536
Notre Dame Journal of Formal Logic
Volume 28, Number 4, October 1987

Variations on a Thesis: Intuitionism and Computability

CHARLES McCARTY*

1 Prelude The theme of this paper is Church's Thesis (or CT) as it is normally understood by intuitionists and by logicians concerned with constructivity. This is to be distinguished from the more familiar "quasi-empirical" statement of the same name—that

every mechanically computable function is general recursive.

Rather, we will use CT to denote one or another version of the intuitionistic mathematical statement that

every total natural number function is general recursive.

There are three variations. The first is an extended argument for a reappraisal of the status of CT within intuitionism. Traditionally, the intuitionists' attitude toward CT has been strongly negative; it was thought that Church's Thesis was obviously false. The fact that it is consistent with the main bulk of constructive mathematics was either to be deplored or ignored.

We think this attitude unfortunate. As it seems to derive a good part of its impetus from an unnecessary identification of intuitionism with *reductive intuitionism*, we devote the bulk of the first variation to suggesting that reductive intuitionism might itself be either deplored or ignored.

Of course, the idea that CT is obviously false can be reinforced from other quarters. Logicians often appeal to a kind of hypothetico-deductivism and argue that CT is false because its mathematical consequences are largely untoward. The

*We are grateful to the Philosophy Departments of the Ohio State University and of the Florida State University for opportunities to present material from this paper. Judith George, Steve Harris, Jaakko Hintikka, Hilbert Levitz, Barbara Scholz, George Schumm and Stewart Shapiro deserve special thanks for their various individual contributions.

Received August 24, 1987

idea of the second variation is that the testimony of negative consequences is inconclusive; CT entails some highly attractive results. We will describe the proofs of three: Brouwer's Theorem for constructive information systems, the categoricity of intuitionistic first-order arithmetic and the existence of a small complete category.

Third, classical mathematicians can and have entertained any number of their own variations on (the empirical form of) Church's Thesis, each arising from a description of an abstract mechanical computing device. The proofs that many of these variations are extensionally coincident provide a form of evidence for CT. Clearly, an intuitionist can consider the same variations and can even accept the associated evidence for ordinary CT, since all the proofs involved are constructive. However, this sort of evidence is inconclusive; its persuasive force is limited by the severe logical constraints set upon classical mathematics.

There are reasonable variations on CT which the intuitionist can entertain but which are classically unavailable. These also come from making more subtle alterations on Turing's concept of machine. We will show that these coincide with standard Turing machines only under assumptions which are independent of the axioms of traditional intuitionistic mathematics. Therefore, the intuitionist has ready access to intelligible and rigorous versions of the notion of computable function which fail to coincide extensionally with those of Church and Turing.

2 Variation I: How to be an intuitionist

2.1 Orientation Before setting off officially, it would be best to say something about our basic orientation. This will preclude later misunderstanding.

I am an intuitionist, at least as far as mathematics is concerned. But that does not mean that I am a constructivist, at least in the sense in which the title is usually conferred. Unlike the constructivist, the intuitionist prefers a mathematics at variance with the classical. To put it another way, I live my mathematical life in happy sympathy with Brouwer's idea that there is great virtue in the investigation of certain forms of mathematics which differ radically from comfortable traditions. Brouwer's alternative mathematics is based upon principles which are neither merely nonstandard nor momentarily exhilarating, as have been various axioms of large cardinals. Admittedly, if these principles are taken in a superficial way, they will seem absurd; in fact, they seem to offend one's most ingrained mathematical sensibilities. But this appearance is completely superficial and dissolves under the more subtle logical methods of the intuitionist. In this context, one does well to recall Hobbes' definition of *paradox* as *an opinion not yet generally received.*[1]

I would not deign to argue that an intuitionistic approach to mathematics is *the only* correct one. For starters, it is difficult to see how such an argument could proceed. The standard of correctness for the steps of the argument would have to be determined at the outset. But, to do that, we would already have to decide whether intuitionistic or classical standards are the more appropriate. My immediate goals are much more limited—to argue that intuitionistic mathematics is as scientifically functional and foundationally attractive as any of the classical alternatives. For that, it will suffice to point out the lively mathematical vistas incorporated within intuitionism's foundational view. The bulk of the present paper is devoted to some sketches of intuitionistic landscapes in the region of computation theory.

Although my sympathies lie with Brouwer, my loyalties need not be wholly undivided. I cannot agree with him that many of the innocent mathematical assertions of classical mathematicians are either meaningless or false. There is, of course, the naive reinterpretation of classical mathematics on which the traditional logical signs are replaced by their intuitionistic counterparts. Needless to say, this interpretation makes classical mathematics demonstrably false. On the naive interpretation, the axioms of intuitionistic mathematics contradict classical theorems.

Even so, I can still exercise a form of criticism. According to the way in which I would prefer to understand classical mathematics, it is lacking neither truth nor sense but only imagination. I prefer to see classical mathematics as intuitionistically true and intelligible by giving it a Gödel–Gentzen interpretation and mapping it semantically into the *hereditarily stable* portion of the intuitionistic mathematical universe. Suffice it to say that, under stabilization, the positive classical connectives

$$\ldots \vee \ldots \text{ and } \ldots \exists \ldots$$

are replaced by their doubly negated counterparts

$$\neg\neg(\ldots \vee \ldots) \text{ and } \neg\neg(\ldots \exists \ldots).$$

The logical result of the replacement is that interpreted statements of classical mathematics turn out to be true but only boringly so—thanks to the fact that stabilized expressions are prohibited any meaningful interchange with the sorts of computable mathematical evidence which form the very essence of the intuitionistic approach. (The relation between a completely stabilized object and the evidence for its existence is always trivial. In the terminology soon to be introduced, if P and a are hereditarily stable and if p is any probject (proof object) showing that $P(a)$, then we can assume that $p = 0$). By contrast with the regions of the intuitionistic universe which contain the exciting prospects to be surveyed in Variation II, the domain of hereditary stability is a mathematical suburbia which is ponderously dull. (Full technical details of the interpretation can be gleaned from [1], [10], or [28].)

2.2 Reductionism and realism There are at least two approaches to the foundations of intuitionistic mathematics. One is broadly "reductionist" while the other is—for lack of a better term—"realist". Reductionism has been very popular, especially among the ontologically thrifty and semantically conservative. For such individuals, it offers an attractive countenance in league with a whiff of racy excitement. Until quite recently, the goal of a great many of the investigations into the foundations of constructive mathematics has been the improvement of the intelligibility and maintenance of the attractions of the reductionistic approach.

The desire for reductionistic intuitionism gets its urgency from the desire for a full, higher-order mathematics which does not rely for its foundations upon stock Platonistic metaphysics. The statements of mathematics are to be reduced to more-or-less everyday statements about more-or-less ordinary mathematical proofs together with our knowledge of and capacities for manipulating them. The propositions expressed by sentences of intuitionistic mathematics are not properly interpreted as making the usual pronouncements about numbers, sets and functions, conceived as the somewhat unworldly denizens of an extraworldly reality. Instead, they are supposed to tell complicated but sundry tales about *constructions*—those operations which we can and do perform in building (what purport to be) representations of numbers, sets and functions. To quote Dummett,

> On an intuitionistic view . . . , the only thing that can make a mathematical statement true is a proof of the kind we can give: not, indeed, a proof in a formal system, but an intuitively acceptable proof, that is, a certain kind of *mental* construction. [Mathematical objects] exist only in virtue of our mathematical activity, which consists in mental operations, and have only those properties which they can be recognized by us as having. ([5], p. 7)

Reductionistic intuitionism, if attainable, would be a form of *scientific antirealism*; the metaphysical urge to posit lonely, timeless and causally inert realms of mathematical fact is supposed to vanish with the success of the reduction.

As with other reductionistic proposals, such as psychological behaviorism, reductionistic intuitionism is purported to entail a form of *semantical antirealism*. It is thought that the principle of bivalence and the logical law of the excluded third (or TND) would fail to be universally valid. The reasons for the failure are thought to be simple and straightforward. According to the reductionist, the usual statement of Riemann's Hypothesis (RH) is a mere shorthand for a statement about proofs. For example, the textbook formulation of RH is short for something like "A proof of RH is available to me".[2] So, RH will be true only if there is available a proof of RH and likewise for its negation. Replacing ϕ in TND,

$$\phi \vee \neg\phi,$$

by RH, we obtain

$$\mathrm{RH} \vee \neg\mathrm{RH}.$$

Intuitionistically as classically, a disjunction will be true only on the condition that one of its disjuncts is. Therefore, for RH $\vee$ $\neg$RH to be true, we need have at our disposal either a proof of Riemann's Hypothesis or a refutation of it. As it happens, we have neither. Hence, the law of the excluded third fails.

No one has supposed that the route to reductionism is clear sailing but many have thought that the trip would be a success. We would prefer not to be so sanguine: the route is fraught with hazards the rigors of which are not universally appreciated. The next few sections afford a chart of the most prominent obstacles, those associated with (i) mathematical solipsism, (ii) idealization, (iii) intuitionistic proof, and (iv) intuitionistic truth. It is not our contention here that the difficulties are insurmountable. After all, unattainability does not always constitute an absolute prohibition: there is still a great deal to be learned from attempts to approximate the impossible ideals of the Hilbert Programme. Rather, it is our contention that reductionism is so troubled that alternative approaches to intuitionistic foundations be preferred.

A principle of total disclosure demands that we explain the immediate bearing of our remarks about reductionism. A reductionistic form of intuitionism is obviously inconsistent with well-diluted forms of CT. To enhance the plausibility of CT, one needs to argue the unacceptability of reductionism. The elimination of the possibility for unrecognized mathematical truths has to form a plank in the reductionist platform. Were there unrecognized truths, they must, according to the reductionist, be true in virtue of something other than our existing constructions. They could only be true in virtue of the subsistence of an independent realm of mathematical fact. So, when the intuitionist says that RH is true only if there is available a proof of RH, he means that there is a proof available to me of RH—one which I can take in and recognize as such. In fact, the idea is better expressed were we to say that RH is true only if there is a proof-available-to-me of RH. In order to rule out the possibility for unrecognized mathematical truths, the reductionist must insist that there be no such thing as a proof which might (or might not) be available to me and which serves as the truth condition for a mathematical statement. As far as proofs go, there are only those I can completely construct.

Now, consider a constructive theory of elementary syntax, say, Robinson's Q formalized in intuitionistic predicate logic. Let $\mathfrak{F}$ be a standard formal theory which is intuitionistically sound and extends Q. Since each $\mathfrak{F}$ formula which is intuitionistically provable (and here we mean 'informally provable') can be recognized as such, we are able to enumerate the Gödel numbers of the provable formulas. That is, there is an intuitionistic number-theoretic function f whose range is the set of codes of provable formulas. The existence of f is inconsistent with the following weak form of CT, which we will call '$\mathfrak{F}$CT':

Every number-theoretic function is definable in $\mathfrak{F}$.

Given $\mathfrak{F}$CT, f is definable in $\mathfrak{F}$ and we can take $\mathrm{Bew}(m)$ to be the formal expression for the relation

$$\exists n f(n) = m.$$

Since $\mathfrak{F}$ is sound and extends Q, we are right to appeal to the formal fixed-point theorem and obtain a formula ϕ such that

$$\phi \leftrightarrow \neg \mathrm{Bew}([\phi]).$$

The reasoning of the First Incompleteness Theorem will now lead, from the assumption that intuitionistic methods are sound, to the conclusion that they are unsound. Therefore, since intuitionistic methods are (we presume) correct, there is a function f which is demonstrably not $\mathfrak{F}$-definable and $\mathfrak{F}$CT is false, given the basic assumptions of reductionism.[3]

2.3 Mathematical solipsism In reductionism, as in old-fashioned forms of perceptual idealism, we find an unfortunate affinity for solipsism. Once we show how the affinity arises from the constraints upon the availability of proof, we can argue for the need to avoid solipsism and point out the difficulties inherent in doing so.

As we said, intuitionistic antirealism depends upon the doctrine that the only intuitionistically legitimate concept of proof is that of available proof. In the rejection of

$$\mathrm{RH} \vee \neg \mathrm{RH},$$

our testimony concerning the existence of proofs of RH had to be taken as gospel. It would be very natural to move from "the only proofs are those available to me" to "mathematics, like raw feelings or hidden longings, is essentially a private matter". Indeed, the move may even be necessary. If the complete reduction of intuitionistic mathematics is to succeed, then there cannot be legitimate mathematical properties of mathematical items which go unremarked. Consequently, one cannot identify the available proofs of intuitionistic mathematics with ordinary physical objects open to public display, such as actual inscriptions of proofs in monographs or textbooks. We have no difficulty in admitting the possibility that physical objects participate in abstract facts which go wholly unremarked. We can even imagine that, like a settee or a tugboat, such an object might exist in complete independence of its availability to us and that it might stand in unavailable abstract relations to other such objects.

Nor could we fall back upon the possibility that proofs—and constructions in general—could belong to the same attentuated sort of public objects as symphonies, laws, and poems. And for much the same reasons: abstract relations can subsist among these kinds of objects as readily as they can among pieces of furniture and with as little regard for our abilities to construct or manipulate them. For example, the fundamental laws of our mathematics may have the property of consistency but, famously, we may—due to the fact that they are consistent—be totally incapable of recognizing them as such.

Of course, were we to take on idealism, a form of reductive intuitionism about the physical world, the objections would disappear along with the objects. Were we to be reductionists about ordinary objects, they could possess no unrecognizable features. We could then construe the proofs as a portion of the realm of ordinary macroscopic beings without our previous worries. However, the deficiencies of such a tactic are manifest—the maneuver simply begs the question by seeking to reduce all the difficulties which we think attend mathematical reduction to those which we know to crowd around perceptual idealism. Alternatively, one might hazard the suggestion that spatial, geometrical, temporal, logical, and cardinal properties of public objects are not mathematical and so stand in need of no reduction. However, intuitionistic mathematics could be of little interest if its coherence were to rely upon an insistence that, when I say

I know two different proofs of the Artin–Schrier Theorem,

I am not applying the mathematical concept of *two*.

As in the quotation from Dummett, the proper objects of intuitionistic mathematics are supposed to be mental entities. Constructions are thought to be mental operations and their mental effects, among them the thought processes of constructing proofs and the results obtained. If we subdivide the mental into the *intensional* and the *phenomenal*, then the phenomenal seems to afford the only category in which to place the constructions. As the intensional encompasses the objects of belief, thought, and desire conceived as such, the reduction of mathematics to this sort of object cannot succeed. Again, we allow that beliefs—as intensional items—have properties, such as consistency and coherence, which may literally be impossible to detect. For instance, there are second-order inferences which hold among our thoughts which we not only fail to draw but are incapable of drawing.

