifier-free system F_1 [this JOURNAL, vol. 17 (1952), p. 47, para. 38] the schema for 'ordinal induction of finite order' can be replaced by the ordinary schema of complete induction. *Remark* 1. The parallel question of dropping (c′) in favour of (d′) is somewhat artificial because then the φ_n would not be identified. *Remark* 2. The argument can be iterated for relations $\mathrm{a} \prec \mathrm{b}$ in the new notation. (*Received October 25, 1959.*)

SAUL A. KRIPKE. *Distinguished constituents.*

The device of "distinguished" constituents of Ackermann XXII 327(2) can be adapted to the problem, posed in Curry's XVI 56, of finding a formulation of his LD satisfying the Gentzen subformula principle. We allow plural right sides, with some constituents distinguished; the primes have form X, A $\Vdash$A, Z^*. The positive part of the system is like LC, with the principal constituents not distinguished. For Pr (and Πr if present) we assume that all parametric constituents on the right are distinguished (the "strong" restriction). Nr is as in LK; Nl is also as in LK, but with the restriction that there must be a parametric, negated, non-distinguished constituent on the right. We adopt a rule Dr, subject to the same restrictions as Nl, allowing a non-distinguished constituent to become distinguished. A rule Dr′, allowing us to make a distinguished constituent non-distinguished at will, completes the new LD system.

If we weaken the restriction on Pr (and Πr) to assert that all parametric constituents on the right are distinguished or negated, the result is LG; HG is characterized by adding $\neg\neg(\neg\neg\mathrm{A} \supset \mathrm{A})$ to HD. If we drop the notion of distinguished constituents from LD (or LG), the result is LE ("classical refutability", cf. XXII 330 (4), axioms 1–11). The positive part of LD gives a plural LA; this can be extended to plural versions of LM and LJ. Define LAV (LCV) by adding negation as a *verum* operator to LA (LC). Then LE = LCV $\cap$ LK, LG = LAV $\cap$ LK. Using distinguished constituents, we can also define LB = LAV $\cap$ LJ (HB = HM + $\neg\neg(\neg\neg\mathrm{A} \supset \mathrm{A})$). All these systems have certain variant formulations using distinguished constituents, as well as singular, T, and H formulations. Throughout $A_1, \ldots, A_m \Vdash B_1, \ldots, B_n, C_1^*, \ldots, C_p^*$ can be interpreted as $A_1 \wedge \ldots A_m .\supset. B_1 \vee \ldots B_n :\vee: C_1 \vee \ldots C_p$ (in LD, equivalently: $A_1 \wedge \ldots A_m \wedge \neg C_1 \wedge \ldots \neg C_p .\supset. B_1 \vee \ldots B_n$). We obtain generalized Glivenko theorems, and, of course, elimination theorems. (*Received September 1, 1959.*)

SAUL A. KRIPKE. *Semantical analysis of modal logic.*

Semantical completeness theorems are now available for various systems of modal logic, using an appropriate model-theory to define completeness for each system, and using Beth's semantic tableaux to facilitate the proof. The systems involved are: (1) Lewis's S2, S3, S4, S5; Feys- Von Wright's M; Lemmon's E2, E3, E4, E5′ (XXIII 346); related systems intermediate between S2 and M; systems using the *Brouwersche* axiom; S6, S7, S8; various systems of deontic logic; modifications in the direction of Prior's Q. These methods lead to simple decision procedures, infinite matrices, natural deduction methods, etc., for all systems mentioned. (2) Quantifiers can be added, with completeness theorems preserved. The axiom $(x)\Box A \supset \Box(x)A$ turns out to hold when there are no "possible existents" beyond the individuals of the real world. The problems regarding necessary existence raised by Prior can be solved by several approaches, including systems like his Q, and alternatives to this. (3) If identity is added, completeness theorems can be derived either on the assumption $(x, y)\ (x = y \supset \Box x = y)$ or without this assumption. The resulting semantical notions shed new light on questions such as the morning star paradox, and provide a semantical apparatus for sense and denotation, extension and intension, and related concepts. (4) The methods for S4 yield a semantical apparatus for Heyting's system which simplifies that of Beth. They also suggest certain metamathematical applications of modal logic. (For systems based on S4, S5, and M, similar work has been done independently and at an earlier date by K. J. J. Hintikka.) *(Received October 21, 1959.)*

SAUL A. KRIPKE. *The problem of entailment.*

Consider the pure implication part of Curry's LK (as in his ***Theory of formal deducibility,*** but with K as postulated rules, and primes of form A ||- A only.) The resulting "material implication" is "paradoxical". We eliminate some paradox by restricting Pr to be singular on the right; this yields LJ. If we restrict LJ by abandoning the rules K, we get Church's weak implication. If we restrict Pr in LJ so that all parametric constituents are of form $C \supset D$, we get the pure implication part of S4. If we apply *both* restrictions on Pr to LJ, we get a formulation of I (defined by Belnap from (1)–(4), α and δ, in Ackermann XXII 327). For all these systems, the elimination theorem holds. The decidability theorems are problematic in the absence of K, since the usual methods depend on the presence of the converse of W; but this difficulty has been circumvented by a more general argument not requiring this rule, yielding in particular decision procedures for I and weak implication.

