Mathematical note: Logic, set theory, completeness, incompleteness, and the rot in the foundations of mathematics

Warren D. Smith
wds@research.NJ.NEC.COM

date = October 27, 1998

Abstract — **The discussion of Gödel's incompleteness theorem in my "introduction to computer science" had caused confusion in a number of people who knew something about mathematical logic. Trying to unconfuse them and me, I discovered to my astonishment how completely awful a state the Foundations of Mathematics are in. We'll discuss that and how it relates to incompleteness and completeness theorems from logic and computer science.**

This note lies outside of the main stream of ideas in this course.

Keywords — Zermelo-Fraenkel axioms of set theory, logic, incompleteness and completeness theorems, the Turing machine paradox, philosophies of mathematics.

To understand the foundations of mathematics, you need to know about logic (§1, §2), i.e. the language we are allowed to express logical statements in, and the axioms of set theory (§3), i.e. the "intuitively obvious" statements that all else is supposed to be deduced from.

But then, the completeness and incompleteness theorems soon make you realize that, in many ways, mathematics is resting on a very shaky or inadequate foundations! I claim nobody really knows either what the integers are, nor what it means for a Turing machine to "not halt." For me, this realization crystallized in the form of the "Turing machine paradox." I describe two forms of this paradox in §7. The three main philosophies of mathematics are sketched in §??. I think the main psychological problem most people have with my Turing machine paradox is that most people are "realists," i.e. subscribe to the "realist" philosophy of mathematics (whether they knew it or not). My Turing machine paradox starkly dramatizes the fact that the current notion of the foundations of mathematics is simply insufficient to satisfy the desires of realists.

1 First order logic

Andrews [1] defines the "well formed formulae" (WFFs) in "first order logic" in his section 20 on page 45.

These include

1. "improper symbols": $\forall$ (for all), $\exists$ (exists), AND, OR, NOT, parentheses
2. variables
3. functions of n variables (for any $n \geq 1$)
4. integer constants
5. propositions
6. predicates (boolean valued functions)

and rules for what you are allowed to do with them. *Only* variables may be quantified (i.e. occur in forall's and exists's).

A statement (WFF) is "valid" if always true for all possible values of the free variables. It is "satisfiable" if it is true for some values of the free variables (i.e., its negation is not valid).

A "model" of a logic is a set, called the "universe" and a function assigning to each variable, function symbol, and relation, actual objects (respectively elements, functions, and predicates) in the universe. The equality relation has to correspond to element equality. The functions have to obey the properties the logic says they do.

Theorem 1 (Gödel's famous "completeness theorem for first order logic") *True statements (i.e. those valid in every model obeying some axiom set*[1]*) always have proofs.*

A sample of completeness theorems (thms 2509-2514 Andrews) for first order logic:

1. If A is a finite set of axioms (WFFs) and if a statement S is valid in all "frugal models" of A, then there is a *proof* of S from A.
2. If A is consistent (cannot be used to prove false) than it has a model.

[1] The set of axioms may be either finite or infinite, but if the latter, it must be "recursively enumerable," that is, the full list could be printed out by a Turing machine. Also, all "statements" have to be WFFs in first order logic.

3. Every valid statement S is a theorem (i.e. has a proof from A).

4. (Löwenheim-Skolem theorem) If a countable set of formulas has a model, then it has a countable model.

5. If S is valid in every "countable interpretation" (seems more general than "frugal model") then S has a proof from A.

6. A set of sentences are valid iff it has a model, iff it has a frugal model, iff every finite subset of the set has a model.

Proof sketch: The key step is showing that any unprovable statement is true in some models but false in others, by showing existence of suitable models, where the "model" is defined largely by a function mapping logical statements to alleged truth values, with those values obeying the laws of logical inference. Such models may be constructed by considering going through all logical statements, choosing either truth value whenever we have a choice, i.e., whenever we reach a statement not implied by (or whose negation is implied by) the previous ones, i.e. whenever we reach an unprovable statement. (This procedure not be algorithmically implementable, i.e. may require a "higher-level" Turing machine, but that does not matter for us.) QED.

Application: by enumerating all proofs, a Turing machine could print out all valid statements (each of which would be theorems) of first order logic that follow from any finite axiom set A.

Application (of the final item, called "compactness"): If the 4-color theorem is true (it is) for finite planar graphs, then it is true for infinite planar graphs.

Application: Any statement unprovable from the Peano axioms of arithmetic (viewed as a set of first-order logic statements which a Turing machine could print out) is true in some, and false in other, models of the integers, where all of these models are at least as consistent as the Peano axioms themselves.

2 Second order logic

"Second order logic" is defined in Andrews [1] sec 50, and Enderton [4] chapter 4. (However, their two definitions of "model" differ... we will follow Enderton's in this section.) It is like first order logic but quantification on predicates, propositions, and function variables is now permitted in WFFs.