Second, if we identify proofs with objects of thought, we seem to be faced with a classical problem one might call 'the third construction'. Objects of thought stand in logical relations and satisfy coherence conditions which are set, not by other objects of thought, but by the laws of mathematics and logic. Proofs of the trisection of the angle by Euclidean means cannot be thought because they are impossible, as Lindemann's proof showed. The thought that induction up to ϵ_0 is not formalizable in arithmetic is constrained to follow logically from the thoughts that arithmetic obeys Gödel's Second Incompleteness Theorem and that ϵ_0-induction suffices to give a consistency proof for arithmetic. The fact that there is such a logical relation would be, on the view we are presently assaying, nothing more than the existence of a construction as an object of thought. The fact in question is now to be explained with reference to a logical relation holding among four objects of thought: the three thoughts and the construction. But this relation obtains in virtue of a logical constraint, which must, in turn, be understood in terms of the existence of a further construction. And so on.

Now, we seem to be left with only one alternative: that constructions are themselves phenomenal objects akin to pains and afterimages. Their intrinsic properties are only those which they seem to have and these are solipsistic: unshared, unsharable and, on some outlooks, incommunicable. As is well known, Brouwer encouraged just this sort of mathematical solipsism. He declared intuitionistic mathematics to be the record of the fruits of the creative activity of a single individual. Constructions are phenomenal objects which, in the mind of the mathematician, make up a kind of Lego set, pieces of which can be assembled and displayed on the inner visual field. Ultimately, the facts of mathematics are just those which he can put together from his fundamental elements.

It is clear that we ought not to follow Brouwer. As Kreisel has emphasized, the dialectic of the intuitionist has both *positive* and *negative* tropes. The positive pertains to the development of intuitionistic mathematics *in se*. The negative is outward-looking; it is the critical side of intuitionistic mathematics, the one that *inter alia* opposes classical logical laws with counterexamples. It is obvious that, if reductionism were to dissolve into solipsism, the negative doctrine would be insupportable. Indeed, intuitionism could be nothing but a rare form of insanity. Anyone who questions commonly accepted scientific truths, especially laws of logic, and proceeds to set up idiosyncratic standards of validity in their place and does so by harkening to their own inner voice, would rightly be counted insane.

Worse, from the vantage point of solipsism we cannot see why mathematics ought to be the way it is. One of its prominent features is that intersubjective *agreement* has a paramount place. Mathematics and mathematicians exhibit a very low tolerance for dissension over the basic mathematical principles and objects. (The poor fortunes of intuitionism afford a veritable case study in mathematical intolerance.) Generally, proofs are inadmissible until they have been vetted by the relevant experts and, should a purported proof be seen to fail of validity, strenuous efforts are made either to "patch it up" or discard it altogether. Solipsism, the identification of constructions with phenomenal objects, does not seem to offer any explanation for this phenomenon. If proofs are anything like sensations, then we ought, it seems, to tolerate all kinds of disagreements over their phenomenal properties. Indeed, we might even tolerate considerable differences as to whether some object is or is not a proof, just as we would allow someone to hold that tickling can be painful.

2.4 Idealization As we said, the reductionist must insist that there is no such thing as a proof which is not a proof-available-to-me, one whose existence and basic properties are settled primarily by my say-so. One could well object to the reductionist that there certainly are proofs—in the usual sense of the term—which are not available to me. My mathematical ambit would be narrow indeed if it were restricted to propositions whose proofs I can literally carry out. I know that the Adjoint Functor Theorem is true but this knowledge cannot involve the ability to produce a proof of it at the drop of a hat. I know that there is a proof of Poincaré's conjecture in dimension four but I know little or nothing of its details. Appel and Haken devised a computer-assisted "proof" of the Four Color Theorem; I could not, in any real sense whatsoever, produce such a proof *in toto*.

Consequently, there is a demand on the reductionist to admit a liberal interpretation of the "proof-available-to-me" concept. But the reasoning of the counterexample sets limits on its legitimacy. As we said, to argue convincingly that RH is intuitionistically untrue, the reductionist must accept as evidence for the nonexistence of an intuitionistic proof of RH the testimony of individuals. And that testimony is only that there is no proof available.

The trend of thought suggests that one allow a proof to count as available-to-me in the liberal sense when I am able to access the proof in some regular, assured fashion. There must be some procedure which I could in fact carry out and which would certainly lead to a condition in which the proof would be available in the strict sense. In the case of the Poincaré conjecture, I can read and study the proof in a research report. In the case of the Four Color Theorem, the sense in which I *could* carry out the computerized procedure which would bring me to a full cognizance of the proof is, admittedly, somewhat more attenuated. One would have to make the further allowance that I *could do* certain things which can only be done, properly speaking, by some "idealization" of myself. The sort of idealization we have in mind is encoded in the vision of a supermathematician with enhanced memory and lifespan; one presumes that he could carry out the computerized procedure which would constitute the strictly available proof of the Four Color Theorem

It is a theorem of intuitionistic arithmetic that every natural number is either prime or composite. Consequently,

either n is prime or n is composite

is intuitionistically true. This is so even if 'n' is an Arabic numeral for the precise number of quarks in the universe. But it is certainly not true that I have either a proof-available-to-me, even in the liberal sense, of

n is prime

or one of

n is composite

for this particular n. As we suggested, the way out of the potential dilemma is for the reductionist to allow that there are proofs-available-to-me which I could not, in any practical sense whatsoever, carry out. The relevant proof-available-to-me for this case is the proof of one or the other disjunct which is *potentially* available in virtue of my actual knowledge of some primality algorithm. Given my grasp of the algorithm, I *could*, if I lived longer and had a larger memory, give a proof of one or the other disjunct. So, the proofs-available-to-me liberally are actually those which are strictly available to the aforementioned supermathematician, a mathematically more substantial version of myself.

Saul Kripke, in [18], has maintained a highly skeptical attitude toward such idealizations. He holds that we really know very little about the mathematical behavior of my more long-lived and retentive counterpart. Kripke's suggestion seems to be that we would likely find such a being cognitively impenetrable. Like a mathematical version of the Cumean Sybil, his faculties would be so advanced relative to our own that we could have little insight into their workings.

No doubt, the correctness of Kripke's attitude would spell doom for the reduction. In order to reduce truths of mathematics to statements about my knowledge, I would have to know a goodly amount about the abilities of the "super version" of me. To see this, return to the presumptive counterexample to TND. If

n is prime

can be intuitionistically true in virtue of a proof which only my counterfactual counterpart could carry out, then we could make the same allowances for RH. As a result, we might consider RH to be true in a similar way. It might be that, if I had greater mathematical staying power, then I could prove RH. In fact, we can imagine that, with enough processing power, RH would be as easy for me to prove as is Euclid's Prime Number Theorem.

Without question, this allowance would violate the ban on unrecognized mathematical truths, provided that the mathematical potential of my counterpart were not in some way given to me. The reductionist must, therefore, insist that anything provable by my counterpart be somehow known to me. Presumably, this knowledge would be mine in virtue of my grasp of an effective procedure like a primality algorithm, which I know would produce the appropriate proof when put into the hands of the supermathematician.[4]

Any threat of circularity could be avoided were this further knowledge nonmathematical. Unfortunately, this will be anything but the case. Thanks to the efforts of computability theorists, the concepts of *algorithm* and *effective procedure* are now recognized as mathematical concepts. So, if the reduction is to go through, reference to procedures or algorithms must also be analyzed away.

On the face of it, algorithms are themselves abstract objects; they are recipes to be compiled into the machine code of a mathematical automaton. We cannot simply replace talk of algorithms by talk of operations which I can perform. In the primality example, this was just the problem. We had to introduce the smart counterpart, the supermathematician, just because there were certain algorithmic procedures which I physically cannot carry out. Nor can we plausibly say that a procedure is algorithmic just in case there is a recipe which some counterpart or other of me could carry to completion on each input. After all, there is an imaginable counterpart of me which can pick out, by following a finite procedure, all and only those numbers which code truths of arithmetic. But if this were what the intuitionist meant by 'algorithm', then

$$\phi \vee \neg\phi$$

would be intuitionistically true for all arithmetic substituends ϕ.[5]

Even if the difficulty with "algorithm" is circumvented, my knowledge of the properties of those algorithms and, hence, my knowledge of the behavior of the counterpart will, in general, come to me in care of some (possibly highly complex) mathematical proof. The fact that my counterpart can check that n is prime may only be known thanks to a proof that involves the evaluation of integrals or the sort of statistical reasoning which goes into Monte Carlo factorization techniques. Noncircularity in the reduction will require that this proof also be available to me in the strict sense. Moreover, there are still other constraints on the proof, an appreciation of which calls for a study of the intuitionistic proof concept itself.

2.5 Intuitionistic proof When the reductionist says that a mathematical proposition like RH is intuitionistically true just in case there is a "proof" of it, he could not have meant 'classical proof'. For one thing, the reductionist needs the *disjunction property*:

$\phi \vee \psi$ is provable only if either ϕ is provable or ψ is

just to get his counterexample to TND off the ground. Famously, the disjunction property does not hold of classical provability: without mathematical assistance, classical logic will give a correct proof of $G \vee \neg G$, where G is a Gödel sentence for ZF set theory. So, if 'proof' meant 'ordinary proof', we could not presuppose that intuitionistic truth commutes with disjunction, viz., that a disjunction is provable only if one or the other disjunct is.

Naturally, by 'proof', the reductionist means 'intuitionistically correct proof'. But this is just where the interlocutor—the person to whom the reductionist presents the proof and who admits that he knows no proofs for RH—ought to balk. The casual recipient of the counterexample reasoning will have very little inclination to accept the idea that RH has no intuitionistically correct proofs, short of knowing a good deal more about intuitionistic proof. For all he knows, RH might have an intuitionistically acceptable disproof which is only two lines in length.

To a constructivist in the style of Errett Bishop, one whose mathematical results are consistent with classical mathematics, the appropriate notion of proof will not pose such a problem. For him, if neither RH nor $\neg$RH are provable classically, then they fail to be provable constructively. So, a moderate familiarity with classical mathematics would suffice to convince the interlocutor of the cogency of the counterexample reasoning. But there is little consolation in this for the intuitionist who follows Brouwer. He is on the lookout for theorems which contradict those of classical mathematics, at least on its naive interpretation. The intuitionist claims to be able to prove that no real-valued function of a real variable is discontinuous and that there is, up to isomorphism, a unique model of first-order arithmetic. For such a concept of proof, the nonspecialist would be ill-advised to agree that RH is intuitionistically untrue.

The reasoning of the counterexample only becomes probative once there is an explanation of the concept of *intuitionistic proof* according to which a good part of the traditional intuitionistic corpus can be verified. The account of the concept must appear in a particularly sharp form. Otherwise, reductive intuitionism will fall prey to the defects of other reductionistic persuasions—specifically, of psychological behaviorism.

The greatest obstacle to the reduction of mental states to behavioral proclivities is the sheer variety of behavior associated with any particular state. Consider a specific state of imagining, say, imagining of the taste of last Christmas's pudding. Even though the state is specific, the behaviors which could be thought to manifest and constitute the state defy finite specification. While imagining the taste, I might be staring into a grocery window and hungrily scanning a stack of canned puddings. Or, I might just have been reading about the famous Christmas repast at Tom Cratchit's. Or about the very different Christmas gathering described by Joyce in *Portrait of the Artist*. There is an unimaginable variety of ways in which I could act (or fail to act) and on account of which it would be acceptable to say of me 'he is imagining the taste of last year's Christmas pudding'. In part, behaviorism fails because specific thinkings, hopings, desirings, imaginings, and a host of other quite particular mental goings-on do not reduce to any specific forms of behavior. They are only loosely associated with an unregimented motley of external activities.

The reductionist for intuitionism must face the same specificity problem. Corresponding to the truth of an individual mathematical proposition and constitutive of its content must be a specific range of intuitionistic proofs. But, on the face of it, such specificity will be elusive. Intuitionistically as well as classically, there are any number of ways in which one might know via proof that $\mathbb{Z}$ (mod p) is a field if p is prime. One way is to work laboriously through the computations requisite to showing directly that addition and multiplication *modulo p* satisfy the field axioms. Or reference could be made to the fact that (p) is a prime ideal in the ring $\mathbb{Z}$. Altogether, the cogent alternatives are myriad. It begins to look highly unlikely that the intuitionistic reductionist can circumscribe intuitionistic proof conditions for the statement that $\mathbb{Z}$ (mod p) is a field. One need only consider the vast number of mathematical notations in which such a proof might be expressed: there are the languages of algebra, number theory, set theory; there are the objects and arrows of the category of commutative rings. Which of these many would one have to know in order to know that $\mathbb{Z}$ (mod p) is a field?

Early intuitionists such as Brouwer and Heyting were well aware of this sort of variety. Brouwer insisted that no rigorous specification could be given of legitimate intuitionistic methods of proofs. But for intuitionism to succeed in its reductionistic form, some specification has to be provided: the reductionist must demonstrate that the fundamentals of mathematics are organized in ways that those of folk psychology are not. The precision of mathematical statement has to be preserved. Usually, the reductionist will ask us to grant that there is something in common to all intuitionistically correct proofs of a specific mathematical statement. Specifically, we are asked to allow that there be some central or direct kind of proof a potential ken of which would be the quintessence of the mathematical statement.

Michael Dummett [6] and Dag Prawitz [29] have suggested that there is a discriminable concept of just this sort of direct or, in their terms, *canonical* proof. These are to be particularly elementary proofs represented in a particular notation. They are intended to afford the touchstone of intuitionistic truth; all correct intuitionistic proofs are thought to be in some fashion normalizable to proofs of this kind. (Dummett and Prawitz have in mind the normalization sequences which feature in the proof of the normalization theorem for natural deduction.) So, if we accept the doctrine of canonical proofs, proposition p is true when there is available to me (or perhaps to my counterpart) a canonical proof of p.

Obviously, in order to communicate the concept, the canonical proofs must be circumscribed. Presumably, this will be accomplished via some kind of recursive definition, the prospects for which are improved by likening the statements of intuitionistic mathematics to the formulas of a formal system. Any formula is a recursive construction from the logical signs and the basic formulas which express the system's primitives. Normally, the collection of primitives will be finite. As a result, any such system will represent a finite number of primitive mathematical concepts; every other concept of the system is expressed in terms of compositions of the primitives with logical signs. So, the concepts and statements of the formal language can be arranged in the well-founded subformula order. Consequently, a recursive specification of the "proof conditions" of a formula could well succeed: once we specify what counts as a correct intuitionistic proof of the basic formulas and explain how proof conditions interact with the logical operators, we have a potential explanation of the proof conditions of any formula. In this way, the reductionist's debts to intelligibility are paid in full and the reasoning of the counterexample will go through.