If we wish to add other connectives (conjunction, disjunction, negation, quantification) various alternative sets of rules can be used, which, although equivalent in the presence of K, are not equivalent in its absence.

The rule K was dropped because it allowed the introduction of "irrelevant" constituents. If we are interested in a "minimal logic" (Church), we might consider dropping the rules W, or placing even stronger restrictions on Pr. (My thanks to A. R. Anderson and Nuel D. Belnap for stimulating my interest in these problems.) *(Received October 21, 1959.)*

W. V. QUINE. *Eliminating variables without applying functions to functions.*

Schönfinkel's elimination of variables used functions which applied to themselves and one another. A general set-theoretic ontology seems called for to house these objects. I shall show, in contrast, how to eliminate variables by adopting six functors which operate iteratively on the primitive predicates, whatever they may be, to yield predicates defined over the original universe alone. The functors are: (1) *Complementation.* Applied to an n-place predicate, it gives the complementary n-place predicate. (2) *Cartesian multiplication.* Applied to an m-place predicate and an n-place predicate, it gives the $(m + n)$-place predicate which the name suggests. (3) *Extreme permutation.* Applied to a predicate of $n > 1$ places, it gives a predicate satisfied by the n-tuples which we get from those satisfying the original predicate when we permute their initial places to final position. (4) *Penultimate permutation.* Similar, but with penultimate places permuted to initial position. (5) *Fusion.* Applied to a predicate of $n + 1$ places, it gives a predicate satisfied by those n-tuples which, with their last place repeated, satisfy the original predicate. (6) *Projection.* Applied to a predicate of $n + 1$ places, it gives a predicate satisfied by the n-tuples obtainable by curtailing the $(n + 1)$-tuples which satisfy the original predicate. Applied to a one-place predicate 'F' it yields a sentence to the effect that $(Ex)Fx$.

Consider any theory, standardized thus: there are just its primitive predicates and notations for existential quantification, conjunction, and negation. Adding the six functors as further notation, we rid any formula of any innermost quantifier and its variable as follows. First we export from the quantification any predications lacking the variable of the quantifier. This can be done for innermost quantifications by familiar transformations. Then we rewrite the surviving scope of the quantifier as a single predication, with a complex predicate formed from the old predicates by applying complementation and Cartesian multiplication in parallel to the original structure in terms of negation and conjunction. To this complex predicate we apply the functors of permutation and fusion, each time conformably adjusting the appended sequence of argument variables, until the only occurrences of the variable of quantification are the one in the quantifier and one at the end; this can always be done. Finally, by projection, we eliminate the quantifier and that terminal occurrence. By getting rid thus of all innermost quantification and so working outward, we get rid of all quantifiers and variables. (*Received November 17, 1959.*)

W. W. TAIT. *A characterization of ordinal recursive functions.*

The (Gödel) primitive recursive functionals of finite type are defined by the following schemata: I. $\varphi(\mathfrak{B}) = 0$; II. $\varphi(\alpha, \mathfrak{B}) = \alpha$; III. $\varphi(\mathrm{n}, \mathfrak{B}) = \mathrm{n} + 1$; IV. $\varphi(\mathfrak{B}) = \lambda\alpha\psi(\alpha, \mathfrak{B})$; V. $\varphi(\alpha, \mathfrak{B}, \mathfrak{C}) = \alpha(\mathfrak{B})$; VI. $\varphi(\mathfrak{B}) = \psi(\mathfrak{B}_\pi)$; VII. $\varphi(\alpha, \mathfrak{B}) = \chi[\psi(\alpha, \mathfrak{B}), \mathfrak{B}]$; and the recursion schema VIII. $\varphi(0, \mathfrak{B}) = \psi(\mathfrak{B})$, $\varphi(\mathrm{n} + 1, \mathfrak{B}) = \chi[\mathrm{n}, \varphi(\mathrm{n}, \mathfrak{B}), \mathfrak{B}]$ — where α and $\mathfrak{B}$ are, respectively, a variable and a list of variables (of the appropriate types), ψ and χ are functional constants and $\mathfrak{B}_\pi$ is a permutation of the list $\mathfrak{B}$. Gödel has shown that every ordinal recursive function is a PR functional, and by a result of Kreisel, the converse is established: A. Every PR functional of type (0, 0) is ordinal recursive. We establish A by a method more direct than Kreisel's and one which, moreover, promises interesting extensions — e.g. B. Every function definable by means of I–VIII and the fan theorem functional:

$$\varphi(\alpha^2, \alpha^1) = \mu y[(\beta^1)_{\leq\alpha'}(\gamma^1)_{\leq\alpha'}\{(x)_{\leqq y}[\beta^1(x) = \gamma^1(x)] \rightarrow \alpha^2(\beta^1) = \alpha^2(\gamma^1)\}],$$

is ordinal recursive.

Call a term *normal* if it is a variable (of any finite type), a numeral, or is of one of the forms $\lambda\alpha.\sigma$ where σ is normal, $\sigma_0(\sigma_1, \ldots, \sigma_p)$ where $\sigma_0, \sigma_1, \ldots, \sigma_p$ are normal or $\varphi(\sigma_1, \ldots, \sigma_p)$ where φ is a PR functional constant (with a given PR definition) and $\sigma_1, \ldots, \sigma_p$ are normal terms. A term τ' is called a *reduction* of a term τ if it is obtained by replacing a normal part σ of τ by σ', where (a) $\sigma = \sigma'$ is an instance of one of I–VII, (b) σ is of the form $\varphi(\mathrm{n}, \mathfrak{B})$, where φ is defined by VIII, and σ' is $\chi[n, \chi[n - 1, \ldots, \chi[0, \psi(\mathfrak{B}), \mathfrak{B}], \ldots, \mathfrak{B}], \mathfrak{B}]$, or (c) σ is $(\lambda\alpha\rho(\alpha))(\pi)$ and σ' is $\rho(\pi)$. τ' is called a *derivative* of τ if it is obtained from τ by a sequence of reductions. C. If τ is a derivative of a normal term $\varphi(n)$, then either τ has a reduction or else it is a numeral. D. We can assign ordinals $< \varepsilon_0$ to the terms in such a way that, if τ is a derivative of a normal term $\varphi(n)$, then its reduction has a smaller ordinal than has τ. From C and D, we obtain A in the form: If φ is a PR functional of type (0, 0), htere is an ordinal $\xi < \varepsilon_0$ and primitive recursive *functions* θ and χ and γ such that, for every n, $\theta(n + 1) \underset{\xi}{<} n + 1$ (where $\underset{\xi}{<}$ is the standard ordering of type ξ of the non-negative integers) and

$$\text{for } \psi(0) = \mathrm{K},\ \psi(\mathrm{n} + 1) = \chi[\mathrm{n}, \psi(\theta(\mathrm{n} + 1))],\ \varphi(\mathrm{n}) = \psi(\gamma(\mathrm{n})).$$

By vote of the Executive Committee it has been decided to discontinue the service available to European members of paying dues in the currency of Belgium or The Netherlands. Beginning March 31, 1961 all payments are to be made in dollars to: The Association for Symbolic Logic, 190 Hope Street, Providence 6, Rhode Island, U.S.A.

There will be a meeting of the Association for Symbolic Logic at the Hotel Willard, Washington, D.C., on Tuesday, January 24, 1961, in conjunction with a meeting of the American Mathematical Society. The chairman of the Program Committee is Professor David Nelson, Department of Mathematics, The George Washington University, Washington 6, D.C. Members desiring to present papers should submit abstracts in duplicate to the chairman.

A SYMPOSIUM ON RECURSIVE FUNCTIONS, jointly sponsored by the Association for Symbolic Logic, the Association for Computing Machinery, and the American Mathematical Society, with financial support from project FOCUS of the Institute for Defense Analyses, will be held at the Hotel New Yorker in New York City, on April 6 and 7, 1961 in connection with the April meeting of the American Mathematical Society at which time, from April 6–8, there will also be a symposium on Mathematical Problems in the Biological Sciences.

Three sessions ar planned for the symposium on recursive functions, the first two on the notion of recursive function and traditional applications, and the third on such newer applications as to computing, automata, and problem solving.

The Organizing Committee of the Symposium consists of Professors S. C. Kleene (University of Wisconsin), Chairman; J. B. Rosser, (Cornell University), J. C. E. Dekker, (Rutgers, the State University), Joseph R. Shoenfield, (Duke University) and John McCarthy, (Massachusetts Institute of Technology). The Symposium will contribute to and be a continuation of the reports in the same general field as last year's Symposium on the Structure of Languages.

Programs of the two Symposia will appear in the December 1960 issue of the NOTICES of the American Mathematical Society.