Some of the completeness theorems above for first order logic work and some fail for second order logic:

Theorems:

1. (non-compactness; Enderton thm 41A) There is an unsatisfiable set of second order statements, any finite subset of which is satisfiable.

2. (non-enumerability of validities, 41C) No Turing machine program can output all valid sentences in second order logic. In fact, the set of such sentences (the "second order validities") is not even definable by a finite set of WFFs in logic of any finite order, or even countably infinite order.

3. (compactness, Enderton p.286) If every finite subset of a set of second order WFFs has a "general model," then so does the whole set.

4. (enumerability, Enderton p.286) A Turing machine can output the set of second order sentences true in every "general structure."

Uses of second order logic: One can define the cardinality $2^{\aleph_0}$ of the reals in second order logic. One can define a predicate to test if a set S is infinite in second order logic, but not in first order logic[2].

Fagin's theorem ([5]; also theorem 8.3 page 173 of [9]): The class of graph theoretic properties expressible in existential second order logic is precisely the computational complexity class NP. For example, a particularly clean NP-complete problem is the question: given a graph, does there exist inside it a clique on half its nodes?

Enderton example 2 p.270: All models of Peano postulates are isomorphic in 2nd order logic. (See below discussion of Dedekind's theorem.) This contrasts with first order logic, where there are an infinite number of non-isomorphic models of the integers obeying the Peano postulates, and Gödel undecidable statements S in arithmetic (of which there are many) are those such that in some models of the integers S is false, and some models S is true.

3 The ZFC axioms of set theory – the foundation of mathematics

1. (Set equality.) $A = B$ if and only if A and B have the same elements. In symbols: $\forall u(u \in A \Leftrightarrow u \in B) \ \Leftrightarrow\ A = B$. Equivalent form: $A \subseteq B$ AND $B \subseteq A \ \Rightarrow\ A = B$.

2. (Pairing.) For any a and b, there exists a set $\{a, b\}$ containing exactly a and b. In symbols: $\forall a \forall b \exists C \forall x(x \in C \ \Leftrightarrow\ (x = a \text{ OR } x = b))$.

3. (Restriction.) If $P(x)$ is a boolean valued function and S is a set, then there exists a set $\{u \in S :\ P(u)\}$. (An immediate consequence: the empty set $\emptyset$ exists. Originally set theory had been formulated with the stronger axiom that $\{u :\ P(u)\}$ is a set, but this leads to contradictions – e.g. "Russell's paradox[3]" arises if one takes

[2] At first it seems that first order logic permits an infinity test. One attempt is that if S is a set of integers with $P(n)$ being the predicate $n \in S$, then "S is infinite$\Leftrightarrow$[P(n) $\Rightarrow \exists m, m > n, P(m)$]. That attempt fails because it is equivalent to "S is finite$\Leftrightarrow$[$\exists n[P(n) \Rightarrow \forall m, m > n, \text{NOT}\, P(m)]$" and the $\forall m, m > n$ part depends on what the notion your model of the integers has, of infinity! E.g. consider a nonstandard model of the integers with elements greater than all the normal integers. Another attempt is "S is infinite$\Leftrightarrow$there exists a 1-1 correspondence between S and a strict subset of S." However, this attempt seems to require set theory as a second order logic...

[3] A barber in a village shaves everybody who does not shave himself. So: who shaves the barber? As a set-theoretic paradox this is: a set has "property P" if it does not contain itself as an element. Now consider the set S of sets with property P. Does S have property P?

$P(x)$ to be $x \notin x$. So the present weaker form was proposed by Zermelo.)

4. (Union.) If S is a set, so is the union of all its elements; the elements of the union are the elements of the elements of S. In symbols: $\forall S \exists U \forall x (x \in U \Leftrightarrow \exists z (z \in S \text{ AND } x \in z))$. (Immediate consequence of this and the restriction axiom: If S is a set, so is the intersection of all its elements.)

5. (Powerset.) For any set S, its powerset (set of its subsets) exists: $\forall S \exists Y \forall x (x \in Y \Leftrightarrow x \subseteq S)$

6. (Infinity.) There exists an infinite set. One popular symbolic form: $\exists S (\emptyset \in S \text{ AND } \forall (x \in S)[x \cup \{x\} \in S])$. This axiom is rejected by "finitists."

7. (Inclusion-Minimal element.) Every nonempty set S contains an element disjoint from it: $\forall S (S = \emptyset \text{ OR } \exists x (x \in S \text{ AND } x \cap S = \emptyset))$. (Immediate consequence: it is impossible for a "set" to exist containing an infinite chain of inclusions $\cdots x_3 \in x_2 \in x_1$.)

8. (Function map.) If F is a function whose domain is a set S, then the range of F is also a set. I.e. $\{F(x) : x \in S\}$ is a set. (There have been several different looking, but actually equivalent, forms of this axiom proposed, involving, e.g. 2-variable boolean valued functions with certain properties. This axiom was added to the previous Zermelo axioms "Z" by Fraenkel in 1922. The resulting combined axiom set is called "ZF.")

