

Re: A little knowledge is a dangerous thing – THE HALTING PROOF

Source: <http://sci.tech-archive.net/Archive/sci.logic/2005-05/msg00083.html>

- *From:* "george" <greeneg@xxxxxxxxxx>
 - *Date:* 6 May 2005 10:11:17 -0700
-

Bhupinder Singh Anand wrote:

- > In footnote 36 of 'Some consequences of
- > defining mathematical objects
- > constructively and mathematical truth
- > effectively', I clarify that:
- >
- > "In other words, we argue that not every effective
- > method is necessarily algorithmic,

No, you don't. I mean, it would be nice if you did; the community allows for the possibility that this might be the case by calling the allegation that it can't be "the Church-Turing THESIS" as OPPOSED to "the Church-Turing POSTULATE", but you personally have never gotten within SNIFFING distance of an actual argument that such a thing (an "effective method" that is not TM-emulatable) actually exists.

- > although every algorithm is an effective
- > method. The possibility that "truth" may be non-
- > algorithmic,

Good scare-quotes. What is being talked about here is NOT "Truth" in some huge mystic medieval sense, BUT RATHER, a very certain specific KIND of truth, namely, first-order arithmetical truths about the natural numbers. And WE KNOW FOR A FACT that THAT kind of truth IS NOT algorithmically confirmable in the universal case.

- > and yet constructive,

Oh, bullshit.

- > is implicit in Gödel's famous 1951 Gibbs lecture [Go51]

No, it isn't. If this is what you took from that then

Re: A little knowledge is a dangerous thing – THE HALTING PROOF

you just plain didn't know what you were listening to.

- > where he remarks:
- >> 'I wish to point out that one may conjecture the truth
- > of a universal proposition (for example, that I shall be
- > able to verify a certain property for any integer given to
- > me) and at the same time conjecture that no general proof
- > for this fact exists.

OF COURSE.

THAT THERE MUST exist P for which $A_n[P_n]$ IS TRUE IN THE NATURAL NUMBERS but IS NOT PROVABLE FROM PA was THE WHOLE CONTENT of Godel's 1st incompleteness theorem! INDEED, the statement encoding "PA is consistent", where P_n means "n is not the Godel-number of a proof of a contradiction from axioms of PA", IS PRECISELY one such statement, with precisely one such property. Since PA is consistent, ONE CAN INDEED verify, after being given a natnum, that it is not the godel number of a proof of a contradiction from PA. But you cannot prove $A_n[P_n]$ in PA.

- > It is easy to imagine situations in which both these
- > conjectures would be very well founded.

Well, of course it is; he already gave the prime example 20 years earlier.

- > For the first half of it, this would, for example,
- > be the case if the proposition in question were some
- > equation $F(n) = G(n)$ of two number-theoretical functions
- > which could be verified up to very great
- > numbers n.' "

Well, that's one possible way of creating these dueling conjectures, but it does not have A DAMN THING to do with Bhup's allegation that anything "constructive" might be happening. Godel here is talking about the case where a proof of $A_n[f(n)=g(n)]$ is IMPOSSIBLE, NOT where it is constructive! A constructive proof of this would be even HARDER than a classical one!

- > In footnote 98 I observe, further,
- > that such a possibility is also
- > implicit in Turing's remarks ([Tu36], §9, para II):

No, it isn't.

- > "Let P be a sequence whose n-th figure
- > is 1 or 0 according as n is or
- > is not satisfactory. It is an immediate
- > consequence of the theorem of

Re: A little knowledge is a dangerous thing – THE HALTING PROOF

- > §8 that P is not computable.
- > It is (so far as we know at present)
- > possible that any assigned number of figures
- > of P can be calculated,
- > but not by a uniform process.
- > When sufficiently many figures of P have
- > been calculated, an essentially new method
- > is necessary in order to
- > obtain more figures".

This implies not only that every individual method is inadequate, but that if you go on, NO FINITE NUMBER of individual methods suffices: you will need INFINITELY many DIFFERENT methods to get to "the end". There is ABSOLUTELY NOTHING CONSTRUCTIVE implicit in ANY of this.

- >
- > Now, in his seminal 1931 paper, Goedel constructs
- > an arithmetical
- > relation $R(x)$, and gives a constructive,
- > and intuitionistically
- > unobjectionable, meta-proof that the
- > formula $[R(n)]$ is provable for any
- > given numeral $[n]$ in any formal Peano Arithmetic,

No, he doesn't. THAT would be a proof of the consistency of Peano Arithmetic. And there is ONLY ONE Peano Arithmetic in any case, and it is NOT intuitionistic, in that treatment.

