Knowledge of proofs*

by Peter Pagin

1. Epistemic constraints on proofs

In the main current of contemporary intuitionism, truth is equated with the availability of proof, or verification.[1] The philosophical underpinnings vary somewhat, but anti-realism is a common denominator. Anti-realism can be a basic stance.[2] You can find it incomprehensible e.g. how some numbertheoretic statement nAn could be true in the absence of proof. What could it possibly amount to for every instance A(1), A(2), A(3)… to simply be true, if we could not verify that each of them is true? And this we cannot do for each instance separately. There are also meaning theoretic arguments for intuitionism, or at least against classical logic. I shall return to that issue later.

What is a proof, say in mathematics? The concept of a mathematical proof is partly mathematical, partly epistemological. A proof is a mathematical construction. We can specify formal properties of proofs. If we are dealing with some formal system S, we can even give an inductive definition of the concept proof-in-S. But we need a different conception if we shall understand why such a definition is a definition of a predicate which applies precisely to proofs in the general sense. This is analogous to what holds for Tarskian truth definitions. As little as we have an inductive defintion of true-in-L for variable L do we have an inductive defintion of proof-in-S for variable S. In other words, as we cannot define inductively what is common to all true sentences we cannot define inductively what is common to all mathematical proofs.

The general concept of a proof is something like: a proof is something that establishes the truth (or correctness, or validity) of its conclusion. But what does "establishes" mean here? Does it mean anything more than this:

(1) if there is a proof for p, then p

But if that were all there is to the general concept of proof, then there would be nothing wrong with saying that the very fact that every instance A(1), A(2), A(3)… is true is a proof for the statement that nAn[3] . Clearly, if every instance is true, then the universal is true. So there must be something more to a proof than being mere truth maker or truth guaranteer.

The mistake was that the epistemological ingredient in the concept had been left out. But it will not do to just add epistemic qualifications to the conditional:

(2) if a proof for p is known (to be a proof for p), then it is known that p

This much follows almost from (1). That is, if someone knows that (1) is true, and knows a proof for p (to be that), then he can simply conclude by (existential generalization and) modus ponens that p is true. Clearly, as it stands principle (2) provides as little, or almost as little, by way of epistemic constraint as does (1). If it is known that the infinitely many instances A(1), A(2), A(3)…are true (and that the inference to the universal is valid), then it is also known that the universal is true.

The problem was that the conditional (2) is true, even vacuously true, if the proof (for some p) isn't knowable at all. We need further to impose the condition that it is possible to know the proof, i.e. to recognize it as a proof of what it proves. But again, the nature of this possibility is not altogether transparent. Michael Dummett writes

> To say [that when a statement is proved, then it is shown thereby to have been true all along] is, in effect, to equate 'A is true' with 'We can prove A' rather than with 'A has been proved', and 'A is false' with 'We cannot prove A'. Such an interpretation remains faithful to the basic principles of intuitionism only if 'We can prove A' ('A is provable') is not interpreted to mean either, at one extreme, that, independently of our knowledge, there exists something which, if we became aware of it, we should recognize as a proof of A, nor, at the other, that as a matter of fact we either have proved A or shall at some time prove it. In the former case, we should be appealing to a platonistically conceived objective realm of proofs; in the latter, we should be entitled to deny that A was provable on non-mathematical grounds (e.g. if the obliteration of the human race were imminent).[4]

One way to understand the main point (or perhaps to state a closely related one) is that we render the concept of knowledge capacity, or possibility of knowledge, epistemologically void if we appeal to some platonistic objective realm of proofs as a sufficient condition for the possibility of knowledge. That is, if we subscribe to

(3) it is possible to know that A is true iff there is a proof of A

and think of the realm of proofs as a pre-existing domain of platonic proof objects, then there is no longer any epistemological content to the general schema "it is possible to know that A is true". It appears that then we have eliminated the epistemological ingredient from the concept of a mathematical proof.