9. (Axiom of choice.) For every set S such that $\emptyset \notin S$, there exists a function F such that $X \in S \Rightarrow F(X) \in X$. (Choice was shown by Gödel and Cohen to be logically independent of the ZF axioms. ZF with Choice added is called "ZFC." Although the Axiom of Choice seems obvious, constructivists reject it because it is a nonconstructive existence statement. Also, it leads to certain paradoxical-seeming consequences in measure theory such as the "Banach-Tarski paradox" that a ball may be partitioned into a finite number of disjoint subsets, which may then each be moved by rigid motions to assemble two balls, each congruent to the original ball. The only way this can happen is if the subsets are "nonmeasureable." Certain special cases of Choice are immediately provable constructively from the other axioms, for example if every $X \in S$ is a singleton $X = \{x\}$, if S is finite, or if every $X \in S$ is a well ordered set, e.g. of real numbers.) Here are 3 equivalent formulations.

   - (Zermelo's form, 1904) Given any set S of mutually disjoint nonempty sets, there is a set C containing a single representative from each element of S.
   - (Zermelo showed this was a consequence of his first form, and it obviously implies it by picking the least elements as the representatives) Every set can be well ordered.
   - (Russell's form 1908) The Cartesian product of nonempty sets is nonempty, even if the product is infinite.

The ZFC axioms are generally regarded as the foundation upon which the rest of mathemetics is built. (Indeed, the books by Bourbaki as essentially an effort to make that explicit.) It is quite amazing, actually, that essentially all of mathematics is based, at bottom, solely on these 9 axioms.

Quote by Saharon Shelah, which I agree with: "My feeling is that ZFC exhausts our intuition except for things like consistency statements, so a *proof* means a *proof in ZFC*."

Thanks to some effort to avoid paradoxes, it is now generally believed that ZFC are consistent. However, the second Gödel incompleteness theorem shows that there cannot be a *proof* of the consistency of ZFC (by using ZFC only in that proof).

However, as we've seen, the finitists, constructivists, and intuitionists[4] [2] [7] do not accept some of the ZFC axioms – so I guess they are not as "obvious" to some as to others!

The "continuum hypothesis" (CH) states that there does not exist an infinity larger than the integers but smaller than the reals. Both CH and the stronger "generalized continuum hypothesis" that $2^{\aleph_k} = \aleph_{k+1}$ for all $k \geq 0$, were shown by K.Gödel and P.Cohen to be logically independent of ZFC.

Quote by Paul Cohen: "The notion of a set is too vague for the continuum hypothesis to have a positive or negative answer."

3.1 On the character of ZFC axioms

First, many of them may be thought of as "definitions" (or "union," "set" etc.) rather than axioms. This view makes no real difference.

Second, there is an important difference of opinion between among many mathematicians and many logic books concerning whether the axioms of ZF are statements of first order or second order logic.

As we made clear by giving explicit symbolic expressions, the ZF axioms are all writeable in first order logic. *But*, the axiom of restriction and Fraenkel's function map axiom involve "for all predicates P..." and "for all functions F..." and hence are statements of second order logic. Furthermore, the axiom of choice involves a "there exists a (choice) function..." and hence also is second order. *But*, many authors view the axiom of restriction and Fraenkel's function map axiom instead as "axiom schemes," i.e. each are really an *infinite set* of axioms, one for each possible predicate P or function F respectively, and *if we demand that any predicate or function be expressible with first order logic formulas* then this is just a recursively enumerable set of *first order* logic axioms. In this view, one refuses to concede the existence of functions not definable with formulae, or, while perhaps conceding their existence, one still

[4]Intuitionists deny the "exclusion of the middle" i.e. believe that statements exist which are neither true, nor false. They therefore do not accept proofs by contradiction ("A leads to a contradiction, so NOT A"). They are a subset of constructivists.

demands that the ZF axioms only pertain to the formulae and not to non-formulae functions.

Furthermore, the axiom of choice is also interpretable as a first order statement in two different ways:

1. "there exists a formula (i.e. an integer, if it is encoded using "Gödel numbers")..." although in this interpretation, Choice would seem a lot less "intuitively obvious!" This interpretation is usually *not* adopted, although I suppose that the constructivists would want to do something like this, assuming there were any pro-choice constructivists.

2. You can write down the axiom as symbols as

$$\begin{aligned} \forall x \forall y (x \in A \,\mathrm{AND}\, y \in A \Rightarrow x \cap y = \emptyset) \,\mathrm{AND} \\ \forall x (x \in A \Rightarrow x \neq \emptyset) \\ \Rightarrow \exists C \forall x [x \in A \Rightarrow \exists u (C \cap x = \{u\})] \end{aligned} \tag{1}$$

   which means if both x and y are disjoint subsets of a set A of nonempty sets, then there exists a choice *set* C which has exactly one member in common with each member of A, i.e. is a set of *representatives.* Note, in this way the Axiom of Choice is merely asserting the existence of a set, not a function, just like the other ZF axioms. This is the way Choice is usually interpreted.