- > and that the formula
- > $[(\forall x)(R(x))]$ is not provable in the Arithmetic.

It is not provable IF PEANO ARITHMETIC IS CONSISTENT.

- > Prima facie, using Occam's razor,
- > a straightforward interpretation of
- > this is that the arithmetical relation
- > $R(x)$ is effectively verifiable instantiationally,

EVERYthing is "effectively verifiable instantiationally"! EVERYthing!! If you ONLY HAVE ONE instance of something, and that instance is finite, then you can just say "this one instance is verified", AND THAT CONSTITUTES a verification! It might be wrong, but you could also have equally said "this one instance is refuted/rejected", and GUESS WHAT: ONE of the two MUST be right: it MUST be the case. It gets better: suppose you have A FINITE NUMBER of things that may or may not be acceptable. If that number is n then there are 2^n different possibilities as to which of the things are acceptable and which not. ONE OF THESE

Re: A little knowledge is a dangerous thing – THE HALTING PROOF

2^n POSSIBILITIES IS *RIGHT*/factual/correct/true.

JUST ASSERTING the truth of THAT possibility CONSTITUTES VERIFYING all n of these things!

You need to put "verifiable instantiationally" right out of your head. There is no such thing as an INSTANCE that is HARD to verify. As long as you are talking about a finite number of things, verification is trivial.

The problem

CAN ONLY ARISE FOR DENUMERABLE FAMILIES of things.

Axiom: IN THIS WORLD, DEFINITION: a PROBLEM is A DENUMERABLE FAMILY OF YES–NO QUESTIONS.

If you want your answers to be more complex than that, say you want them to be natnums, then you just migrate from "for input (Q), the answer is (n)", to "for input (Q,n), the answer is (yes)".

> but that it is not uniformly (i.e., algorithmically)

> verifiable – hence it is not Turing–computable.

The question becomes, HOW DID YOU LEARN that all the individual instances were, not merely verifiable, but TRUE? In the case of G1, this was NOT learned.

G1 DOES NOT contain a proof of the consistency of Peano Arithmetic.

> Such an interpretation

Oh, just STOP.

You DO NOT HAVE an "interpretation", suchlike or otherwise.

> would, of course, need to appeal to a

> provability thesis such as:

>

> Provability Thesis (PT): A true arithmetic relation

Again, stop. Terminology is incoherent already.

This is NOT about "true arithmetic relations".

In the first place, "relation" already has a definition and it is not even the KIND of thing that CAN be true or false. What you are ACTUALLY talking about is a true Universal Generalization in first–order arithmetic over the natural numbers.

> is Turing–computable, when treated as a Boolean function,

> if, and only if,

SHUT UP! "Turing–computable" ALREADY HAS a definition!

YOU do NOT get to say when something is TM–computable and when it isn't! TURING ALREADY SAID that!!

Re: A little knowledge is a dangerous thing – THE HALTING PROOF

> it is PA–provable.

Again, a relation, whether treated as a Boolean function OR NOT, IS NOT the kind of thing that can or cannot be PA–provable. THE ONLY things that can be PA–provable are sentences in the first–order language of PA.

I could go on but you are going to have try to reformulate this coherently in normal language. I would especially encourage you to re–check your

- > Goedel constructs an arithmetical
- > relation $R(x)$, and gives a constructive,
- > and intuitionistically
- > unobjectionable, meta–proof that the
- > formula $[R(n)]$ is provable for any
- > given numeral $[n]$ in any formal Peano Arithmetic,

In the first place, $R(x)$ IS NOT a relation. A relation is a set of ordered pairs. $R(x)$ is a unary predicate of natnums. In the second place, $R(n)$ basically says that n is not the Godel number of a proof of a contradiction from axioms of PA. Goedel does NOT give a proof, meta– or otherwise, that this is always true. Rather, he gives a proof that $R(n)$ really does encode provability (from PA, of the contradiction) properly, when n is a natural number. From THIS it follows that $R(n)$ must be true IF PA IS CONSISTENT. But he does NOT prove that PA is consistent. That is a harder problem that has to wait for heavier machinery. His whole point is that neither he nor anyone else CAN hope to prove that PA is consistent, using only PA.

.

• **References:**

- ◆ **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
 ◇ From: george
- ◆ **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
 ◇ From: Charlie–Boo
- ◆ **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
 ◇ From: Bhupinder Singh Anand

- Prev by Date: **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
- Next by Date: **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
- Previous by thread: **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
- Next by thread: **Re: A little knowledge is a dangerous thing – THE HALTING PROOF**
- Index(es):

Re: A little knowledge is a dangerous thing – THE HALTING PROOF

- ◆ Date
- ◆ Thread