Against this view of Dummett's, however, Dag Prawitz writes:

> I fail to see this, however, since in such an objective realm of proofs there can be no question of the existence of a proof that is not in principle recognizable by us. This is so because a proof is by its very nature something that is related to our recognitional capacities, unlike classical truth conditions that are understood as possibly obtaining although we may be in principle unable to recognize that they obtain.[5]

What is Prawitz's point? It seems to be that there is nothing wrong with conceiving of mathematical proofs as platonic and preexisting as long they *are* knowable, i.e. as long as they satisfy some epistemic constraints, moreover, constraints relating to *our* capacities. If satisfying epistemic constraints is part of our *concept* of a proof, then it is correct to say that it is in the nature of a proof to be knowable. But to say this is, in a sense, to restate the question: what *are* the epistemic constraints on proofs?

Suppose we formulate the following constraint:

(4) if something is a proof, then it we can recognize it as a proof

There is an immediate ring of implausibility about (4). Clearly it is too much to require that *we*, with all our limitations, should be able to recognize all proofs. What about proofs that are too complex, that would take more than a lifetime just to read through? But then again, who says that there *are* such proofs? We should be consistent and apply verificationist reasoning when we talk about proofs. What could, after all, amount to a *verification* of the existence of proofs that we are unable to recognize as proofs?

Still, such results seem not hard to come by. Consider the intuitionistic explanation of the meanings of the logical constants in terms of *direct* or *canonical* proofs.[6] We need canonical proofs for a correspondence between the form of proofs and the form of propositions proved. Thus a canonical proof of conjunction *A* & *B* is a pair a,b where a is a proof of *A* and b is a proof of *B*, which is to say that a canonical proof of *A* & *B* has as its immediate subderivations a proof of *A* and a proof of *B*. A proof in general of a conjunction need not look like this. There are also non-canonical proofs, and they are conceived of as *methods* for arriving at canonical proofs. Hence, if there is a proof of *A*, then there is a canonical proof of *A*.

For arriving at canonical proofs from non-canonical ones we apply reductions.[7] For instance, a non-canonical proof of B may look like this:

$$\dfrac{\dfrac{\begin{array}{c}A\\ \Sigma\\ B\end{array}}{A \rightarrow B} \qquad \begin{array}{c}\Pi\\ A\end{array}}{B}$$

where ∏ represents a proof of A. Suppose that B is a conjunction C&D, and that the derivation of B from A has the required form, i.e. has two immediate subderivations of the conjuncts of B. Now this proof of B can be directly transformed into a canonical proof of B by appending the proof ∏ of A to the assumption A in the derivation of B from A.. So it will look like this:

$$\begin{array}{c}\Pi\\ A\\ \Sigma\\ B\end{array}$$

But now suppose that the proof ∏ of A is extremely complicated. It may take most of a human lifetime to check. Suppose also that the derivation of B from A is quite complicated, and that in fact A occurs as a premiss in that derivation no less than 1000 times. All these occurrences are simultaneously discharged at the → introduction in the non-canonical proof. Then the canonical proof of B will in fact have 1000 occurrences of the proof ∏ of A . So a simple checking of the canonical proof would require much more time than is humanly possible to spend. Hence no human being can do it.

The non-canonical proof satisfies the epistemic constraints. The canonical proof does not. So, given (4), we must conclude that it is not really a proof. But we can still produce a much shorter canonical proof, by way of making the proofs of the conjuncts non-canonical:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\underline{A}\\ \Sigma\\ \underline{C}\end{array}}{\underline{A}\to\underline{C}} \qquad \begin{array}{c}\Pi\\ \underline{A}\end{array}}{\underline{C}} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\underline{A}\\ \Sigma\\ \underline{D}\end{array}}{\underline{A}\to\underline{D}} \qquad \begin{array}{c}\Pi\\ \underline{A}\end{array}}{\underline{D}}}{\underline{C}\&\underline{D}}$$

This canonical proof only contains two occurrences of the proof Π of A. The increase in size is not as dramatical as before, but given the assumption about the size of Π, even this is beyond human capacity to check. So again we infer from (4) that it is not really a proof. Moreover, we are free to assume that there are no shorter proofs of A, C and D, and hence no shorter canonical proof of C&D. If we adhere to (4), then we must deem that there *is* no canonical proof.[8] So we must conclude that (4) is inconsistent with the intuitionistic meaning explanations, since these require that if there is a proof, then there is also a canonical proof.[9]

Can't we say simply that (4) is refuted? We know that we are in possession of a general method for transforming non-canonical into canonical proofs. Does this not simply establish the existence of the canonical proof? No. Properly speaking, what we know is that we are in possession of a general method of transforming particular non-canonical *constructions* into canonical *constructions*. The existence of this method together with the existence of the non-canonical construction does establish the existence of the canonical construction, a mathematical object. Whether or not that construction is also to be regarded as a *proof* is another question. There is no problem in accepting the existence of the canonical proof if no restriction like (4) is imposed, but if it is, then there is no mathematical demonstration of the existence of the canonical proof.