My personal view is that, if you want ZFC to serve as a "foundation for mathematics," then you have to allow functions and predicates not definable with formulae axioms. The reason I claim that is as follows. Obviously formulae are countable, in fact recursively enumerable. So order all predicates with one integer argument P_1, P_2, P_3, ... and[5] then define (I modestly name the following predicate with my own initials)

$$\mathrm{WDS}(n) \;=\; \mathrm{NOT}\, P_n(n). \tag{2}$$

This predicate is not a member of any countable set of "all" predicates! I think any reasonable notion of "mathematics" shouldn't refuse to allow such predicates!

So with this second-order interpretation of ZFC, statements provable from ZF or ZFC are not necessarily provable in the sense of first order logic, i.e. a finite proof starting from a recursively enumerable set of axioms with all steps in the proof being statements of first order logic. The completeness theorem then does not hold, and in fact, ZFC is *incomplete* – i.e. there exist true, but unprovable, statements in ZFC. (See below on Gödel incompleteness theorem.)

On the other hand in the first order interpretation (and the corresponding first order interpretation of the Peano axioms of the integers) Gödel's completeness theorem does hold, and every true statement is provable. Furthermore by the Löwenheim-Skolem theorem, there is a countable model of set theory! This seems rather amazing in view of Cantor's well known proof[6] that uncountable sets (i.e. the real numbers in $[0, 1)$) exist. But it is possible (the mapping to the model is not what you think it is) to resolve this apparent paradox.

4 Peano's axioms (G.Peano, 1889) for the natural numbers

1. $0 \neq n + 1$
2. $n + 1 = m + 1 \Rightarrow n = m$
3. $n + 0 = n$
4. $n + (m + 1) = (n + m) + 1$
5. $n \times 0 = 0$
6. $n \times (m + 1) = n \times m + n$
7. For all predicates $P(n)$, $P(n)$ AND $\forall n (P(n) \Rightarrow P(n + 1)) \Rightarrow \forall n\, P(n)$.

All of these are statements of first order logic except for the last, which again I would interpret as a statement of second order logic. But many people instead regard it as an axiom scheme, i.e. an infinite, recursively enumerable, set of first order logic axioms defined by *formulae.*

By setting up a correspondence

$$n \;\leftrightarrow\; \underbrace{\{\emptyset \cup \{\emptyset\} \cup \{\{\emptyset\}\} \cup \cdots\}}_{n \text{ terms}} \tag{3}$$

one may see that Peano's axioms are a consequence of ZFC.

The "Paris Harrington theorem" [10] is an arithmetical statement of first order logic, not provable from the Peano axioms alone, but nevertheless true (i.e. provable in ZFC).

5 Group axioms

These are a particularly simple set of axioms, which are a useful test case to think about when you think about axiom sets. We need a binary function "$\circ$" and a constant "1."

1. Associativity: $\forall a \forall b \forall c\, (a \circ b) \circ c = a \circ (b \circ c)$.
2. Identity: $\forall x (x \circ 1 = 1 \circ x = x)$.
3. Inverses: $\forall a \exists b\, (a \circ b = b \circ a = 1)$.

The additional axiom $\forall a \forall b (a \circ b = b \circ a)$ of commutativity would be logically independent of the other axioms since abelian and nonabelian groups both exist. The group axioms are not complete in the sense that there exist finite

[5] Or with one set-valued argument, and only depending on the set's cardinality, if you haven't figured out what the integers are yet.

[6] Suppose the real numbers in $[0, 1)$) were countable. List them in order x_1, x_2, x_3, etc. There is a slight difficulty because numbers ending "10000..." are also representable as ending "01111..." but this is only going to add a countable number of extra representations (indexed by the position of the first 1 or 0 in the infinite sequence) and so it will not affect the countability of the real numbers if we forbid the second kind of representation or of we count all numbers of this form twice. Now consider the real number C whose nth binary digit after the "decimal point" is the opposite of the nth binary digit of x_n. C cannot be in your alleged list of all real numbers. Contradiction.

sets of generators and relations for which it is *undecidable* if a corresponding group exists [12]. (This result was originally due to A.Turing.) This incompleteness is possible, despite Gödel's completeness theorem for first order logic, because of the implicit "there exists a function $\circ$," which is a statement of second order logic.

6 Gödel's incompleteness theorem and Turing and Gödel undecidability

Fix[7] some programming language. For simplicity, the language has no input; programs just run and produce some answer. In fact use LISP so that programs and answers are the same thing. We have a function Size which takes a program or answer and tells you how many characters are in it.

Definition. A program is "elegant" if it halts and it is the smallest program (according to the Size function) which produces whatever answer it produces. Break ties lexicographically.

Observation. For any answer, there exists a unique elegant program which produces that answer, and it must be no bigger than the answer plus a constant.

Observation. There are an infinite number of elegant programs.