Again, things cannot be as simple as they seem. First, a difficulty appears the minute we return to the comparison between reductive intuitionism and behaviorism. The latter fails, in part, because those concepts which purport to be the "primitives" of purely mentalistic discourse cannot be logically ordered. The concepts associated with belief, desire, intention, and volition seem neither interdefinable nor reducible to some more fundamental mentalistic notions. To put it another way, we cannot explain what would count as the behavioristic analogue for 'Susie believes Ortcutt to be a spy' without referring to other concepts which must themselves be explicated in terms of belief.

The reductive intuitionist hopes to skirt this pitfall by insisting that the logical and definitional network which binds intuitionistic mathematics together is fundamentally different from that of folk psychology. Indeed, he would like to insist that it bears the structure of a formal system. But, for this to be credited, we would have to allow that every concept of intuitionistic mathematics be definable from some finitely circumscribed collection of primitives. The metamathematical facts of the matter seem to discount any possibility for this sort of organization. For one thing, the Fixed Point Lemma inherent in the usual proofs of the Gödel–Tarski incompleteness theorems is intuitionistically provable. It follows immediately that any formal system which suffices to encode the concepts of a relatively impoverished arithmetic is expressively incomplete. Hence, there ought to be many mathematically respectable concepts which cannot be expressed in any proposition which gets a canonical proof.[6]

Second, despite the vividness of the analogy between normalized deductions and canonical proofs, the latter cannot constitute any sort of formal system or reasonable segment thereof. A formal system is an abstract mathematical structure, identical *qua structure* to a real-closed field or a Turing machine. It could not, therefore, lie at the terminus of a successful, noncircular reduction of mathematics. Next and notoriously, proofs in formal systems usually support a ready distinction between proof "in itself" and proof "available to me". In any ordinary formalism, there will be proofs whose complications outstrip my faculty of appreciation. It seems that the ability to recognize canonical proofs must also be attributed to my enlarged counterpart, the intuitionistic supermathematician. And, once again, if we are not to lose the concept of intuitionistic truth altogether, this ability of the counterpart can only be a *facon de parler* for my possession of an algorithm which would serve to pick out the canonical proofs if I had the capacities of the counterpart.

As you recall, we left a discussion of the supermathematician *in medias res*; this is an apposite time to return. As we said, when the reductionist explains the concept of intuitionistic proofs as applied to disjunctions, he needs to avail himself of the notion of a grasp of an algorithm. In general, a proof-available-to-me of a disjunction will be the firm grasp of a procedure which, I am assured, my counterpart can use to yield up a canonical verdict upon one or the other of the disjuncts. Now, it ought to be clear that the assurance which is a feature of my firm grasp might be spelled out in terms of my knowledge of a proof, so long as the statements which appear in that proof are less complex than the disjunction in question. On the analogy with formal systems, the target disjunction must, in the well-founded ordering of all statements, appear farther up the subformula tree than any statements which appear in the proof. Otherwise, one could never explain what it is for a disjunction to be true.

This constraint is severe and it is fairly clear that relatively few disjunctions will actually satisfy it. One need only think of the relative difficulty of proofs for the correctness of quantifier elimination algorithms. Indeed, there can be no *a priori* limit set upon the complexities of the concepts which feature in the correctness proof. Were the constraint to be taken seriously, it seems likely that the total number of intuitionistic truths would be amazingly small. There would remain relatively few disjunctions whose truth could be known in such a restricted way.

Lastly, one ought to raise a question about our assurance that every correct intuitionistic proof can be "normalized" into a canonical proof. If we cannot be so assured, then canonical proof cannot be any sort of legitimate candidate for "proof-available-to-me". If I cannot turn the ordinary sorts of constructive proofs into canonical proofs, the real proof-conditions of intuitionistic statements might lie outside my ken. At worst, it would be possible to have an ordinary, correct but noncanonical proof of a statement without being in a position to recognize that statement as true.

Under the preferred analogy between intuitionistic theories and theories in formal systems, the requisite assurance would be afforded by some kind of normalization theorem. But, as normalization theorems lead directly to consistency proofs (simple inspection is all you need to see that $0 = 1$ has no normal derivation in arithmetic), these proofs cannot themselves be represented in the formal system which is their object, as long as that system is sufficiently strong and satisfies the conditions of the Second Incompleteness Theorem. Therefore, assurance takes the form of mathematical knowledge which cannot itself be represented in terms of a knowledge of canonical proofs. The tempting replies—that the assurance is either nonmathematical or somehow "direct and unanalyzable"—are wholly unconvincing.

2.6 Intuitionistic truth

2.6.1 Time and truth If the truth conditions of RH are given by the report,

I have a proof-available-to-me of RH,

then we are ready to apply temporal discriminations to the truth of RH. Just as with present-tense sentences reporting on the current position of Mars or the ripeness of an apple, the displayed statement seems to contain a suppressed 'now' which is available for modification into 'then' or 'hence'. We can sensibly assert that RH was true or will be true or is not yet true, or was true last Tuesday. If it were thought that RH would certainly be proved at some stage in the future, we could indicate as much by saying that RH is not true now but will certainly become true. As for matters of time, the reductionist rendering of RH contains no more lofty a claim than 'Dear, I think I left the stove on' or 'The Yankees will win the series in six'. We could allow that RH might become true tomorrow and that it would be alright to say 'Yesterday, RH was not true but today it is'. *Prima facie* the possibility is opened that a mathematical proposition might even cease to be true—perhaps because all proofs have been lost and no memory of them remains. For all we know, there may have been statements in the missing books of Euclid's *oeuvre* whose proofs have never been rediscovered. At the very least, we would need a special explanation (perhaps another dose of supermathematical idealization) in order to bar this possibility.

Like J. S. Mill, the reductive intuitionist also takes mathematical truths to be contingent. Unlike Mill, he takes them to express contingent facts about human history. To take a specific example, it may have been a matter of pure chance that Eudoxus—or anybody—proved the prime number theorem, the one attributed to Euclid. It seems perfectly possible that the theorem might fail to be humanly provable. (We can imagine that humans are far less adept mathematically than they actually are.) Hence, on the intuitionist view, the prime number theorem is not a necessary truth—it might well not have been true. Heyting

[12] seemed to embrace this idea wholeheartedly; he even referred to intuitionistic mathematics as "empirical".

As Frege pointed out, one gets a conceptual headache trying to make this sort of empiricism fit pedestrian mathematical theories. Although it might be easy to admit of a universe in which the gas laws are suspended, it is hard to make any sense of a universe in which the laws of primitive recursive arithmetic fail to hold. Dummett, in [6], made a suggestion which looked to eliminate the temporal relativity of the reductionist concept of truth together with attendant headaches. Instead of equating RH with

I have (now) a proof-available-to-me of RH,

one might equate it with

I can produce a proof-available-to-me of RH.

The latter sort of statement, just as the former, is to be true in virtue of the actual production—by me or a counterpart—of a suitable proof. But, unlike the former, it is to be considered timelessly true; once the actual production has occurred, it is seen to have been true always. If acceptable, Dummett's proposal would obviate reluctance toward tensed mathematics. Were RH to receive a constructive proof tomorrow, it would be true today; it would have been true in 43 BC.

Putting aside the question whether there really are in mathematical parlance any of the sort of statements Dummett imagines, we can see that the suggestion will not do. To make the counterexample to TND stick, the reductionist has to claim that RH is not now true. But, if RH is timelessly true à la Dummett, he cannot support the claim that RH is not now true by referring to the present-day dearth of proofs. To certify that RH is not intuitionistically true, he would have to show that RH will never be proved. Short of giving a full-scale independence result, this is something he cannot do. Worse, Dummett's proposal again opens up the possibility for unrecognized mathematical truths. Mathematical facts could obtain not in virtue of our current abilities, even if idealized, but in virtue of our future ones. But these may be as dark to us now as sheaf theory would have been to Raymond Lull.

2.6.2 Nothing could be further from the truth The weight of received philosophical opinion seems to be behind the notion that the scheme of disquotation,

$$\mathrm{Tr}(\phi) \text{ iff } \phi,$$

is a necessary feature of any successful account of truth. But none of this can be effective with the reductionist; unrestricted disquotation would undermine the counterexample to TND. First, since ϕ in the above scheme can be any statement, from general disquotation follows disquotation for negated statements,

$$\mathrm{Tr}(\neg\phi) \text{ iff } \neg\phi.$$

Second, even if the biconditional expresses only material equivalence, we can negate both sides to obtain

$$\neg\mathrm{Tr}(\phi) \text{ iff } \neg\phi.$$

It follows immediately that

if $\neg \mathrm{Tr}(\phi)$ then $\mathrm{Tr}(\neg\phi)$.

So, once we successfully argue that the left disjunct of

$\mathrm{RH} \vee \neg \mathrm{RH}$

is not intuitionistically true, we know automatically that the right disjunct, $\neg$RH, holds. Therefore, the reductionist must refuse to allow that negation commutes with the truth predicate. In particular, he must not accept that

if $\neg \mathrm{Tr}(\phi)$ then $\mathrm{Tr}(\neg\phi)$.

Disquotation cannot govern the reductionistic truth concept.

One ought not conclude that only one half of the disquotation principle, the right-to-left or "quotation" direction:

if ϕ, then $\mathrm{Tr}(\phi)$

conflicts with reductionistic strictures. Some considerations, equally weighty, can be lodged against the other or "disquotation" half:

if $\mathrm{Tr}(\phi)$, then ϕ.

These will be considerations of a more formal nature.

Reductionists agree that, if intuitionistic truth is not itself decidable, that is, if it is not the case that every proposition is either intuitionistically true or it is not, then, it is at least positively decidable. In other words, if there should be a proof of a proposition, then we have the means to register the availability of that proof. This is yet another way of stating the requirement that there be no unrecognized mathematical fact. Also, the idea that intuitionistic truth might admit of articulate mathematical treatment is accepted as coherent, at least pending further investigation. It would not be inappropriate, then, to ask that truth be given expression within a formalized version of an intuitionistic theory which is recognizably sound and extends elementary syntax. But, if this is allowed, then the "disquotation" half of the disquotation scheme yields contradiction. (A note for afficionados: disquotation plus the decidability of the proof predicate entails the Brouwer-Kripke Scheme, which many have thought objectionable.)

First, we are assuming that Tr is expressible as a one-place predicate which holds (or fails to hold) of numerical codes of closed formulas of the system. Then, we make the seemingly reasonable and modest assumptions that the "disquotation" part of disquotation (call it 'D') holds

if $\mathrm{Tr}(\phi)$, then ϕ,

along with the fact that this last is itself intuitionistically true:

$\mathrm{Tr}(\mathrm{Tr}(\phi) \rightarrow \phi)$,

and, finally, that formal derivability preserves truth at least in the case of some individual formula-types. In particular, we assume that

if $\mathrm{D} \vdash \neg\phi$ and $\mathrm{Tr}(\mathrm{D})$, then $\mathrm{Tr}(\neg\phi)$.

It is a simple manipulation to show that these three assumptions are inconsistent. First, since the system in which we are working extends elementary syntax, there is a formula ψ which fixes the predicate

$$\mathrm{Tr}(\neg \ldots).$$

It follows immediately that

$$\mathrm{D} \vdash \neg\psi.$$

Then, from the other two assumptions, one can easily show that

$$\mathrm{Tr}(\neg\psi),$$

and, since ψ is a fixed point, that

ψ follows from the second and third assumptions.

Therefore, the three assumptions are jointly inconsistent. It is worth pointing out that a recourse to some sort of type theory does not seem to circumvent this dilemma, as the reader can easily confirm.[7]

It is something of a puzzle then that there remain independent considerations for insisting upon disquotation. Not the least among these is the fact that, intuitively, disquotation ought to be intuitionistically true. If we read the logical signs with a constructive gloss, then from the fact that ϕ is intuitionistically true, we can discover a proof of ϕ. Hence, ϕ should follow from the assertion that ϕ is true. For the converse, we know that, intuitionistically, ϕ can hold only in virtue of a proof for ϕ which we can, at least in principle, discover. But finding this proof is just getting into a position in which we see that True(ϕ) holds.

It behooves the reductionist to explain the proof conditions of negated statements in such a way that the failure of disquotation becomes intelligible. Usually, some notion of necessity is put to work to fulfill this obligation. Specifically, the reductionist differentiates between $\neg\mathrm{Tr}(\phi)$ and $\mathrm{Tr}(\neg\phi)$ by saying that the former reports that no proof of ϕ is now available, while the latter makes the intuitively stronger claim that a proof of ϕ is shown to be mathematically *impossible*. To be more precise, the reductionist will explain that $\neg\phi$ is intuitionistically true when one has an effective procedure which maps any possible proof of ϕ into a proof of an obvious absurdity such as $0 = 1$. An apparently less stringent condition is associated with $\neg\mathrm{Tr}(\phi)$: an empirical claim like $\mathrm{Tr}(\phi)$ is false when it fails to correspond with the supposedly manifest facts of my mental history.

For this explanation to buttress the counterexample, the word 'possible' in the phrase 'any possible proof' must get a nonvacuous modal twist. If the reductionist meant by 'possible proof', merely 'proof-(now)-available-to-me,' then the prospects of the counterexample of TND would evaporate. The reductionist needs to grant that either RH now has an available proof or it does not. If the former, then RH is intuitionistically true. If the latter, then we have ready-to-hand an effective procedure for mapping all available proofs of RH into any value we please. If there are no available proofs, then any effective procedure, say $\lambda x.0$, will suffice. It would then follow that $\neg$RH is intuitionistically true. (Incidentally, the reductionist can hardly refuse to accept the instance of TND which just appeared, *viz.*, that RH either has an available proof or not. The reasoning of the presumptive TND counterexample relied upon the assumption that one can accurately determine, for any proposition, whether or not a proof of it is available.)

So, the words 'possible proof' must not mean 'proof-available-to-me'. Nor can it be short for 'proof which would be available to one of my supermathematical counterparts but not, perhaps, to me.' Recall that I could only claim access to the mathematical pronouncements of my counterparts on the basis of my own mathematical abilities. As we said, a proof will be possible for my counterpart just in case it is available-to-me in the extended sense where that, in turn, consisted in general of my possession of an algorithm. If 'possible' meant 'proof available to me in the extended sense', then we can return to the argument of the preceding paragraph. That argument's only substantial assumption was that one could decide whether a proof of RH was available or not. But this assumption is in place regardless of our understanding of 'available'. Whether strict or extended, one can—according to the reductionist—always tells when a proof is available and when it is not.