The intuitionist who defends this kind of explanation of the meanings of the logical constants must therefore reject the suggested epistemic constraints on proofs. But this still seems to be in accordance with the general intuitionistic outlook. The intuitionist does not accept any finite bounds on mathematical capacity. The only restriction is that for each solvable problem there be *some* finite capacity sufficient for in practice solving the problem. Dummett has stressed this many times.[10] We cannot understand what it would be to have the capacity to check infinitely many inferences in finite time, but we can understand what it would be to have finite extensions of our actual capacities, and this is all we need.[11] The canonical proof in our example does exist, since it requries only a finite extension of our capacities to check it in detail.

2. Unknowable propositions

We apparently have at least a preliminary answer to our question about the epistemological character of the concept of a proof. Proofs must be recognizable as such by beings with some finite extension of our cognitive capacities. However, some very peculiar statements seem to threaten this constraint on proofs.

Consider

(5) the number of library copies of Word and Object on October 1st 1993 is odd

Disregard vagueness and open texture, what to count as a copy, etc. I take it that (5) is either true or false, that a decision of it is or could be effectively carried out. But it is safe to say that no one will ever bother to do the counting. As time goes on it will be more difficult to establish a result, and far enough into the future there is no telling (today) how to do it (then). Then we have as candidates for being true sentences

(6) (5) is true and (5) will not ever be verified

(7) (5) is false and (5) will not ever be falsified

Intuitiviely, either (6) or (7) is true. But neither can be known to be true. For suppose that (6) is true, and that NN has come to know this. Then we can credit NN with a knowledge also that (5) is true. But then (5) has been verified, so the second conjunct of (6) is false. Hence (6) is false, contrary to the assumption. The step in the argument from knowing the truth of a conjunction to knowing the truth of the conjuncts (or of its left conjunct), is perhaps not completely trivial, but still I think that there is better support for the step than there is for doubting it.

(6) and (7) have the form of sentences crucially figuring in what has come to be known as Fitch’s paradox.[12] I shall here consider one possible response on the part of the intuitionist to porblems created by that paradox, which essentially are the problems created by our example.

Clearly (6) and (7) pose a problem for both the classical and the intuitionistic verificationist.

It appears that one of these sentences is true, and that it cannot be verified. If that is so, then verificationism, i.e. the thesis that

(8) if a statement is true, then it is verifiable

seems simply refuted. Either (6) or (7) is a counterexample. But, of course, things are not that simple.

There are some possible escape routes. One is to try to save verificationism by weakening it, i.e. by rejecting (8) and replacing it by some other principle which still captures the verificationist's basic point of view.[13]

Another is to reject the assumption that either (6) or (7) is true. If neither can be known, then neither is true. Both are false and their negations true. But the consequences aren't welcome. The negation of (6) is classically equivalent with

(9) if (5) is true, then (5) will at some time be verified

But (9), intuitively understood, is clearly absurd. We have no reason whatsoever to believe it. Moreover, we can put in any sentence in place of (5). The general result is that all true sentences will be verified. Recall the quotation from Dummett

> […], nor, at the other, that as a matter of fact we either have proved A or shall at some time prove it. In the former case, we should be appealing to a platonistically conceived objective realm of proofs; in the latter, we should be entitled to deny that A was provable on non-mathematical grounds (e.g. if the obliteration of the human race were imminent).

It seems that if accepting (9) is the alternative to rejecting verificationism, then the latter alternative is preferable. But again things are less simple. The verificationist can defend (9), by appealing to a verificationist understanding of conditionals: a conditional is true iff [if there is a verification of the antecedent, then there is a verification of the consequent]. By this understanding of conditionals (9) would indeed come out true. The problem is that this interpretation, for cases like (9), apparently <u>distorts</u> the meaning.