Definition. By a "formal system" we will mean a finite proof checking algorithm `CHECKER`, which, given a purported proof, will return

```
proof ok
```

or

```
that was no proof.
```

Theorem 2 (Chaitin's elegance theorem.) *There is a constant K (not depending on our formal system) such that if FS is a formal system which is not inconsistent (i.e., we can't prove a false statement in FS) and if P is an elegant program, and you can prove (in FS) that P is an elegant program, then*

$$\mathrm{Size}(P) \le K + \mathrm{Size}(FS). \tag{4}$$

Remarks. This is truly amazingly bad. It means in *any* fixed formal system, there are an infinite number of true statements of the form "X is elegant" which we can't prove – in fact, there are only a finite number of statements of this form that have proofs. So we trivially get Gödel's incompleteness theorem (there exist true but unprovable statements) and Turing's theorem on the existence of uncomputable functions (the function mapping programs to 1 if elegant, 0 if not, is uncomputable).

Proof. Consider the following program CHAITIN.

```
Let pf loop through all purported proofs in order
   of increasing  Size  with ties broken lexically.
          Call CHECKER(FS, pf)
          If the result is "proof ok"
               and  what pf proved is that some
               specific program P halts and
               is elegant, and
                      Size(P) > Size(CHAITIN)
               then exit the loop.
   If we get here, P is a program which we've
   proven halts, we have proven is elegant, and
   is bigger than CHAITIN.  Since FS is consistent,
   P must really halt, so:
   Run P.
   Return the result of P and halt.
```

Now CHAITIN either halts or it doesn't.

Suppose it does halt. The result of CHAITIN is the result of running the P that it found. But CHAITIN is smaller than P, and we have proven (using FS) that P is elegant, so no program smaller than P produces this result. Contradiction.

So CHAITIN doesn't halt. So it never finds a proof that a program bigger than Size(CHAITIN) is elegant, but it goes through all possible proofs, from short to long. Thus, no such proof can exist, or it would have come to it eventually (along with all kinds of bogus proofs that the `CHECKER` program would have rejected, of course).

Hence: there is no program P which halts, is elegant, which you can prove is elegant (in FS) and which satisfies Size(P) >Size(CHAITIN). Since Size(CHAITIN)=Size(FS)+constant we are done. QED.

7 The uniqueness of the integers? The Turing machine paradox

Here is an apparent paradox, which I call the "Turing machine paradox," and its attempted resolution.

Paradox:

1. The finite description (transition function and nonblank initial portion of its tape) of a Turing machine, and the claim that "it halts" (or "it does not halt"), and the Peano axioms of the integers, may all be written[8] as statements of first order logic.

2. Turing's proof (or Chaitin's proof in §6) shows that there exist Turing machines T for which no proof exists that T does not (or does) halt.

3. Gödel's completeness theorem shows that for any statement of first order logic which has no proof, the statement is true in some models, and false in other models, of the integers (all of these models being equally consistent).

4. Horrors!! It seems our Turing machine must say to itself: "I wonder which model of the integers I feel like

[7] This is a nice proof of Gödel's incompleteness theorem, due to G.Chaitin, but rewritten by Henry Cejtin and then rewritten again by me.

[8] For simplicity use a counter machine rather than a Turing machine. The two counters are definable via Peano's axioms. The statement "T is halted at time n" is a property $P(n)$ of integers n and "T never halts" is $P(n) \Rightarrow P(n+1)$.

supporting today? Ah – that one! OK, *now* I'll decide whether I'll halt." But that is ridiculous. Put another way – how does the Turing machine know the model in Alice's mind? Or in Bob's mind? All it can know is its transition function, defined by a *finite* table!

An even worse-appearing version of this paradox[9] is: there exist programs which are, or are not, "elegant" (defined in the previous section) depending on which model of the integers we are in. But this is truly insane. Surely a program for a Turing machine either is the shortest program outputting whatever it outputs, or it isn't! How can it be both/neither!??

Well, there are two possible explanations of these paradoxes, depending on which camp you are in – i.e. on whether you believe that Peano's axioms and ZF are second order or first order logic statements.

If you are in the first-order camp, then you really do believe that some Turing machines cannot be said to halt or not halt until you know which model of the integers is your favorite! The crux of the difficulty is the nature of time. Time is an integer parameter (if we are dealing in discrete Turing machine steps). Well, suppose in our universe, time is governed by a nonstandard model of the integers containing "extra infinities" beyond the standard infinity. Since in first order logic there is no way to test finiteness, there is no clear (i.e. model independent) meaning of the notion that a Turing machine halts in "finite" time. Maybe my "infinite" is your "finite." Of course, those machines which obviously go into an infinite loop (provably do not halt) do not halt in all models of the integers, and those which obviously provably always halt do so in all models of the integers. Just the ones with undecidable halting problem are nasty and do different things in different models of the integers. Similarly, a program P may be the shortest program outputting its answer – but in a nonstandard model of the integers in which a shorter Turing machine program, rather than doing nothing "forever," instead at some higher, nonstandard infinity of time will output something... P is not the champion!