The reductionist seems to be relying upon a concept of mathematically possible proof which he has yet to explain in fully reduced terms. It may not, however, be necessary to chase this concept any further, as there is a more telling problem, one which will attend any view calling upon a fairly strict distinction between "mathematical" and "empirical" statements. According to the reductionist, mathematical negation (the one marking a reduction to absurdity) can sensibly attach only to mathematical statements—those which fit into the rubric governed by *reductio* proofs. Empirical negation is semantically distinct and attaches only to correspondingly empirical statements. There must be some manner of semantic divide between the two.

Quite simply, the problem is that no one—from the days of Hume's *Enquiry* up through *Language, Truth and Logic*—has ever been able to draw a clear and convincing line to separate the mathematical from the empirical. For one thing, the status of a whole raft of reasonable assertions like

> Brahms wrote no more symphonies than there are roots to a general quintic polynomial

and

> The number of planets is not such that, when added to two, it yields seven

seem to defy ready classification. In each case, the reductionist would have to explain which of the two negations was appropriate.[8]

We are now skirting the edge of an admission which, if granted, would disbar reductionism altogether. Throughout his work, Brouwer presupposed that mathematical proofs and other forms of evidence possess a discernible structure which can itself be put to honest mathematical work. It is doubly significant that Brouwer's idea of evidence comes to the fore quite plainly in his most "Brouwerian" contributions: in the proofs of Brouwer's Theorem and of the Fan Theorem and in the foundations of the theories of the creative subject and of choice sequences. We like to think that this idea—that mathematical evidence is itself suspectible to full-scale mathematical analysis—is the very heart of intuitionism. Our treatment of the issues surrounding "possible proofs", solipsism, and algorithms strongly suggests that this is something reductive intuitionism cannot encompass. The coherence of reductive intuitionism seems to require that mathematical evidence fail to be mathematical. Again and again, the reductionist is forced to boil intuitionistic mathematics down to concepts such as "phenomenal construction" and "possible proof" which do not themselves admit mathematical characterization. This is especially clear in the case of intuitionistic truth. The facts about mentalistic proofs, to which mathematical facts are supposed to be reduced, are not mathematical. It is not just that they lack a smooth mathematical treatment; we have no idea how to begin to sort them out.

Perhaps we should say that intuitionistic reductionism fails for the same sort of reason behaviorism did. In the latter case, the "logical texture" of claims about stimulus and response did not match that of claims about beliefs and feelings. So also in the former: statements about mental phenomena lack the sort of "logical texture" required if they are to replace statements of mathematics—even of intuitionistic mathematics.

Maybe this is all to the good. As far as intuitionism is concerned, reductionism has always been a public relations failure, for at least two reasons. First, it abandons intuitionism to some very bad company. It makes a respectable form of mathematics out to be just another "form of antirealism" akin to fictionalism or instrumentalism or finitism. As a result, intuitionism has borne a guilt by association which has curtailed its appreciation.

Second, reductionism fosters the invidious idea of a deep and fundamental rift lying between intuitionistic mathematics and its classical counterpart. On most of the charts, the divide is seen to run between the solid ground of classical, realist semantics and the marshy, vaprous zone of antirealism. The former contains the prosperous regions populated by solid and successful mathematical citizens such as Tarskian model theory and Montague semantics, the latter a neighborhood where property values are markedly lower, elbow-to-elbow with philosophical pariahs like subjectivism and idealism.

So much for reductionism; the realist has no such problems of public image. He thinks that our maps of intuitionistic territory are due for the sort of revision detailed in the section to follow.

2.7 How to be an intuitionist

2.7.1 The status of bivalence It is not difficult to sever the supposed connection between intuitionism and antirealism by showing that intuitionistic mathematics is independent of the failure of bivalence. It is worth noting that failure of bivalence alone cannot serve the semantical needs of even an emasculated constructivism, since it cannot account for all of the classical laws which the constructivist believes will fail. For example, there is the "law of constant domains":

LCD $\forall x(Px \vee Q) \rightarrow (\forall xPx \vee Q)$.

Here, Q is supposed not to contain x free. LCD is classically correct—it features in the usual proof of the prenex normal form theorem—but it is constructively invalid. The intuitionist may use the usual interpretation of predicate logic over locales to prove that the acceptance of LCD forces the acceptance neither of TND nor of bivalence. Consequently, if the failure of bivalence were to express the "semantical essence" of intuitionism, the failure of other laws would require new and nonessential semantical dispensations. (To dispel possible misunderstanding, we must say that the intuitionist need not, in order to avail himself of this reasoning, take the interpretation of logic over locales to be in any way standard. All he needs is the proof that Heyting's predicate logic is sound with respect to the interpretation over a locale given by a two-element set. The required proof is intuitionistically correct.)

Even a cursory glance at Kleene's realizability interpretation [17] suffices to show that the intuitionist can live a full mathematical life without the failure of bivalence. There is no mathematical reason not to use classical logic as a metalogic in which to set up the realizability interpretation. If one does so, each individual instance of the law of bivalence is realized. Even so, one can show that the law of excluded third is not (realizably) valid and that many of the familiar axioms of Brouwerian intuitionism, among them Brouwer's Theorem and the Uniformity Principle, remain true.

In concentrating upon bivalence, it may be that logicians have missed the truly essential point of difference between classical and intuitionistic mathematics.[9] The mathematical core of intuitionism appears to be independent of what many have taken to be its fundamental semantic feature, failure of bivalence. The viability of Kleene realizability opens up the possibility that one can remain a "full-fledged" metaphysical realist about mathematical objects and facts within a thoroughly intuitionistic mathematical universe.

2.7.2. Presentability and truth Of intuitionism, Heyting wrote

> While you think in terms of axioms and deductions, we think in terms of evidence; that makes all the difference. ([11], p. 13)

As we said, the hallmark of intuitionistic semantics ought to be the fact that it takes the abstract form of constructive mathematical evidence as a subject for mathematical inquiry and a crucial element in the truth conditions of mathematical statements. As a result, truth conditions can themselves be given a clear mathematical formulation. To preserve these ideals, we adopt an antireductionist stance. We take the objects of intuitionistic mathematics to be objects *sui generis*, among them are numbers, sets, and functions. They need not be mental entities; they are not to be conceived as essentially mind dependent. The intuitionistic facts in which they participate are *echt* facts. They are as objective as mathematics itself; they carry on without our explicit intervention.

Accordingly, we study the foundations of intuitionistic mathematics much as we do the foundations of a classical domain. In particular, we admit that we already understand some constructive mathematics on its own terms and without the need for reductive explanation. We admit that we already grasp the senses of the intuitionistic logical signs without reconstrual. In devising and exploring foundations for intuitionism, we hope to sharpen and broaden a preexistent intuitive understanding.

With this in mind, we can begin. It is not mere wordplay to hold that, in its foundations, intuitionism ought to be intuitive if anything is. So the foundational concepts ought to be few in number. There seem to be two basic and traditional ideas: constructive truth and the presentability of existence. Upon these, a large part of the intuitionistic corpus can be based.

The fundamental idea of constructive truth is that it is not fundamental; it is defined in terms of other mathematical notions, in particular, in terms of an abstract concept of evidence. This is embodied in the demand that, for propositions ϕ,

$$\mathrm{Tr}(\phi) \text{ hold if and only if } \exists p\, p \models \phi.$$

$\models$ is the relation of constructive evidence. It holds between interpreted propositions ϕ and objects p which are the mathematical forms of immediately discernible reasons. Since these are generalizations of both ordinary constructive proofs and so-called "data objects"—bits of computational information—we call them *proof objects* (or just *probjects* for short). The terminology is supposed to prevent possible confusions between probjects and formal proofs. In saying that truth consists in the existence of a suitable probject, we are giving expression to the thoroughly intuitionistic picture of the realm of mathematical fact as wholly delimited by an abstract representation of our facility with proofs, computations, and other kinds of abstract mathematical evidence.

Like the members of groups and rings, probjects are best conceived of structurally, as denizens of various applicative algebras. As an algebra, a collection of probjects sports an operation of pairing which is total and an operation of application which may well be partial. If p and q are probjects, then $\langle p,q\rangle$ is their pair and $p(q)$ is the result of an application of p to q. Since we can think of probjects applying to each other as function and argument, the notion of probject preserves the innocent ambiguity exploited in using the single word 'construction' as the name for two seemingly different kinds of things: objects and operations. Officially, probjects are both. The natural numbers are assumed to be probjects as well; this is reasonable, since natural numbers are the premier forms of mathematical data.[10]

In our view, it is not an extra constraint to insist that constructive truth be a recognizable form of truth. Among other things, we require that truth be the ultimate condition for the literal correctness of a statement. This requirement is just the principle of disquotation, so maligned by the reductionist:

$$\mathrm{Tr}(\phi) \leftrightarrow \phi.$$

As a consequence, truth commutes with the intuitionistic logical operators. The recursion clauses associated with the semantical research of Tarski (cf. [37]), clauses such as

$$\phi \wedge \psi \text{ is true iff } \phi \text{ is true and } \psi \text{ is true,}$$

hold sway over intuitionistic truth just as much as over classical. (A number of philosophers have troubled to point this out; cf [26].) So, Tarskian model theory—even Montague semantics when properly understood—may be just as intelligible, interesting, and fruitful as they are within the standard context. At times, they can be even more interesting, as we shall see.

Next, there is the presentability of existence. There have been any number of traditional formulations; most of them seem to involve the idea of "explicit presentation": a constructive object can only be given to us as a real presentation, that is, in terms of data which represent the object and which can be appreciated computationally. Since the probjects will do the presenting, all probjects must be finitary and the basic operations they represent must be, intuitively speaking, computable.

Presentability is also allied to existential quantification. The intuitionist understands $\exists n.\phi(n)$ in such a way that, when it is true, there is a computation leading to some specific n and a reason for claiming that $\phi(n)$. According to the intuitionist, this is the only legitimate way in which a number can be "given". When existential claims have free parameters, instances of the existentials must still be "given"—in this case, it is in terms of computations on the parameters. A contemporary rendering of the traditional idea is contained in the scheme

$$\forall p(p \models \phi \rightarrow \exists q.\psi[q]) \Rightarrow \exists r \forall p(p \models \phi \rightarrow \psi[r(p)]).$$

This is the general presentability principle. It says that, if an existential claim $\exists q\psi(q)$ about probjects is based upon the intuitionistic truth of ϕ, then instances of the existential must be computed (using the r of the formula) from the truth conditions of ϕ.

Heyting [11] insisted that intuitionism stood in no need of an extramathematical foundation like that exemplified in the logical principles of *Principia*. Heyting described intuitionistic mathematics as "antimetaphysical". In part, he meant that, in explaining the nature of the intuitionistic discipline or in justifying a mathematical axiom, we need no recourse to considerations either metaphysical or psychological. If a piece of intuitionistic mathematics requires a semantical justification, it is to be given in strictly mathematical terms by referring to abstract evidence and its formal properties. So, in going from reductionist to realist foundations, we think of ourselves not as turning away from the intentions of the early intuitionists but as giving them useful mathematical expression.[11]

From the principles of truth and presentability, we can deduce the general form of an explanation of intuitionistic meaning. For example, we can now show that if the content of a statement is to be given in terms of its truth conditions it must be done as Heyting recommended, in terms of a recursive specification of conditions on the evidence relation $\models$. The direct "proof" conditions of complex mathematical statements must be set out in terms of the direct "proof" conditions of their simpler constituents. (As will be clear from the forgoing, 'proof' is used advisedly. We think it less dangerous, when dealing with intuitionistic mathematics, to speak of mathematical evidence rather than of proof.)

We will restrict ourselves to two examples, truth conditions for disjunctions and for universal quantifications. According to disquotation and the definition of constructive truth, we can assert that

$$\exists p\; p \models (\phi \vee \psi) \Leftrightarrow \exists q\; q \models \phi \vee \exists r\; r \models \psi.$$

By means of a slight detour through intuitionistic arithmetic, we find that

$$\forall p[p \models (\phi \vee \psi) \rightarrow \exists \langle q,r\rangle (q = 0 \wedge r \models \phi) \vee (q = 1 \wedge r \models \psi)].$$

With a little help from the presentability principle, one then sees that there must be a computable operation given by a probject s such that, for any p, if

$$p \models (\phi \vee \psi),$$

then, $s(p)$ exists and gives a pair $\langle s(p)_0, s(p)_1 \rangle$ such that either

$$s(p)_0 = 0 \wedge s(p)_1 \models \phi$$

or

$$s(p)_0 = 1 \wedge s(p)_1 \models \psi.$$

The converse principle also holds: there is a computable operation represented by the probject t such that, if $\langle r,s \rangle$ is the sort of pair just described, then t will accept it as an input and will output a probject $t(\langle r,s \rangle)$ which stands in the relation $\models$ to $(\phi \vee \psi)$.

The same sorts of consequences ensue in the case of universal quantification. From presentability and the commutativity of truth, it is easy to derive the familiar "proof conditional" explanation of the intuitionistic quantifier. (For the sake of the present example, we assume that x ranges over the collection of probjects itself.) If we make the uncontentious assertion that

$$\mathrm{Tr}[\forall x \phi(x)] \leftrightarrow \forall x \mathrm{Tr}[\phi(x)]$$

and claim that truth be constructive:

$$\mathrm{Tr}[\phi] \leftrightarrow \exists p\, p \models \phi,$$

we can readily infer that

$$\mathrm{Tr}[\forall x \phi(x)] \leftrightarrow \forall x \exists p\, p \models \phi(x).$$

With presentability, we conclude that

$$\mathrm{Tr}[\forall x \phi(x)] \leftrightarrow \exists q \forall x\, q(x) \models \phi(x),$$

which is an instance of Heyting's definition of intuitionistic truth.

So, given constructive truth and presentability, we deduce that there must be a probject-definable, computable operation which calculates, from the truth conditions of a disjunction, truth conditions for one or the other of the conjuncts as indicated by operation. Moreover, there is a uniform procedure for computing, from the truth conditions of a universal statement, the conditions of each of its relevant instances. Similar conditions can be determined for all the connectives. The readiest way of satisfying these is to adjust the collection of probjects so that the computable operations described, e.g., the one taking the evidence for a disjunction and converting it into evidence for one of the disjuncts, become the identity. The result of this transformation is just Heyting's semantics [11] for the intuitionistic logical signs.