But the intuitionist need not take this line, since (9) does not follow intuitionistically from the negation of (6).[14] What does follow, however, is the contraposition

(10) if (5) will not ever be verified, then (5) is not true

This is, intuitionistically, not the same as saying that the truth of a statement consists in its being verified at some time, but it sounds almost as bad, since it amounts to saying that the falsity of a statement consits in (or at least is equivalent to) its never being verified. This can hardly be what the intuitionist intended.

Still, there is a case for (10). The antecedent of (10) involves quantification over an infinite totality, viz. all future times. Hence it is not possible, i.e. not for finite beings, to verify it by checking for each time that (5) has not been verified. Neither could we really know that it will not be verified if our basis for believing so was that the obliteration of the human race were imminent. Other beings might verify it. Rather, a verification of the antecedent of (10) must be of a more principled nature. The only definitive obstacle (that we can know of) to ever verifying (5) would be its falsity. Thus, again, if the truth of the antecedent consists in there being a verification of it, then (10) is true, since a verification of the antecedent must involve a falsification of (5).[15]

So, a hardheaded intuitionist can defend (10) and conclude that there is no problem after all. But this way out will not satisfy the intuitionist who retains a solid common sense. Intuitively, both (6) and (7) can be true. Intuitively, a statement may be true and yet never verified. In fact, we have excellent reasons to think that such statements abound. As in the (classical verificationist's) defence of (9), we seem to have a distortion of meaning.

Dummett has written about the origin of the concept of truth.[16] He observes that if sentences would only be used by themselves for making categorical assertions, then we would not have any need for distinguishing between truth and correct assertibility. The relevant notion of correct assertibility is this: if a statement is correctly assertible, then it is true, but it can be true without being correctly assertible, viz. if there is not sufficient evidence at hand. Since the conditions for correctly asserting p are the same as the conditions for correctly asserting "it is correctly assertible that p", we could substitute the one for the other salva veritate if simple assertions were all there is to assertoric usage. But there are contexts where this equivalence does not hold, in particular antecedents of conditionals.

(11) if (it is true that) the total amount of matter exceeds x, then the universe will contract

(12) if it is correctly assertible that the total amount of matter exceeds x, then the universe will contract

clearly do not have the same meaning. In fact, as material conditionals (11) may be false and (12) true, i.e. in case the common consequent is false and it is true, but not correctly assertible, that the total amount of matter exceeds x.

Conditionals thus provide a type of context which reflects the difference between truth and correct assertibility. The point about distortion of meaning can be brought out by a parallel.

(13) if it is verifiable that (5) will not ever be verified, then (5) is not true

intuitively does not have the same meaning as (10). (13) is arguably true, while (10) may still be false. That is, we have a distortion of the meaning of (10), if the sound argument for the truth of (13) is used also to argue for the truth of (10), and this is what the hardheaded intuitionist does.

Apparently the sentence matrix that results from deleting the occurrences of ‘(5)’ in (10) is a very special context. It seems to exhibit a lack of transparency of the intuitionistic concept of truth, i.e. as equated with verifiability. Standardly, "it is true that p" is guaranteed to be equivalent with p. This is sometimes referred to as the transparency of the concept of truth. As is shown by (11) and (12) the concept of correct assertibility does not have this property. And the pair of (10) and (13) seems to show that neither does the concept of verifiability.[17]

3. Verifications without knowledge

Then what way out remains for the intuitionist who does not want to jettison his common sense understanding of (6), (7) and (10)? Must he not give up his equating of truth with verifiability? Indeed he must. But verifiability, as the notion has been used, is complex. It involves on the one hand the component of something, like a proof object, which guarantees truth , and on the other the component of the knowability of that truth guarantee. We clearly can’t give up only the first component, but we can give up the second and hope to retain the first. That is, we can attempt to save the intuitionistic concept of truth by still equating truth with the existence of proof, or verification, while denying that proofs, or verifications, must be knowable.

But if this line is taken, the main point of section 1 is given up. There it was stressed that the epistemic constraint on proofs must be the possibility, no more and no less, of being known by some being with at most a finite extension of our cognitive powers. Now, on the other hand, we are prepared to accepts proofs that are in principle impossible to know.