Of course, a lot of people (at least, those who believe in excluding the "middle") find it intuitively obvious that a Turing machine (which is, more or less, a clearly defined object within the physical universe) either definitely halts or definitely does not halt! And a computer program is either shortest possible, or not!

If you are one of these poeple, maybe you'd better join the second-order logic camp. But even then, as we'll see, the Turing machine paradox can still sting you badly.

If you are in the second-order camp, then for a while, everything looks OK. ZFC, which most people agree is the foundation of mathematics, is *not* complete. Within ZFC, *all models of the integers are isomorphic* and *any arithmetical statement of first order logic has a truth value independent of the model.* This important theorem of the uniqueness of the "standard integers" is due to Richard Dedekind in 1888 and is proven in [3] to follow from the second order logic interpretation of ZFC. The key fact that allows it to work is that the notion of "all models" or the notion of "all subsets of the natural numbers" is a notion of second order logic, expressible in ZFC, but *not* expressible in first order logic.

Dedekind's proof [3] involves a double induction to construct the isomorphism to the "natural" version of the integers we'd explained previously in showing how to get the Peano postulates from ZF. One must induct both on n and on possible functions performing the isomorphism on integers below n.

Hence, it would seem: there are no nonstandard integers, integer time is a unique notion, Turing machines either halt or do not, and we are OK.

As another example: due to the incompleteness of ZFC, it remains entirely possible at this point that (for example) the statement "there are an infinite number of primes of the form n^2+1" is both true, and no proof of it exists (starting from the Peano axioms and/or ZFC). This statement may be entirely phrased[10] as a statement of first order logic.

On the other hand, if you are in the first-order camp, then "there are an infinite number of primes of the form n^2+1," if undecidable, must be true in some models and false in other models of the integers, and thus cannot really be said to have a truth value at all.

So now... if you think that the second-order interpretation of ZFC has saved us from the Turing machine paradox... and have breathed a sigh of relief... you lose! The reason is, there are nonstandard models of set theory (i.e. of ZFC) itself! All of these models are equally consistent. (For example, we've already mentioned that there are two equally consistent models of set theory, in one of which – constructed by Gödel – the continuum hypothesis is true, while in the other – by Cohen – it is false.) Within these models, all the nonstandard models of the integers arise, as the unique integers within each such nonstandard set theory, via Peano's axioms and Dedekind's theorem.

Hence, it would seem that Turing machines first ask themselves "hmmm. What model of *set theory* do I or my master prefer today? *Now* I'll decide whether to halt." The whole second order view has only "upped the ante" and has not resolved the paradox.

Can we make a higher set of axioms, enclosing set theory (analogously to the way set theory encloses the integers) in which there is only one, "standard" model of ZFC? Yes; it is called the "cumulative type structure." But... before you breathe a sigh of relief... there are at least three different well accepted models of the cumulative type structure, leading to different set theories. This just ups the ante once again, without exploding the Turing machine paradox, and at the cost of making the foundations of mathematics vaguer!

My personal conclusion is that the foundations of math-

[9] "Worse," because this restatement appears to avoid any reference to anything infinite.

[10] E.g. the notion "a divides b" is $\exists c(c \in \mathbf{Z}\,\mathrm{AND}\, a \times c = b)$. The notion "$p$ is prime" is $\mathrm{NOT}\,\exists c(1 < c < p\,\mathrm{AND}\, c \in \mathbf{Z}\,\mathrm{AND}\, c\,\mathrm{divides}\, p)$. The notion "$x$ is of the form n^2+1" is $\exists n(n \in \mathbf{Z}\,\mathrm{AND}\, x = n \times n + 1$. With $P(x)$ denoting the property "x is a prime of form n^2+1", the notion "there are an infinite number of primes of the form n^2+1" is $P(n) \Rightarrow \exists m(m > n\,\mathrm{AND}\, m \in \mathbf{Z}\,\mathrm{AND}\, P(m))$.

ematics are in big trouble if we cannot even figure out how to define a unique notion of the *integers*. And, as far as I can tell, nobody can. However, you may console yourself with the following thought:

Anything that seems "observable" in the universe really does seem to be uniquely specified by mathematics, despite any ambiguities in the definition of "mathematics." For example, nobody has ever observed a Turing machine not halting forever! The difficulties only arise when we mess with infinity, and we presumably are only ever going to observe concrete, finite things.

Quote by K.Gödel [6]: "...the objects of transinfinite set theory... clearly do not belong to the physical world."

8 Andrews's Q_0 (type theory) and higher order logic

To do mathematics we need both some foundational axioms (ZFC generally play that role) and laws of allowed logical inferences, and a language to express statements in. First order and second order logic are not the most comprehensive possible languages.