Three examples: implication, existential quantifier and universal quantifier, serve to illustrate Heyting's ideas. Here, p and q are probjects, S names an intuitionistic set, and a ranges over the collection of entities from which members of S are taken. Intuitionistically as classically, a set is given (for purposes of semantics) by a direct specification of its membership conditions. So, S is specified by describing the conditions under which $p \models a \in S$, for various a.

1. $p \models (\phi \rightarrow \psi)$ iff, for all q, $p(q) \models \psi$ whenever $p \models \phi$
2. $\langle p,q \rangle \models \exists x_s \phi(x)$ iff, for some a, $p \models a \in S$ and $q \models \phi(a)$
3. $p \models \forall x_s \phi(x)$ iff, for all a, $p(q) \models \phi(a)$ whenever $q \models a \in S$.

In more everyday parlance, 1 says that p is direct mathematical evidence for a conditional whenever it is a computable operation which transforms mathematical evidence for the antecedent into evidence for the consequent. According to 2, direct evidence for an existential claim about S is a package with two compartments, one containing a reason for believing that some a belongs to S and the other containing evidence that a possesses the property in question. Finally, by 3, the primary form of evidence for a universal claim is a computable operation which converts evidence that a belongs to S into evidence that a has the desired property; the operation must be uniformly successful for every such a.[12]

As we said, this is a more general and regularized version of Heyting's 1932 interpretation.[13] Once we relativize to the set $\mathfrak{N}$ of natural numbers, the schemes take on precisely the cast which Heyting originally gave them. $\mathfrak{N}$ is the unique collection such that

$$p \models a \in \mathfrak{N} \text{ if and only if } p = a \in \mathfrak{N}.$$

In other words, only the natural numbers can belong to the species $\mathfrak{N}$ and a direct proof that n is a natural number is abstractly represented by that very number itself.[14]

After substituting $\mathfrak{N}$ for S in 2 and 3 above and making the obvious maneuvers, we arrive at 2_N and 3_N:

2_N $\langle p,q\rangle \models \exists x_N \phi(x)$ iff $p \in \mathfrak{N}$ and $q \models \phi(p)$
3_N $p \models \forall x_N \phi(x)$ iff $p(q) \models \phi(q)$ whenever $q \in \mathfrak{N}$.

Of course, 2_N is just another expression of the leitmotif of presentability. At bottom, the only writ for claiming the constructive truth of existentials is *habeas corpus*: one must yield up both a specific natural number and a demonstration that it has the property in question.

The relevance of disquotation to Church's Thesis should now be obvious. From it and Heyting's explanation comes a proof that every number-theoretic function is computable. If we assume the first line below, then the others follow on *seriatim*. (x and y range over $\mathfrak{N}$; p and q over the collection of probjects.)

1. $\forall x \exists y\, y = f(x)$
2. $\exists p\, p \models \forall x \exists y\, y = f(x)$
3. $\exists p \forall x\, p(x)_1 \models (p(x)_0 = f(x))$
4. $\exists p \forall x\, p(x)_0 = f(x)$
5. $\exists q (= \lambda x.p(x)_0) f = q \restriction \mathfrak{N}$.

Every operation given by a probject is computable, so every function on $\mathfrak{N}$ can be effected by applying to the members of $\mathfrak{N}$ a computable operation.

Contrary to the intimations of [1] (*v.i.*), the onus is now upon any intuitionist who despairs of Church's Thesis not to explain how he can "live with" it, but rather, how he plans to live without it! As we have understood it, 'Church's Thesis' refers to all instances of the scheme

$$\forall x \exists ! y \phi(x,y) \rightarrow \exists e\, \forall x [\{e\}(x) \downarrow \wedge\, \phi(x, \{e\}(x))].$$

With Heyting's explanation in place, this boils down to

[*] $\forall q((q\colon \mathfrak{N} \to \mathfrak{N}) \to \exists e\, q[\mathfrak{N} = \{e\})$.

The essence of the probject is its presentability, its computability. The intuitionist, on our interpretation, has set himself the task of devising a completely mathematical semantics. The present-day status of the Church–Turing concept of computable function is reasonably secure; it stands relatively unchallenged as a mathematically rigorous and successful explication of the intuitive computability concept. So it falls to the realistic intuitionist who harbors qualms about CT to explain how he is to succeed and yet resist [*]. To put a fine point on it: the intuitionist needs some mathematical account of computability to get his mathematics off the ground. Without doubt, the notion of recursive function is the most successful notion of computability extant. The intuitionist who rejects CT has some explaining to do. Even if one cares to avoid the barefaced truth that computability is the *central issue* of intuitionistic foundations, the responsibility to CT cannot be avoided.[15]

The realist is free from the philosophical ills which beset reductionism. For example, considerations of computability suffice to give counterexamples to TND. Intuitionistic logic alone prohibits the possibility of a "straight" counterexample to an instance of TND, since logic proves that it would be absurd to deny any instance of TND:

$$\models \neg\neg(\phi \vee \neg\phi).$$

But, to show that TND is not universally valid, we need only make the uncontentious assumption that noncomputable properties of the natural numbers are readily definable. Let $\mathcal{K}$ be one of these. Since probjects are computable, there is no probject q such that, for every $n \in \mathfrak{N}$, $q(n) = 0$ or $q(n) = 1$ and

$$\forall n \in \mathfrak{N} q(n)\ 0 \Leftrightarrow \mathcal{K}(n).$$

It follows immediately from the semantics of disjunction and universal quantification that

$$\neg\forall n \in \mathfrak{N}(\mathcal{K}(n) \vee \neg\mathcal{K}(n)).$$

Hence, TND is not intuitionistically valid.

Finally, we can now "turn around and go back": from the presentability principle, the constructive definition of truth, and Heyting's schemes, we can derive the form of Tarski's recursion clauses. This confirms that our intuitionistic notion of truth engenders none of the headaches brought on by its reductionistic counterpart. For example, if we apply the presentability principle to Heyting's explanation of implication,

$$p \models (\phi \to \psi) \Leftrightarrow \forall q(q \models \phi \to p(q) \models \psi)$$

we can show that

$\mathrm{Tr}(\phi \to \psi)$ iff $\mathrm{Tr}(\phi) \to \mathrm{Tr}(\psi)$.

In short, with computability in the background, Tarski's "definition of classical truth" and Heyting's "definition of intuitionistic truth" are equivalent. It would not be unfair to say that Heyting's semantics is just "Tarski plus computability" (although this is in no way to belittle Heyting's original achievement).

4 Variation II: Life with Church's Thesis Beeson's "Living with Church's Thesis", the fourth chapter of [1], is a fine example of constructivism *noir*. It is a whirlwind tour through recursive mathematics (drawing special attention to analysis), the prime motive of which is the fostering of a negative attitude toward the sort of mathematics we favor. Two of the chapter's presuppositions are of particular concern. First, Beeson assumes that Church's Thesis is indeed something to be "lived with", as if it were a particularly gruesome style of mathematical deformity. In surveying results in recursive analysis, he enjoys characterizing seemingly nonintuitive theorems as "bizarre", as if they were obviously repulsive and freakish. Within such an atmosphere, it is easy to start thinking of CT as an unfortunate feature of the constructive logical environment, something with which the intuitionist has to "cope".

Needless to say, this view should leave the intuitionist puzzled. For anyone who is already aware that intuitionistic and classical analysis must be very different, there is little entertainment in Beeson's sideshow. Unless one has already adopted a thoroughly classical standpoint, the results of recursive analysis hardly appear abnormal.[16]

Second, Beeson supposes that we will be shocked by the scenes in his gallery or disappointed by the seemingly adverse climate of recursive mathematics. But we ought to refuse this kind of response; shock or disappointment would only show that inappropriate standards have been adopted. It is inappropriate to rate intuitionism on its congruence with classical analysis. Intuitionists have developed an analysis of their own. They are not trying to capture classical theorems but to find new, characteristically intuitionistic ones. So there is no contest with classical mathematics on its own ground.

In assessing the potential of intuitionistic mathematics, we ought to be on the lookout for more appropriate comparisons. At the very least, this will afford a more well-rounded view of the subject. When we look, we find regions of classical mathematics that share central intuitionistic concerns, those devoted to the understanding of the finitary and the computable. These are the areas in which intuitionism ought to excel.

The theorems whose proofs we will sketch come from two of these areas: model theory for first-order arithmetic and models of the lambda calculus. These are strikingly *positive* consequences of forms of CT and associated principles. In presenting them, our goal is the elimination of invidious comparison; we do not pretend that it can be achieved so briefly and so cheaply. A more lengthy advocacy would be called for. But there are many other results from areas as diverse as set theory and combinatorics which might have been mentioned and which cannot be encompassed in the space here.

4.1 There are no nonstandard models No classical first-order theory with infinite models determines its models up to isomorphism. There is nothing one could say in the language of Dedekind–Peano arithmetic which would preclude its interpretation over a nonstandard model. From this sort of fact, Skolem concluded that, paradoxically enough, the quintessence of arithmetical structure could not be expressed in a first-order language suitable for expressing the axioms of arithmetic. Skolem went on to conclude, as well, that the very notions of finite and infinite were mathematically insecure. David Hilbert had thought that classical logic and mathematics were the only things which could prevent our eviction from "Cantor's paradise"; Skolem worried that, with classical logic and metamathematics, we would not be sure that we had ever moved in.

The intuitionist need have no such concerns. On the assumption of Weak Church's Thesis (or WCT),

every number-theoretic function is $\neg\neg$ recursive,

he can prove that there are absolutely no nonstandard models of arithmetic. We understand this as metamathematical confirmation of Brouwer's insistence that the intuitionist, thanks to the way in which he conducts his mathematics, has a firmer grasp (perhaps the only adequate grasp) of the natural number concept.

Theorem *Given WCT, there are no nonstandard models of arithmetic.*

Proof: Let $\mathfrak{N}$ be the standard model of intuitionistic first-order (or Heyting) arithmetic. Let $\mathfrak{M}$ be a nonstandard model. As in the classical case, there are simple facts which follow directly from the axioms of arithmetic and suffice to show that $\mathfrak{N}$ must be an initial segment of $\mathfrak{M}$.

Again, as in classical arithmetic, we can avail ourselves of the existence of provably inseparable sets. Let $\phi(x)$ and $\psi(x)$ be the ordinary Σ_1 expressions for the predicates

$$\{x\}(x)\downarrow \wedge \{x\}(x) = 0$$

and

$$\{x\}(x)\downarrow \wedge \{x\}(x) = 1,$$

respectively. The extensions of these formulas cannot be recursively separated in $\mathfrak{N}$; this we can prove in Heyting arithmetic.

Since $\mathfrak{M}$ is nonstandard, there is an $a \in \mathfrak{M}$ such that a exceeds any standard n. It is a theorem of Heyting arithmetic that

$$\forall x \neg\neg \forall y < x(\phi(y) \vee \neg\phi(y)).$$

Once we interpret this in $\mathfrak{M}$, instantiate to a and remove (temporarily) the leading $\neg\neg$, we obtain

[*] $\mathfrak{M} \models \forall y < a(\phi(y) \vee \neg\phi(y))$.

Since a exceeds every standard number, we know that, for all $n \in \mathfrak{N}$,

$$\mathfrak{M} \models \phi(n) \vee \mathfrak{M} \models \neg\phi(n).$$

Finally, we assume CT,

every natural number function is recursive.

Then the 0, 1-valued function f defined by the scheme

$$f(n) = 0 \Leftrightarrow \mathfrak{M} \models \phi(n)$$

is recursive. Since ϕ and ψ are Σ_1, f separates their standard extensions recursively. This is a contradiction.

Obviously, a contradiction can be expressed as a negative formula. So, we can add judicious double negations to CT and to [*] and the reasoning just described will be preserved. Therefore, given WCT, M cannot be nonstandard.

Markov's Principle (MP) is the assertion that

every nonempty decidable subset of ω has an element.

In symbols, MP is often represented as

$$[\forall n(\phi(n) \vee \neg\phi(n)) \wedge \neg\forall n\neg\phi(n)] \Rightarrow \exists n\phi(n).$$

A version of MP will play a large role in matters under discussion in Variation III. For now, it suffices to note that MP is independent of intuitionistic set theory and that, using it, one can derive from the preceding result the stronger conclusion that Heyting arithmetic is categorical.

This result can, in turn, be sharpened to the point at which there appears a single arithmetic sentence which is categorical. It then follows that constructive validity is nonarithmetic. (cf. [21].) With reference to Beeson, it is noteworthy that the proof in this section was inspired by a nonfreakish bit of classical recursive mathematics, Tennenbaum's Theorem on nonstandard models, from [38].

4.2 Brouwer's Theorem and information systems Naturally, one of the great attractions of a type-free lambda calculus is type freedom. A domain over which the calculus held sway would be egalitarian: there will be no class distinctions between function and object. The operation of application will be indifferent to the "order" of its arguments. To model such a domain it would be ideal to have a set X of which the function space $X \Rightarrow X$ is a natural substructure; that way, the functions from $X \Rightarrow X$ could be identified with objects from X.

From the standpoint of model theory, the great attraction is also the great drawback. Using classical reasoning, Cantor proved that there are no nontrivial sets X for which $X \Rightarrow X$ has these sorts of properties—at least when $X \Rightarrow X$ is the set of all functions from X into X. Dana Scott showed us how to overcome the difficulties by solving equations of the form

$$(X \Rightarrow X) \sqsubseteq X$$

and even

$$X \cong (X \Rightarrow X)$$

in such a way that $X \Rightarrow Y$ is a "suitable" function space (cf. [34]). Solution sets can always be found within various categories of *domains*. (For our purposes, a domain will always be a consistently complete, ω-algebraic cpo.) In the case of domains, the "suitable" function space is that fragment consisting of the *continuous* domain maps. This collection is always "thin enough" that the isomorphism equations can be solved while staying "fat enough" that all the lambda terms get interpreted as the abstracts of actual functions.

The difficulties presented by models of the untyped lambda calculus are inherently classical. This should be no surprise—in the notion of probject, a convergence of operation and argument was "built in" from the start. Cantor's general theorem is intuitionistically false and the intuitionist can assume outright that there are fairly ordinary sets X such that

$$X \cong (X \Rightarrow X)$$

where the latter is the *complete* function space of X. To show that all this is so, one can prove a "Brouwer's Theorem" for domains, i.e.,

Every function between domains is continuous.

More recently, Scott has given us [35] a premier way in which to present a category of domains: as completions of *information systems.* For the sake of uncluttered exposition, we will restrict attention to information systems drawn from subsets of ω.

Definition A triple

$$\mathcal{S} = \langle J, \vdash, \Delta \rangle$$

is an *information system* when J is a decidable collection of finite subsets of ω, $\vdash$ is a decidable binary relation holding between finite subsets of ω, and Δ is a distinguished finite subset of ω, all satisfying the axioms to follow. (We are thinking of the finite subsets of ω as given by natural numbers. In the last four axioms, n, m, and p are presumed to be members of J.)