This need not amount to a denial of Prawitz's words "a proof is by its very nature something that is related to our recognitional capacities". It does not if in that passage we interpret 'proof' as meaning mathematical proof. Mathematical proofs was the topic of section 1, while the problematic sentences discussed in section 2 are at least partly empirical (since they are about knowledge, verifications as acts), not purely mathematical. The problems discussed in section 2 are not obstacles to being a verificationist in the philosophy of mathematics, at least not in the sense of exhibiting unwelcome consequences of such a position.

Still there may be cause for concern. Some intuitionists[18] do intend their intuitionism to be general, to cover all areas of human discourse, not just mathematics. More importantly, the reasons for rejecting realism, and classical logic, in mathematics, may be so general that they in fact carry over to most other areas, whether or not intended by the mathematical intuitionist who appeals to them. The problem facing the intuitionist is therefore this: if we are prepared to accept the existence of proofs (verifications) that are in principle unknowable, what reasons are there for rejecting classical logic in favour of intuitionism?

Consider Dummett's famous meaning theoretical argument against classical logic, or, more precisely, against equating linguistic meaning with truth conditions, when truth is taken as supporting the principle of bivalence.[19] In briefest outline, the argument runs as follows:

1. Knowledge of the meaning of a sentence is publicly manifestable
2. Public manifestation of knowledge of the meaning of a sentence consists in exercising the ability to tell whether the central semantic concept applies to that sentence or not
3. If the central semantic concept is the realist concept of truth and the sentence not effectively decidable, then there is no ability to tell whether that concept applies to the sentence.
4. Hence knowledge of truth conditions is not (always) publicly manifestable.
5. Hence knowledge of meaning is not knowledge of (bivalent) truth conditions.
6. Hence meaning is not (bivalent) truth conditions.

The presently crucial point is Dummett's central requirement: given a sentence, and supposed given a sufficient finite extension of my cognitive capacities, I must be able to decide, that is know an effective procedure for deciding, whether the central semantic concept does or does not apply to the sentence. This is the test for any proposed semantic concept, and the realist concept of truth does not pass, since there are classes of sentences for which it is not effectively decidable whether they have the property of being true.

Now contrast the property of being (bivalently) true with the relation x is a proof of y. It has been supposed that this is an effectively decidable relation. That is, for each sentence s and each object a I can (perhaps with some finite extension of my capacities) effectively decide whether or not a is a proof of s. And so knowledge of what to accept as a proof of a sentence could pass as knowledge of the meaning of the sentence.

But this conclusion no longer holds if there are in principle unknowable proofs. If there are such proofs, it may be because they are infinite, requiring more than finite extensions of our cognitive capacities. In that case the relation x is a proof of y is not even effectively decidable in the mathematical sense. On the other hand, the proof may be finite, but it may be logically impossible for us to recognize it as the proof that it is: believing it would amount to a blindspot in the sense of Sorensen.[20] In neither case can it be claimed that someone can have the ability to tell, for each sentence s and each object a whether or not a is a proof of s.

The negative argument against meaning as bivalent truth conditions is still as good as it was before. But now the same argument also excludes the verificationist's counterconception. If this is the argument for giving up bivalent truth conditions and hence classical logic, then intuitionism must be given up as well, and if intuitionistic principles are to be retained, then other reasons for rejecting classical logic must be sought.

Perhaps the crucial sentences, those like (6) and (7), can be accommodated by slightly liberalizing requirements. Granted, it may be in principle impossible for us to recognize something as a proof of (6). But still we know very well what can be counted as a proof of (6), viz. anything that is or can be transformed into a canonical proof of (6), which is to say a pair whose first element is a proof of (5) and whose second element is a proof of the statement that (5) will never be verified. Each of these proofs is in principle available to us (we just can't recognize the pair of them as a proof of (6)), and we know the principle for forming proofs of conjunctions from proofs of their conjuncts. This should be sufficient for crediting us with knowledge of the meaning of (6), despite the fact that it is in principle impossible for us to recognize anything as a proof of it.