In his section 50, Andrews [1] defines something called Q_0, which is a very large set of allowed kinds of statements, apparently subsuming logics of all finite and countably infinite orders. Q_0 is an attempt to be the most comprehensive possible language.

Within Q_0, Andrews has a notion he calls "standard." See his page 186 where this notion is defined in terms of "frames," "interpretations," "models," and sets of boolean-valued functions. "Standard models" are a subset of "general models." I think that "standard models" are the ones compatible with ZFC, but am not sure.

Andrews's Theorem 5404. Every finite model of Q_0 is standard.

Nonstandard models (which we now see are necessarily infinite) can exhibit some very nasty pathologies, many of which are exhibited by Andrews. If you have very little clue about what this all means – neither do I.

Later Andrews defines Q_0^∞... (quote: "We may regard the actual universe as a model for Q_0^∞"). He proves it is consistent (Andrews's 7204).

Theorems:

1. (Andrews's 5403) Q_0 is consistent (cannot prove false).
2. (5501) Every consistent set of sentences in Q_0 has a "frugal general model."
3. (5503; compactness) If every finite subset of a set of sentences in Q_0 has a general model, so does the whole set.
4. (incompleteness 5506) There are sentences of Q_0 true in all standard models of some axiom set, which are not provable from those axioms.
5. There are valid sentences of Q_0^∞ which are unprovable.
6. (7302) The validity of sentences of Q_0 is Turing undecidable.
7. A Turing machine cannot output the valid sentences in Q_0.
8. Any consistent set of Axioms A in Q_0^∞, where there exists an algorithm to decide membership in A, is not complete, i.e. will not suffice to produce proofs of every valid sentence.

9 Truth

Andrews defines the set "truth" to consist of all the valid sentences in Q_0. It is closed under the rules of logical inference.

The meta-conclusion is that "truth is elusive!" Specifically:

1. (7300) Truth is not Turing-decidable (even at any level of the undecidability heirarchy - shown in [11])
2. (7201a) Truth is not even "axiomatizable" by a Turing machine. That is, no algorithm (even running on higher level Turing machines) can output a list of "axioms," i.e. a subset of truth from which the rest of Truth follows by the laws of inference. (Actually, a better word here than "axioms" would be "reachability set" to avoid confusion with *the* axioms of mathematics, i.e. ZFC and the laws of inference.)
3. (7305) Truth is not even definable by logical formulas written in the language in which the truths are expressed.

All of these are also true if instead of Q_0 you use first order or second order logic – in the second-order logic interpretation of ZFC.

All of these are easy consequences of Gödel's incompleteness theorems[11].

10 Find out what kind of fool you are

According to [3] there are three main "philosophies of mathematics," namely the "Platonists" (also called the "realists"), the "Constructivists," and the "Formalists." During the preparation of these notes, I found myself (and others) embroiled in a large number of loud arguments. It was amazing how the arguers seemed automatically to divide themselves into one of these three camps. Which one are you?

10.1 Summary of the Platonist or realist religion

There is a unique structure, the cumulative type structure of sets. This contains the unique standard set theory, the standard integers, and the standard real numbers. There is thus a unique notion of "truth." Mathematics is the study of these standard structures. ZFC is true in the standard

[11]The first Gödel incompleteness theorem is that any logical system big enough to include arithmetic contains statements unprovable from its axioms. The second Gödel incompleteness theorem, which we have not proven here, says that the statement expressing the consistency of the system, is one of them.

structures and describes most of their interesting properties despite the fact that it does not provide a complete description of them, due to Gödel's incompleteness theorems. The incompleteness theorems thus impose severe limitations on our ability to do this study.

Quote by K.Gödel [6]: "...the undecidability of Cantor's conjecture[12] from the accepted axioms of set theory[13]... would by no means solve the problem. For if the meanings of the primitive terms of set theory are accepted... the set-theoretical concepts and theorems describe some well-determined reality, in which Cantor's conjecture must be either true or false. Hence its undecidability from the axioms being assumed today can only mean that those axioms are an incomplete description of reality.

[This belief] is by no means chimerical, since it is possible to point out ways in which the decision of a question, which is undecidable from the usual axioms, might nevertheless be obtained."

Discussion. I think the big mental hurdle everybody seems to experience when they see the Turing machine paradox is due to the fact that everybody, in their heart, is a realist. The Turing machine paradox represents the frustration of realist desires. The realist interpretation of this paradox would probably be as follows: "The Turing machine really does halt or not, in the correct one true model of set theory (i.e. 'reality'). Unfortunately, we currently do not know what that model is." The realist interpretation of the continuum hypothesis is similarly that CH is actually true, or actually false, in the one true model of set theory – we just do not know what that model is, because ZFC does not completely specify it. (I think most mathematicians would vote that CH ought to be true, in which case perhaps it should be added to ZFC as an additional axiom.) In view of the fact that reality is so incompletely specified by ZFC, it is amazing how successful ZFC, and mathematics, has been so far.