A1 $n \subseteq m$ and $m \in J$ implies that $n \in J$
A2 for all n, $\{n\} \in J$
A3 $n \vdash m$ and $n \in J$ implies that $(n \cup m) \in J$
A4 $n \vdash m$ and $m \vdash p$ imply that $n \vdash p$
A5 $n \vdash \Delta$
A6 $n \subseteq m$ implies that $m \vdash n$
A7 $n \vdash m$ and $n \vdash p$ imply that $n \vdash (m \cup p)$.

The connection between information systems and domains is perfectly plain: every information system is a "domain skeleton", the collection of *finite* elements of a domain which arises through a "Cauchy completion" process.

Definition If $\mathcal{S}$ is an information system and f is a sequence of members of J, then f is an *element* of $\mathcal{S}$ provided that, for every n,

$$(f(0) \cup f(1) \cup \ldots \cup f(n)) \in J.$$

Let $\mathfrak{D}$ be the collection of elements of $\mathcal{S}$. On $\mathfrak{D}$ there is a partial order which obtains when one element "approximates" another: we say that $f \sqsubseteq g$ whenever

$$\forall n \exists m (g(0) \cup g(1) \cup \ldots \cup g(m)) \vdash f(n).$$

Proposition *On the assumption that* $\mathcal{S}$ *is an information system, the set of elements* $\mathfrak{D}$ *is a consistently complete,* ω*-algebraic cpo.*

Proof: For definitions and proofs, the reader can consult [35] or [19].

As far as information systems are concerned, the functions of interest are those which are *continuous* on the associated collection of elements. Intuitively, a function is continuous when it respects the topology defined by the *finite* elements:

Definition The *finite* elements of an information system $\mathcal{S}$ are the constant functions

$$[n] = \lambda x.n$$

whenever $n \in J$.

Definition If $\mathfrak{D}$ and $\mathcal{E}$ are the sets of elements of information systems and F: $\mathfrak{D} \to \mathcal{E}$ then F is *continuous* provided that, if $f \in \mathfrak{D}$ and $[n] \subseteq F(f)$, then

$$\exists m\ [m] \subseteq f \wedge [n] \subseteq F([m]).$$

Theorem (assuming CT and Markov's Principle) *If $\mathfrak{D}$ and $\mathcal{E}$ are sets of elements of information systems and F: $\mathfrak{D} \to \mathcal{E}$, then F is continuous.*

Proof: Take $\mathfrak{D}$ to arise from the information system $\mathcal{S}$ and let F map $\mathfrak{D}$ into $\mathcal{E}$. As one can see immediately, to show that F is continuous it suffices to check that, for any $f \in \mathfrak{D}$ and n,

$$F(f)(0) \vdash n \Rightarrow \exists m\, f(0) \vdash m \wedge F(m)(0) \vdash n.$$

We let ρ be a total recursive function such that, for each $i \in \omega$, $\rho(i)$ is an index for a sequence $g(i)$ of finite elements determined by $\{i\}$. We let W_i be the r.e. set which is the range of $\{i\}$ together with Δ and let $W_i(n)$ be its nth member.

$$g(0) = \Delta$$
$$g(n+1) = \begin{cases} g(n) \cup W_i(n) & \text{if } (g(n) \cup W_i(n)) \in J \\ g(n) & \text{otherwise.} \end{cases}$$

For each i, $g(i)$ is a member of $\mathfrak{D}$ and, so, $F(\{\rho(i)\})$ is defined and belongs to $\mathcal{E}$. By CT, $F(\{\rho(i)\})$ is a recursive sequence whose index can be computed effectively from i. Let $\Theta(i)$ be such an index.

Another application of CT proves that the set

$$I_n = \{i\colon \{\Theta(i)\}(0) \vdash n\}$$

is r.e. and extensional. By the Myhill–Shepherdson Theorem (which is itself a consequence of MP), there is a finite initial segment s of f such that $s \in I_n$. The union of the range of s gives us a finite element m such that

$$f(0) \vdash m$$

and

$$F(m)(0) \vdash n.$$

This completes the proof of the theorem.

Corollary *There is a set χ such that*

$$\chi \cong (\chi \Rightarrow \chi)$$

where '$\Rightarrow$' indicates 'complete function space'.

Proof: Scott's D_∞-construction is intuitionistically correct and results in a domain D_∞ which is isomorphic to the set of all continuous functions from D_∞ into D_∞. Since we can assume that every function is continuous, D_∞ is isomorphic to the set of all functions

$$D_\infty \Rightarrow D_\infty.$$

4.3 Small complete categories A category is small when its collection of objects comprises no more than a set. It is cartesian closed when it has finite products and exponential objects—as defined by the adjointness conditions which capture the abstract relation between cross products and function spaces in Set. It is complete when closed under arbitrary limits, including products indexed by all the objects of the category itself.

A small category of this kind would be just the ticket for interpreting the types of the *polymorphically typed* lambda calculus, $P(\lambda)$. The latter is a typed formalism which seems profligate about the sorts of types it will countenance. In particular, it will permit types which are the results of "products" over the entire collection of types. For example, a polymorphic identity function will have type

$$\Pi_{t \in T}(t \Rightarrow t)$$

where T is the collection of all types.

Classically, no very serious category can be small and complete. Moreover, one's immediate impression is that the task of modeling such a construct will be nontrivial. Reynolds, in [32], has shown that first impressions are well confirmed by proving that there are no standard classical models whatsoever for $P(\lambda)$. But Reynold's argument requires an intuitionistically incorrect form of Cantor's Theorem, so it cannot be constructively reconstrued.

Once again, the modeling situation for $P(\lambda)$ is, by intuitionistic lights, totally different. As far as we know, this was first realized in [27]. It follows from an extended version of CT, Markov's Principle, and a plausible principle of uniformity ($v.i.$) that the collection of *presented sets* is equivalent to a small cartesian closed category which is complete.

Definition A *presented set* is any triple $\langle A, X, h\rangle$ where A is a set with stable equality, X is a stable subset of ω, and h is a function mapping X onto A. Once again, a notion is stable when it is closed under $\neg\neg$.

Let ECT be the following extended form of CT. Here, A and B are (the first components of) presented sets $\langle A, X, h\rangle$ and $\langle B, Y, k\rangle$.

> If F maps A into B, there is an index e such that $\{e\}$ is defined on X and, for all $n \in X$, $k(\{e\}(n)) = F(h(n))$.

CT is an obvious consequence of ECT; just consider ω as the presented set $\langle \omega, \omega, id\rangle$.

The Uniformity Principle (UP) is stated for sets A which are quotients of some powerset. For any such A, UP is

$$\forall x \in A \exists n \in \omega \phi(x, n) \Rightarrow \exists n \in \omega \forall x \in A \phi(x, n).$$

The initial negative response to UP is easily overcome. By explaining the way in which probjects present powersets, the anticlassical quantifier exchange in UP can be made perfectly intelligible. UP and ECT both hold in the ordinary Kleene realizability universe.

Theorem *There is a small cartesian closed category which is complete.*

Proof: Unfortunately, there is not space here to give the proof in complete detail. We must console ourselves with the aspect of the proof which features Church's Thesis. It is obvious that the natural category of presented sets is equivalent to the small category of *modest sets*, consisting of partial equivalence relations on ω which are stable. Hence, it suffices to show that the category of presented sets and set functions is complete and cartesian closed. Here, we will demonstrate that this category is closed under the formation of (full) function spaces.

To that end, let $\langle A, X, h\rangle$ and $\langle B, Y, k\rangle$ be arbitrary presented sets. We wish to prove that, if C is the collection of all functions from A into B, then there is a set Z and a function j such that $\langle C, Z, j\rangle$ is presented.

Let Z be the set of natural numbers to which e belongs just in case, for all n, $m \in X$,

$$\{e\}(n)\downarrow \wedge \{e\}(n) \in Y \wedge (h(n) = h(m) \rightarrow \{e\}(n) = \{e\}(m)).$$

Given Markov's Principle and the fact that $\neg\neg$ commutes with $\wedge$, we see that Z is a stable subset of ω.

For each $e \in Z$, we can take $j(e)$ to be the relation

$$\{\langle h(n), k(\{e\}(n))\rangle : n \in X\rangle.$$

$j(e)$ is a functional relation and obviously takes A into B. The statement that j maps Z onto C is equivalent to ECT. This shows that $\langle C, Z, j\rangle$ is a presented set and that the category of presented sets is closed under exponentiation.

5 Variation III: Dedekind finite machines Nonintuitionistic Church's Thesis is said to get indirect support from the claim that

> every plausible and mathematically cogent formulation of the concept "mechanically computable function on the natural numbers" is equivalent to "function computed by a Turing machine."

As we ought to distinguish this from Church's Thesis itself, we will call it 'Church's Hypothesis' or 'CH' for short. Classical mathematicians have given evidence on behalf of CH by formulating variants of and alternatives to Turing's original concept of algorithm and implementation and then proving that the vast majority of these turn out to delineate the same class of functions.

Of course, this sort of evidence can never be wholly conclusive in support either of CH or of Church's Thesis. From a foundational point of view, it appears especially incomplete; there are seen to be obvious variations on Turing's ideas which have yet to be fully investigated. We find these variants by enforcing changes in the fundamental notions by which a concept of computable function is presented. Arguably, the most important of the notions is finiteness. All of the different presentations of abstract computing device take the notion of "finite" completely for granted; the resulting theories appear not to hang upon any particular analysis of the concept. There is continual reference to *finite* states, *finite* controls, *finite* lists of instructions, *finite* alphabets, and *infinite* tapes. It becomes natural—even necessary—to ask, "What happens to Church's Hypothesis once the notion of finite is itself replaced by an alternative? Is the resulting concept still extensionally equivalent to the one with which we started?"

Even classically, the answer to the last question can be 'No'. In the appropriate model-theoretic setting, it is possible to overturn CH.[17] A set is Dedekind finite (or D-finite) when it is isomorphically incomparable with any of its proper subsets. With a countable axiom of choice, one can prove that D-finite numbers correspond with the standard finite numbers. This proof requires choice essentially: there is a forcing model of ZF plus choice for finite sets in which the collection of D-finite numbers is the universe of a nonstandard model $\mathfrak{A}$ for arithmetic. By the proof of Tennenbaum's Theorem on nonstandard models [38], there is in $\mathfrak{A}$ a D-finite number E which indexes a D-finite Turing machine such that the natural number function computed by that machine is total but nonrecursive. Therefore, there is a plausible and cogent alternative to the standard concept of Turing machine which disagrees sharply with it. We can even give the concept a precise "machine-theoretic" description: it comes about by generalizing Turing machines to allow programs, tape inscriptions, and runtimes of D-finite length but to demand that inputs and outputs be of finite length only.

To the intuitionist, the tactic of moving to a nonstandard model of arithmetic is not obviously available; as we saw, Weak (intuitionistic) Church's Thesis implies that there are no nonstandard models. Still, there is a similar line of investigation open to him. As we shall see, there are any number of recognizable finiteness concepts. Of these, we shall use four: *strictly finite, subfinite, semifinite*, and *D-finite* in examining variations on Turing machines. It is a testament to the subtlety of intuitionistic mathematics that the four can be distinguished pairwise. As it is nowise clear which of these, if any, represents a "correct" account of the intuitive finiteness concept, none is especially "nonstandard." Hence, it is all the more important that the intuitionist determine precisely how these alternatives to finiteness affect the concept of Turing computability.

For each of the four, there are concomitant ideas of "finite" machine. In the case of D-finite machines, the appropriate instance of Church's Hypothesis,

Every D-finite Turing machine is equivalent to a finite Turing machine.

proves to be both "constructively consistent" (i.e., it does not entail TND) and independent of intuitionistic set theory. This follows from the fact that it is a consequence, individually, of both intuitionistic CT and the second-order form of Markov's Scheme. Hence, the intuitionist can have recourse to a concept of mechanical computability which differs markedly from the standard. A measure of the difference is that fact that there is a Heyting-valued model of set theory in which the collection of *D-regular* sets (the "Dedekind" analogue of recognition by a finite automaton) fails to be countable.

5.1 A number of finites Throughout this section, sets which are in any sense "finite" will be subsets of ω. This restriction should not engender undue concern; using Kleene realizability, it is easy to prove that such a restriction need not be stultifying. In the usual realizability universe, there is an uncountable collection of D-finite sets of natural numbers which are pairwise distinct in cardinality (cf. [19]).

A fairly complete catalogue of intuitionistic finiteness concepts can be had by consulting [9]. As we said, four concepts suffice for present purposes. The first of these is *strict finiteness.* We will say that a set is strictly finite if it can be enumerated by a natural number, thought of as the initial segment of numbers below it:

Definition $S \subseteq \omega$ is *strictly finite* iff there is an $n \in \omega$ and a surjective function f such that $f\colon n \to S$.

But, as it happens, strict finiteness is too stringent a condition to impose upon a set if we are merely concerned to secure its size relative to individual natural numbers. A less demanding alternative is that of *subfinite*:

Definition $S \subseteq \omega$ is *subfinite* iff there is an $n \in \omega$ and a partial surjective function f such that $f\colon n \to S$.

In other words, a set is subfinite when it is the functional image of a subset of a finite set. Obviously, the class of subfinite sets is closed under subsets but the class of strictly finite sets is not. For expressing concepts like "finite element" (in a lattice) and "finitely generated", subfiniteness may be the most appropriate of the four notions. Classically, finiteness coincides with subfiniteness. But this is a coincidence of logic and has little to do with mathematics: the claim "all subfinite sets are finite" implies the full law of excluded third.

Among intuitionistic notions of finite currently in vogue, Dedekind finite is the most relaxed; if a set is finite, subfinite, semifinite (or even bounded or almost bounded), then it is Dedekind finite. If we take "infinite set" to mean "set of which the collection of natural numbers is a (functional) subset", then to say that a set is Dedekind finite is to say, quite straightforwardly, that it is not infinite. Officially,

Definition $S \subseteq \omega$ is *Dedekind finite* (or simply *D-finite*) just in case there is no injective function mapping ω into S.