In my opinion this is a sound reaction. Understanding surely obeys principles of semantic compositionality to the extent that we can appeal to such principles even for justifying claims of understanding. But again this defence undercuts the reasons for rejecting classical semantics. The defender of classical logic may agree that an understanding of the logical constants must involve knowledge of canonical forms of evidence, like knowledge of the conditions for being a canonical proof of sentences of the various logical forms. Given that a person has this knowledge, he knows the significance of using those constants. If he knows the meaning of A, the meaning of B, and the meaning of $\rightarrow$, then he knows the meaning of $A \rightarrow B$ as a standard case of semantic composition. We need not require the ability to recognize proofs for this very sentence, or for each single sentence. But if that is not required, Dummett's argument is given up.

Perhaps it is better to disregard the meaning theoretical arguments and appeal directly to some basic anti-realism. Mathematical reality depends on our creativity, on our cognitive capacities. So we cannot accept classical logic in mathematics. So the motivation may run. But what is the reason for the step from anti-realism to the rejection of classical logic? Why should we think that acceptance of the law of excluded middle, or the principle of bivalence, expresses a realistic attitude? If the law of excluded middle is what logicians before Brouwer took it to be, a genuine logical law, then there should be no question of accepting it or rejecting it for particular areas of discourse. So it seems that we must first argue against the general acceptance of the law of excluded middle. What are the reasons? We may appeal to the idea of truth as verifiability. But now our argument must be general, and therefore we will have to reckon with sentences like (6), and hence with in principle unknowable proofs. And if there are no epistemic constraints whatsoever on proofs, why should the requirement of the existence of proofs lead us to doubt the law of excluded middle? Again, if proofs are no more than facts in the sense of a correspondence theory, there is no reason for doubt.[21]

To sum up. The middle section presented a complex dilemma for the intuitionist. Give up some firmly entrenched intuitions about the truth of sentences like (9), or give up the claim that what is true is knowable. The second horn is itself a dilemma: give up the claim that true statements have verifications or give up the claim that verifications are knowable.

Cautiously stated, the conclusion of the present section is this: if you are prepared to accept the existence of proofs, or verifications, that are in principle unknowable, then you will have grave difficulties in finding reasons for rejecting classical logic in favour of intuitionistic logic, i.e. reasons that will not also be reasons against intuitionism.

Department of philosophy

Stockholm University

References

Dummett, M.: 1976, 'What is a theory of meaning (II)'
Evans G and McDowell J (eds), *Truth and Meaning*, Oxford University Press, Oxford

— 1977, *Elements of Intuitionism*
Clarendon Press, Oxford

— 1980, *Truth and Other Enigmas,* 2nd ed,
Duckworth, London

— 1980a, 'The philosophical basis of intuitionistic logic'
in Dummett [1980]

Edgington, D.: 1985, 'The paradox of knowability'
Mind 94, 557-568.

Fitch, F. B.: 1963, 'A logical analysis of some value concepts'
Journal of Symbolic Logic 28, 135-142.

Heyting, A.: 1931, 'Die intuitionistische Grundlegung der Mathematik'
Erkenntnis 2, 106-115. Translated in Benacerraf and Putnam (eds),
Philosophy of Mathematics. Selected Readings, Basil Blackwell, Oxford 1964.

Martin-Löf, P.: 1984, *Intuitionistic Type Theory*
Bibliopolis, Napoli

— 1987, 'Truth of a proposition, evidence of a judgement, validity of a proof'
Synthèse 73

Moore, A. W.: 1990, *The Infinite*, Routledge, London

Prawitz, D.: 1965, *Natural Deduction*, Almqvist & Wiksell International, Stockholm

— 1980, 'Intuitionistic logic: a philosophical challenge'
von Wright (ed): *Logic and Philosophy*, Martinus Nijhoff, The Hague

— 1987, 'Dummett on a theory of meaning'
Taylor (ed), *Michael Dummett: Contributions to Philosophy*, Martinus Nijhoff, Dordrecht

— 1987a, 'Some remarks on verificationistic theories of meaning'
Synthèse 73

Rabinowicz, W. and Segerberg, K.: 1994, 'Actual truth, possible knowledge', *Topoi*, this issue

Williamson, T.: 1988, 'Knowability and constructivism'
The philosophical Quarterly 38, 422-432

— 1992, 'On intuitionistic epistemic modal logic'
Journal of Philosophical Logic 21, 63-89.

— 1994, 'Never say never'
Topoi, this issue