10.2 Summary of the Constructivist views

Mathematics is the study of constructions. Nonconstructive existence proofs are rejected. The constructive systems are generally much weaker than ZFC. The "Intuitionists" reject the excluded middle: i.e. they reject the notion that statements are either true or false – they could be in the "middle" instead. The "finitists" reject infinity.

Quote by L.Kronecker: "God made the integers, all else [which Kronecker preferred to dispense with] is the work of Man."

Discussion. Now at first, it may seem ridiculous to assert the nonexistence of (and refusal to consider) infinity. Or to reject the notion of proof by contradiction. These moves instantly destroy a great deal of mathematics! But, then consider the view that infinities are never "observable" and so, as far as mathematics describing the observable world is concerned, the finitists in some sense have lost nothing. The intuitionists actually do accept proof by contradiction in all finite situations – it is just that when infinities (which they accept) enter the picture, they lose confidence in the excluded middle.

For example, consider the famous statement "this statement is a lie." Well, it cannot be true, and it cannot be false. Must be in the middle. Now this may be valid as English, but it is actually not a permitted logical sentence according to, e.g., the rules of first order logic. But still, the existence of such beasts is enough to shake your confidence in the excluded middle. And the Turing machine paradox would presumably no longer qualify as a paradox if we rejected the excluded middle. For example, Turing's proof that algorithmically undecidable halting problems exist, is a proof by contradiction, and since undecidability is always a non-existence argument, presumably it will always be one.

I think the intuitionists in many ways are realists; they do have the notion of one true reality, but the only part of that reality which they claim we can ever be totally sure of, are the parts of it we construct.

10.3 Summary of the formalist view

Mathematics is just playing games – studying systems of axioms and their consequences, with no claim of any external meaning. Who cares. There is no particular point to trying to define a "unique standard structure" to study – that would just restrict the games we can play.

Discussion. An argument which makes formalism sound better and realism sound worse, is as follows. Consider the axioms of groups in §5. It is ridiculous to say that there must be a single "reality" in which, say, the commutativity law is really true, or really false, we just can't tell which from the group axioms. Obviously, there is no "one true group" – there are many groups, some commutative, some not, and it is worthwile to study them all. Good. Now, consider the ZFC axioms of set theory. Why is there any reason to believe (as the realists do) that set theory is specially different from group theory, and hence there should be this notion of the "one true model" of set theory?

11 Acknowledgements

Thanks to: Henry Cejtin, Stephen Omohundro, Slava Rytchkov, Stephen Weeks, Peter Winkler.

References

[1] Peter B. Andrews: An introduction to mathematical logic and type theory; to truth through proof, Academic Press 1986. [Very good book. Absolutely brutal to read, but if you dig hard enough, you can learn a lot. Covers Gödel's and others's completeness and incompleteness theorems. Does not discuss set theory at all, instead prosyletizes "type theory."]

[2] L.E.J.Brouwer, collected works. North-Holland 1975-1976.

[12] That is, the continuum hypothesis.
[13] That is, ZFC.

[3] F.R.Drake & D.Singh: Intermediate set theory, Wiley 1996.

[4] H.B.Enderton: A mathematical introduction to logic, Academic Press 1972 [Not so great, but has a whole chapter on 2nd order logic, which the other books mostly do not discuss.]

[5] R.Fagin: Generalized first order spectra and polynomial time recognizable sets, pp. 43-73 in "complexity of computation," (ed. R.M.Karp) SIAM-AMS proceedings 7 (1974).

[6] K.Gödel: What is Cantor's continuum problem?, (1964) reprinted 254-270 in *Collected Works II*, Oxford U.Press 1990. Quotes I've extracted from this paper were pointed out by Penelope Maddy.

[7] A.Heyting: Intuitionism; an introduction, North-Holland 1971 (3rd revised ed.)

[8] Thomas Jech: Set theory, Springer (2nd corrected edition) 1997.

[9] C.H.Papadimitriou: Computational complexity, Addison-Wesley 1994.

[10] J.B.Paris & L.Harrington: A mathematical incompleteness in Peano Arithmetic, appendix pp. 1133-1142 in J.Barwise (ed.) Handbook of Mathematical Logic, North-Holland. See also [Laury Kirby and Jeff Paris: Accessible independence results for Peano arithmetic, Bull. London Math. Soc. 14 (1982) 285-293].

[11] Raymond M. Smullyan: Gödel's incompleteness theorems, Oxford University Press, 1992.

[12] A.Tarski, A.Mostowski, R.M.Robinson: Undecidable theories, North-Holland 1971 (3rd printing).

[13] Alfred Tarski: A decision method for elementary algebra and geometry, prepared for publication with the assistance of J.C.C. McKinsey (2nd ed.) Berkeley, University of California Press, 1951; also this may be the same as The completeness of elementary algebra and geometry. Paris, Centre national de la recherche scientifique, Institut Blaise Pascal, 1967.

[14] S.Wagon: The Banach-Tarski paradox, Cambridge University Press, 1985.