The 'Dedekind' title is conferred with due respect for historical proprieties. Intuitionistically, a set is D-finite in our sense just in case it is finite in the original sense of Dedekind.[17] However, the class of D-finite sets can now be a proper extension of the class of finite sets, even in the presence of the axiom of countable choice. One rather formal way to see this is to note that a general equation between finite and D-finite sets would imply the full quantified TND. A more intuitive way of coming at the distinction is by thinking of the relevant probjects as bits of "computational information" encoded by the two notions. Seen in this light, to be finite is to come accompanied with a probject which is a natural number yielding cardinality information. On the other hand, for a set to be Dedekind finite is for that set to come equipped with a "precluder": an operation which precludes the possibility that any given recipe will describe a function which maps ω faithfully within the set. But there is no way of computing cardinality information continuously from precluders and, since our logic is computationally sensitive, we cannot conclude that all D-finite sets are finite. One can embrace all sorts of choice principles, including countable choice, without blurring the distinction. Metamathematics confirms the intuitive impression of the probjects: under Kleene realizability, Dedekind finite subsets of the natural numbers whose membership conditions are stable (i.e., closed under $\neg\neg$) correspond precisely to the classical isolated sets while finite sets correspond simply to classical finite sets. Since there are nonfinite isolated sets (cf. [3], [33]), the realizability interpretation forces a firm extensional distinction between the two notions.

Lastly, there is a finiteness concept which, as we shall see, features prominently in Dedekind finite machine theory:

Definition $S \subseteq \omega$ is *semifinite* just in case it is $\neg\neg$ finite.

Intuitionistically, the extensions of our four notions make a tower: every strictly finite set is subfinite, every subfinite set is semifinite and each of these is, in turn, D-finite. None of the inclusions can be reversed.

5.2 D-finite automata But, before going into Turing machines *per se*, we prefer to test the waters by devising a D-finite alternative to the theory of *regular events*. This proves not to be a detour, but a revealing propaedeutic to a more general theory of D-finite machines.

Definition As usual, an *acceptor* $\mathfrak{M}$ is defined to be a quintuple

$$\mathfrak{M} = \langle Q, \Sigma, \delta, q_0, F \rangle,$$

where Q is a set of states, Σ is the input alphabet, $q_0 \in Q$ is the initial state, $F \subseteq Q$ is the set of final states, and δ is the transition function. All these notions and those of acceptance for $\mathfrak{M}$, acceptance language $\mathrm{L}(\mathfrak{M})$, and equivalence of acceptors get standard definitions, as in [13].

Definition An acceptor is *finite* (or a DFA) whenever it is deterministic and its set of states Q is strictly finite. An acceptor is *D-finite* (or a DDFA) iff it is deterministic and its set of states is D-finite. It is said to be *semifinite* (or constitute an SDFA) iff it is deterministic and its set of states is semifinite.

Definition A set of words over the alphabet $\{0,1\}$ is D-regular iff it is the acceptance language of some DDFA.

The principal result on the D-regular concept connects D-finite acceptors to ones which are semifinite:

Theorem *An acceptor is a DDFA iff it is equivalent to an SDFA.*

Proof: Every SDFA is, by definition, a DDFA. For the converse, let $\mathfrak{M}$ be a DDFA. The sequence $\langle Q_i \rangle_{i \in \omega \cup \{-1\}}$ of sets of states is defined recursively by the conditions:

$$Q_{-1} = \varnothing$$
$$Q_0 = \{q_0\}$$
$$Q_{i+1} = \bigcup\{\{\delta(q,a)\}: a \in \Sigma \wedge q \in Q_i\}.$$

Each Q_i is decidable and finite. $\bigcup\{Q_i: i \in \omega\}$ is the collection of accessible states of $\mathfrak{M}$. Now, we set, for $i \in \omega$,

$$R_i = Q_i \backslash \bigcup\{Q_j: j < i\}.$$

R_i is the collection of states which are "newly reached" at stage i, in other words, the set of those states which are accessible from q_0 by processing some word of length i but which were not accessible by processing any word of shorter length. All the R_is are finite and decidable.

As Q is itself D-finite, it is impossible that R_i be inhabited for all i. Further, since $R_i = \varnothing$ is always decidable, we have that [*] is true:

[*] $\neg\neg\exists i.R_i = \varnothing.$

We then assume [**], where [**] is [*] less the double negative prefix:

[**] $\exists i.R_i = \varnothing.$

The decidability of $R_i = \varnothing$ permits us to pick an m to be the least i such that $R_i = \varnothing$. We define S to be the finite set

$$\bigcup\{Q_i: i < m\}.$$

Let $\mathfrak{N}$ be the DFA with S as its set of states, δ restricted to $S \times \Sigma$ as its transition function and as final states the intersection of S with $\mathfrak{M}$'s set of final states. The initial state is unchanged. A simple constructive argument shows that $\mathfrak{M}$ and $\mathfrak{N}$ are equivalent.

But this conclusion follows from [**], whereas we are only allowed to assume [*]. Thankfully, the restoration of [*] to its rightful place in the argument affects only the size of S. Using [*], we can define $\mathfrak{N}$ and prove it equivalent to $\mathfrak{M}$ but we can conclude only that $\mathfrak{N}$ is an SDFA.

Note [for the foundationally wary]: The proof of the theorem is readily formalizable in a weak fragment of second-order Heyting arithmetic.

Corollary *When $\mathfrak{M}$ is a DDFA, $L(\mathfrak{M})$ is $\neg\neg$ regular.*

Corollary *Let $\mathfrak{M}$ be a DDFA. Then, if $L(\mathfrak{M})$ is D-finite, it must be semifinite. As a result, no nonfinite D-finite set can be accepted by a DDFA.*

Proof: This comes to us courtesy of the Pumping Lemma, by which we know that any regular language is either finite or infinite. Hence, if a language is accepted by a semifinite DFA and if it is not finite, then it is $\neg\neg$ infinite. Therefore, no nontrivial D-finite set can be D-regular.

Understandably, this result puts a limit on the sorts of sets which can be D-regular but not regular. As the proof of the theorem shows, the passage from D-finite to finite acceptors boils down to the transition from [**] and [*]. As it happens, the correctness of the transition is equivalent to a well-known constructive principle. Markov's Principle for sets (or MPS) is the claim that, for all $S \subseteq \omega$,

$$[\forall n(n \in S \vee \neg n \in S) \wedge (\neg\neg\exists n.n \in S)] \rightarrow \exists n.n \in S.$$

My [23] is a sampler of the mathematical relations between forms of MPS and the arithmetic on Dedekind finite sets. To cite a characteristic example, MPS is equivalent, in intuitionistic set theory or higher-order arithmetic, to the Myhill–Nerode Extension Lemma. MPS also keeps a high profile in the nonstandard theory of automata:

Theorem *MPS is equivalent to the statement that every DDFA is equivalent to a DFA. Hence, MPS is equivalent to the statement that every DDFA accepts a regular set.*

Proof: Obviously, MPS will license the direct replacement of [*] by [**] in the last main proof.

Conversely, assume that S is a decidable subset of ω:

$$\forall n(n \in S \vee \neg n \in S),$$

and that it is almost inhabited:

$$\neg\neg\exists n.n \in S.$$

Let $\mathfrak{M}$ be the DDFA wherein the set of states is the D-finite set

$$Q = \{m\colon \forall n < m \neg n \in S\} \cup \{x\}.$$

x is intended to be distinct from any member of $\{m\colon \forall n < m \neg n \in S\}$ and will serve as a "trap state". We take 0 to be the initial state and let the transition function be given by the recipe

$$\delta(q,a) = \begin{cases} q+1 & \text{if } q+1 \in Q \\ x & \text{otherwise.} \end{cases}$$

Finally, a state q of $\mathfrak{M}$ will be final whenever it is prime.

$\mathfrak{M}$, so defined, is a DDFA. The only words (over $\{0,1\}$) which $\mathfrak{M}$ accepts are of prime length. By assumption, $\mathfrak{M}$ is equivalent to a finite DFA with n states. Let p be the least prime larger than n. Simple reasoning—starting from the Pumping Lemma—shows that p does not belong to Q. Therefore, $\exists n.n \in S$ and MPS is shown to be correct.

Note [more for the foundationally wary]: The equivalence of the theorem is provable in any suitable fragment of second-order Heyting arithmetic.

As we mentioned, MPS is independent of intuitionistic set theory. A very simple construction with topological models shows this: MPS fails over the structure whose Heyting values are the open sets of the order topology on the ordinal $\omega + 1$. ([10] provides a concise introduction to the construction of Heyting-valued universes.) Even though MPS is equivalent to some of the major structure theorems on the D-finites, it can fail under intuitionistic conditions which are still sufficient to guarantee for the D-finites a sensible arithmetic. For example, the closure of the D-finites under arbitrary combinatorial operations is a consequence of the double negation of MPS, which holds under the $\omega + 1$ interpretation just described (cf. [23] for details). As a consequence, such an intepretation validates a theory of D-finite machines in which machines can be manipulated just as we do in the ordinary theory. But the extension of "computable set" in the interpretation is extraordinary: the collection of D-regular sets fails to be countable.

To fill in the details, we let ω have the discrete topology and adjoin another element called '$\omega + 1$'. The open neighborhoods of $\omega + 1$ are stipulated to be the sets

$$X \cup \{\omega + 1\},$$

where X is a cofinite subset of ω. This gives the standard order topology τ on the ordinal $\omega + 1$. Preparatory to a study of the internal mathematics of $\mathrm{V}(\tau)$, we present a general result:

Theorem *Let A be a decidable, semifinite, initial segment of ω which has 0 as a member. The set*

$$\{0^n\colon n \in A\}$$

is D-regular.

Proof: If A is semifinite, then so is $B = A \cup \{a\}$ where $a \in \omega$ is not a member of A. Let $\mathfrak{M}$ be the DDFA where

$$\mathfrak{M} = \langle B, \Sigma, \delta, q_0, F\rangle$$

and in which $\Sigma = \{0,1\}$, $q_0 = 0$, while δ is given by setting, for $x \in A$,

$$\delta(x,0) = \begin{cases} x+1 & x+1 \in A \\ a & \text{otherwise.} \end{cases}$$

The only other value of δ is a. As A is itself decidable, δ is correctly defined. We set $F = A$.

Clearly, the acceptance language of $\mathfrak{M}$ is

$$\{0^n\colon n \in A\}.$$

It follows from the theorem that, to prove that there may be more than countably many D-regular sets in $\mathrm{V}(\tau)$, it is enough to present a suitable collection of decidable, semifinite initial segments on ω.

Theorem *$V(\tau)$, as described above, contains a class of D-regular sets over the alphabet $\{0\}$ which fails to be countable. $V(\tau)$ does not satisfy MPS but does satisfy its double negation.*

Proof: For the sake of this proof alone, our reliance upon classical reasoning will be unabashed.

Let f be any strictly increasing endofunction on ω and let Incr be the collection of all such functions. Let X_f be the internal set whose membership conditions are determined by the cofinal segments of ω above the values f:

$$X_f = \{\langle n, \{m\colon m \geq f(n)\} \cup \{\omega + 1\}\rangle\colon n \in \omega\}.$$

Now, let Seg be the internal collection of such sets understood as "global elements":

$$\mathrm{Seg} = \{\langle X_f, \omega \cup \{\omega + 1\}\rangle : f \text{ is as above}\}.$$

Internally, Seg contains only decidable semifinite initial segments of ω. If we now assume that

$$\mathrm{V}(\tau) \models \mathrm{Seg} \text{ is countable},$$

then there is a $\mathrm{V}(\tau)$-internal object H such that

$$\omega + 1 \in \|H\colon \omega \to \mathrm{Seg}\|,$$

and

$$\omega + 1 \in \|\forall X \in \mathrm{Seg}\ \exists n\, X = H(n)\|.$$

Therefore, for each of the strictly increasing ω-sequences f, we can (with classical metalogic) select a least $n \in \omega$ such that

$$\omega + 1 \in \|X_f = H(n)\|.$$

Let J be the function which makes this selection. If we assume that J identifies increasing functions f and g, then we know that

$$\omega + 1 \in \|X_g = X_f\|.$$

It follows at once that one or the other of f and g agree at all but finitely many of their inputs.

Now, we say that $f \equiv g$, for strictly increasing f and g, whenever they agree at all but finitely many points. $\equiv$ is obviously an equivalence relation on Incr and our reasoning has shown that $J\backslash\equiv$ will map the quotient set $\mathrm{Incr}\backslash\equiv$ monomorphically into ω. But this is impossible because $\mathrm{Incr}\backslash\equiv$ must contain uncountably many distinct equivalence classes of functions.

Therefore, in $\mathrm{V}(\tau)$, the collection of D-regular sets fails to be countable.

A trivial calculation suffices to show that $\mathrm{V}(\tau)$ does not satisfy MPS but does satisfy its double negation. From the latter principle, one can easily prove the closure of the class of D-finite sets under all combinatorial operations.[18]

5.2.1 Dedekind-Turing machines We find the situation here very much the same: MPS supports Church's Hypothesis for D-finite Turing machines and, in structures which refute MPS, there need not be countably many D-recursive sets. However, there is at least one difference; the relevant instance of Church's Hypothesis,

every D-finite Turing machine is equivalent to a finite Turing machine,

is not equivalent to MPS; it follows from CT and does not imply MPS.

Definition $\mathfrak{M}$ is a *Turing machine* when it is a quintuple

$$\langle Q, \Sigma, \delta, q_0, h\rangle,$$

where Q is a set of states, Σ is the input alphabet, $q_0 \in Q$ is the initial state, h is the halting state (which does not belong to Q), and δ is the transition function. δ maps $Q \times \Sigma$ into $(Q \cup \{h\}) \times (\Sigma \cup \{L,R\})$. These notions and those of partial function computed by $\mathfrak{M}$, r.e. set, and equivalence of machines get the definitions familiar from [13].

Definition A Turing machine is finite (or a TM) whenever its set of states Q is finite. It is *D-finite* (or a DTM) iff its set of states is D-finite. Lastly, it is said to be *semifinite* (or constitute an STM) iff Q is semifinite.

Theorem *A machine is a DTM iff it is equivalent to an STM.*

Proof: Every STM is, trivially, a DTM. For the converse, we begin with the DTM

$$\mathfrak{M} = \langle Q, \Sigma, \delta, q_0, h \rangle,$$

and define the obvious associated DDFA

$$\mathfrak{N} = \langle Q \cup \{h\}, \Sigma, \rho, q_0, F \rangle,$$

wherein ρ is such that, when q is not h, it maps $\langle q, a \rangle$ into the value given by composing δ with the left projection and applying the composition to $\langle q, a \rangle$. If $q = h$, then $\rho(q,a) = h$.

Using our proof of the equivalence theorem for DDFAs, we can construct from $\mathfrak{N}$ an equivalent SDFA. The set of states from this acceptor can be used to construct an STM which is clearly equivalent to $\mathfrak{M}$.

Because of the way in which the results of the preceding section have entered into our current effort, we know immediately that

Corollary *MPS implies that every DTM is equivalent to a TM. Hence, MPS implies that every DTM accepts an r.e. set.*

The converse of the corollary is intuitionistically correct if we agree that the following form of CT is true.

CT Every total natural number function is recursive.

Let Equiv be the statement that

every DTM is equivalent to a TM

and let **D** be

every decidable, semifinite initial segment of ω is recursive.

Then, we can prove

Lemma *Equiv holds iff* **D**.

Proof: First, assume Equiv and let Q be a decidable, semifinite initial segment of the natural numbers. As Q is semifinite, it is D-finite and we can easily construct a DTM $\mathfrak{M}$ with Q a collection of its states and such that $\mathfrak{M}$ determines membership in Q. Therefore, Q is recursive and **D** is validated.

On the other hand, we can assume **D** and let

$$\mathfrak{M} = \langle Q, \Sigma, \delta, q_0, h \rangle,$$

be an arbitrary DTM. By our earlier results, we may take it that Q is semifinite. In fact, it would be correct to say that both Q and δ are decidable, semifinite initial segments. Given **D**, Q and δ are recursive sets of natural numbers. It follows that the partial function computed by $\mathfrak{M}$ is Σ_1-definable. Therefore, Equiv holds.

As CT obviously implies Equiv, we have

Corollary *CT implies that every DTM has an equivalent TM.*

There are reasonable and well-behaved intuitionistic universes in which Equiv fails. To name one, there is the $V(\tau)$ structure described earlier. In this structure, the collection Seg consists of decidable, semifinite initial segments, all of which are nonrecursive. Here, the collection of sets accepted by D-finite Turing machines must fail to be countable. This offers us a clear concept of machine: we permit a Dedekind finite collection of states but require that the rest of the parameters take strictly finite form. For this concept, we cannot prove the corresponding instance of CH, even for regular events.

NOTES

1. I will not attempt exegesis of the philosophical views or mathematical results of the historical Brouwer. I believe that, in describing intuitionism, we need be no more exegetical of Brouwer than a contemporary set theorist would need be of Cantor. As will be painfully clear, there are any number of points on which we would disagree with the historical Brouwer. Solipsism and mentalism are only two.
2. Needless to say, the expression 'a proof of RH is available to me' is itself shorthand for a fully reduced expression which does not contain the usual formulation of RH.
3. This argument also provides a counterexample to the weak negative form the $\mathfrak{F}$CT: Every number-theoretic function is $\neg\neg\mathfrak{F}$-definable. To some intuitionists, such weak forms of CT are palatable, even if full CT is not.
4. The traditional intuitionists seemed to be willing to countenance a prospect which would undermine the reductive use of the notion of the supermathematician. Apparently, they allowed that what would count as a proof to me might not count as such to my counterpart. For instance, assume that some mathematical knowledge of mine had been obtained in virtue of my having a proof containing an essential subproof of an implication $A \to B$. Then, since my counterpart might recognize more things as acceptable proofs of A than I would, my proof (which would be an operation which, for me, converts proofs of A into proofs of B) might not work for him. Hence, were this prospect to be a real possibility, I could have a perfectly acceptable mathematical proof without having any assurance that my counterpart would act accordingly. Were the counterpart idea to be of any reductive use, one would have to banish any such possibility.
5. Were we to push the issue of algorithms far enough, we would come up against the "Kripke-Wittgenstein" Paradox. For the intuitionist, there is no paradox—the

reasoning employed by Kripke's "skeptic" is thoroughly nonconstructive. Our attitude toward the "paradox" is described in [24].

6. The obvious rejoinder is not open to the reductionist. It cannot be claimed that notions such as arithmetic truth, which we know to be inexpressible on the basis of the Gödel–Tarski Theorems, are not mathematically respectable. However, to see why this is so, we will have to take up the concept of intuitionistic truth. This we shall do at a later stage.

7. This argument is a version of the familiar Tarski "fixed-point" argument due, we believe, to Kaplan and Montague [16]. We are ignoring some of the niceties of arithmetization, viz., the intensional distinction between formal provability and its coded analogue.

8. One is moved to point out that arguments have been presented for removing negation from intuitionistic mathematics altogether (cf. [11]). Nor is the interest of these considerations merely historical or philosophical. It is known that intuitionistic means suffice to prove the completeness of the negation-free fragment of Heyting's predicate logic with respect to interpretations over Beth trees. No full completeness theorem is obtainable by the use of strictly intuitionistic means.

9. Dummett seems to plump for the centrality of bivalence in his "Preface" to the *Truth and Other Engimas* collection.

10. In speaking informally of 'probjects', I am gesturing toward the members of the App models described by Feferman in [7] and discussed in [1].

11. This does mark a turning away from the view that intuitionism is a form of "antirealism", the idea so thoroughly marketed by Dummett [6], Wright [41], and others. On these accounts, all the heavy foundational work would be contracted out to the epistemologists. Presumably, they would try to devise and to justify a proof conditional semantics with the aid of a sanitized Wittgensteinian theory of knowledge and meaning. Needless to say, this sort of foundation is not, by our lights, "antimetaphysical".

12. We are thinking of the logical signs in use on the right sides of 1, 2, and 3 as themselves intuitionistic. Our construal of this semantics is not intended to be reductive. Without any strain other than peculiarity, one could take the signs in use to be classical.

13. Needless to say, I believe that the needed "regularization" of Heyting's work has already been given by Kleene. The intuitionists who are so keen to reject Kleene's interpretation as nonstandard or construtively incorrect may be somewhat overanxious. Kleene's interpretation is so clear, clean, attractive, and subtle that anyone would have to muster substantial reasons for rejecting it.

14. It should now be painfully clear why Brouwer was appalled by the prospect of logicism. It is (intuitionistically) inconceivable that one extract an understanding of the fundamentals of mathematics from a proper understanding of the logical signs. The only way to come to an understanding of the intuitionistic signs is by way of a knowledge of a nontrivial part of mathematics, namely, the mathematics of probjects. Consequently, the last displayed line would be hopeless as a definition and is not intended as such.

15. I believe that the intuitionist can resist the demands of Church's Thesis. But he cannot merely cite isolated pieces of traditional intuitionistic mathematics which appear to contradict it (for example, the Fan Theorem or the Brouwer–Kripke Scheme) but

has to provide an explication of the sense in which the functions of natural numbers computed by probjects are computable. To succeed, the explication must be rigorous and yet differ in some respect from that of Turing and Church. If such an explication does not exist, Church's Thesis is, for better or for worse, an inevitable consequence of the intuitionistic standpoint. There are interpretations of intuitionistic mathematics which suggest means for circumventing CT in a foundationally respectable fashion. One of these is realizability over the r.e. substructure of the Scott–Plotkin graph model [34]. Here, Full CT is false but WCT or Weak Church's Thesis is realized:

$$\forall f((f\colon \mathfrak{N} \to \mathfrak{N}) \to \neg\neg\exists n\, f[\mathfrak{N} = \{n\}).$$

This is a consequence of a form of 'every function on $\mathfrak{N}$ is computable' which retains many of its attractions while avoiding some consequences which have been thought unfortunate. An interesting application of WCT awaits us in the next section.

16. Beeson's actual discussion may not be as negative in intension as my presentation might suggest. Beeson does allow that

> the world under Church's thesis is an entertaining place, full of surprises (like any foreign country), but not by any means too chaotic to support life.

However, he is not perhaps of one mind about this; he later suggests that the purpose of his tour through foreign mathematical climes has a thoroughly negative motivation:

> The extensive presentation of recursive analysis is of interest here mainly because it shows us what *not* to try to prove constructively.

Our view is quite the opposite: recursive mathematics is not just a travelogue; its great interest arises, in part, because it shows us what to *try* to prove intuitionistically.

17. It is interesting to note that, in the presence of CT, individual D-finite subsets of ω correspond with the *isolated* sets of classical recursion theory and the cardinality-types of the D-finites coincide with recursive equivalence types which are the isols.

18. The use of subfiniteness is not as productive of true alternatives to the traditional concept as is D-finiteness. A bit of simple constructive set theory will show that every acceptor with a subfinite number of states is equivalent to a DFA. This follows from the fact that every decidable subset of a finite set is itself finite. It follows immediately from this that every Turing machine with a subfinite number of control states is equivalent to a standard TM.

REFERENCES

[1] Beeson, M. J., *Foundations of Constructive Mathematics*, Springer-Verlag, New York, 1985.

[2] Davidson, D., "On the very idea of a conceptual scheme," *Proceedings and Addresses of the American Philosophical Association* (1973), pp. 5–20.

[3] Dekker, J. C. E. and J. Myhill, *Recursive Equivalence Types*. University of California Publications in Mathematics, Vol. 3, 1960, pp. 67–213.

[4] Dickens, Charles, *A Christmas Carol*, The Oxford Illustrated Dickens, Oxford University Press, Oxford 1947.

[5] Dummett, M. A. E., *Elements of Intuitionism*, The Clarendon Press, Oxford, 1977.

[6] Dummett, M. A. E., "The philosophical basis of intuitionistic logic," pp. 215–247 in *Truth and other Enigmas*, Duckworth, London, 1978.

[7] Feferman, S., "A language and axioms for explicit mathematics," pp. 87–139 in *Algebra and Logic*, Springer Lecture Notes in Mathematics, Vol. 450, Springer-Verlag, New York, 1975.

[8] Fraenkel, A. and Y. Bar-Hillel, *Foundations of Set Theory*, North-Holland, Amsterdam, 1958.

[9] Grayson, R. J., *Intuitionistic Set Theory*, D. Phil. Thesis, Oxford University, 1978.

[10] Grayson, R. J., "Heyting-valued models for intuitionistic set theory," p. 402–414 in *Applications of Sheaves*, Springer Lecture Notes in Mathematics, Vol. 753, Springer-Verlag, New York, 1979.

[11] Heyting, A., *Intuitionism: An Introduction*, North-Holland, Amsterdam, 1959.

[12] Heyting, A., "The intuitionistic foundations of mathematics," *Philosophy of Mathematics: Selected Readings*, ed. P. Benacerraf and H. Putnam, Academic Press, New York, 1960.

[13] Hopcroft, J. E. and J. D. Ullman, *Automata, Languages and Complexity*, Addison-Wesley, Reading, Massachusetts, 1979.

[14] Hyland, M. E., *Aspects of an Effective World*, Lecture at the Utrecht conference on Church's Thesis, June 1986.

[15] Joyce, James, *A Portrait of the Artist as a Young Man*, Penguin, New York, 1965.

[16] Kaplan, D. and R. Montague, "A paradox regained," *Notre Dame Journal of Formal Logic*, vol. 1 (1960), pp. 79-90.

[17] Kleene, S. C., "An interpretation of intuitionistic number theory," *The Journal of Symbolic Logic*, vol. 10 (1945), pp. 109–124.

[18] Kripke, S. A., *Wittgenstein on Rules and Private Language*, Harvard University Press, Cambridge, Massachusetts, 1982.

[19] McCarty, C., *Realizability and Recursive Mathematics*, D. Phil. Thesis, Oxford University, 1984; also Technical Report CMU-CS-84-131, Department of Computer Science, Carnegie-Mellon University.

[20] McCarty, C., "Realizability and recursive set theory," *Annals of Pure and Applied Logic*, vol. 32 (1986), pp. 153–183.

[21] McCarty, C., "Constructive validity is nonarithmetic," *The Journal of Symbolic Logic* (to appear).

[22] McCarty, C., *Computation and Construction.* Oxford University Press (book in preparation).

[23] McCarty, C., "Markov's Principle, isols and Dedekind finite sets," *The Journal of Symbolic Logic* (to appear).

[24] McCarty, C. and B. Scholz, "On the Kripke–Wittgenstein Paradox" (in preparation).

[25] McCarty, C. and N. Tennant, "Skolem's Paradox and constructivism," *The Journal of Philosophical Logic*, vol. 16 (1987), pp. 165-202.

[26] McDowell, J., "On the sense and reference of a proper name," pp. 42-66 in *Truth and Meaning*, ed. G. Evans and J. McDowell, Oxford University Press, Oxford, 1976.

[27] Moggi, E., Personal communication, Edinburgh University, July 1986.

[28] Powell, W. C., "Extending Gödel's negative interpretation to ZF," *The Journal of Symbolic Logic*, vol. 40, 1975, pp. 221-229.

[29] Prawitz, D., "Meaning and proofs: On the conflict between classical and intuitionistic logic," *Theoria*, vol. 43, 1976, pp. 2-40.

[30] Prawitz, D., "Proofs and the meaning and completeness of the logical constants," pp. 25-39 in *Essays on Mathematical and Philosophical Logic*, ed. J. Hintikka, I. Niihiluoto, and E. Saarinen, D. Reidel, Dordrecht, 1979.

[31] Rabin, M. O., "Lectures on classical and probabilistic automata," pp. 304-313 in *Automata Theory*, ed. E. R. Caianiello, Academic Press, New York, 1966.

[32] Reynolds, J., "Polymorphism is not set theoretic," pp. 145-154 in *Semantics of Data Types, Lecture Notes in Computer Science*, vol. 173, 1984.

[33] Rogers, H., *Recursive Functions and the Theory of Effective Computability*, McGraw-Hill, New York, 1964.

[34] Scott, D. S., "Data types as lattices," *SIAM Journal on Computing*, vol. 5 (1976), pp. 522-587.

[35] Scott, D. S., "Domains for denotational semantics," pp. 577-613 in *ICALP'82, Automata, Languages and Programming, Springer Lecture Notes in Computer Science*, Vol. 140, Springer-Verlag, New York, 1982.

[36] Scott, D. S., *Modest Sets*, Lecture at the Utrecht conference on Church's Thesis, June 1986.

[37] Tarski, A., "The concept of truth in formalized languages," pp. 152-278 in *Logic, Semantics, Metamathematics*, trans. J. H. Woodger, Clarendon Press, Oxford, 1956.

[38] Tennenbaum, S. "Non-archimedean models of arithmetic," *Notices of the American Mathematical Society*, vol. 6 (1959), p. 270.

[39] Trakhtenbrot, B. A. and Ya. M. Barzdin, *Finite Automata: Behavior and Synthesis*, North-Holland, Amsterdam, 1973.

[40] van Dalen, D., *Logic and Structure*, Springer-Verlag Universitext, New York, 1980.

[41] Wright, C., *Wittgenstein on the Foundations of Mathematics*, Duckworth, London, 1980.

Department of Computer Science
University of Edinburgh
Edinburgh, Scotland, UK

and

Department of Philosophy
The Florida State University
Tallahassee, Florida, USA 32306