ADVENTURES IN INCOMPLETENESS

by
Harvey M. Friedman
Distinguished University Professor
Mathematics, Philosophy, Computer Science Emeritus
The Ohio State University
University of Texas
Austin, Texas
March 1, 2017

Nautilus Magazine is an ambitious science magazine only a few years old. They won't let you see the article before it appears. They really have a skilled fact checker who queries you over the phone. We pretty much caught all of the seriously inaccurate statements.

However, one thing they really keep secret until the article appears is the TITLE.

When I read that it was "THIS MAN IS ABOUT TO BLOW UP MATHEMATICS", I got really scared. I was surely going to get paid a visit from the FBI or worse. And then I worried that my Texas visit would have to be cancelled for safety reasons.

So let me try to reassure you: if we all stay cool, we shouldn't have any violence at this talk! Let's see how it goes.

Actually, there are three titles floating around:

THIS MAN IS ABOUT TO BLOW UP MATHEMATICS (actual title)

HARVEY FRIEDMAN IS ABOUT TO BRING INCOMPLETENESS AND INFINITY OUT OF QUARANTINE (subtitle)

THE MAN WHO WANTS TO RESCUE INFINITY (this title was apparently discarded but still lives in cyberspace)

I don't know about you, but I like the second of these the best, especially with "big" inserted.

BRING INCOMPLETENESS AND BIG INFINITY OUT OF QUARANTINE

Well, enough weird fun. Let's do some math.

Incompleteness, in a general sense, started long before the late great Kurt Gödel.

OFA = ORDERED FIELD AXIOMS, based on 0,1,+,-,x,1/,<. What about this famous statement in OFA,

There exists b such that b x b = 1+1

better known as "a square root of 2 exists"?

From about 2400 years ago: there is no rational square root of 2. We conclude, in modern terms, that the above statement is neither provable nor refutable in OFA. I.e., independent of OFA. For we have a model of OFA in which the statement is true - the usual ordered field of real numbers or much smaller ordered fields. And a model of OFA in which this is false - the usual ordered field of rationals.

Fast forward to modern times, and we know how to fix this Incompleteness. There are two well known ways.

1. Algebraically: $(\forall b > 0)(\exists c)(b = c \times c)$. Also: Every polynomial of odd degree in one variable has a root.
2. Logically: The least upper bound principle for all first order formulas.

• Both 1,2 use infinitely many axioms - unavoidable.
• They are logically equivalent - not at all obvious.
• They entirely stamp out the incomplete-ness: the resulting systems prove or refute all statements in its LANGUAGE.
• Axiom instances are easily algorithmically recognized.

There are similar developments in elementary geometry rather than elementary algebra, with a particularly famous example of the parallel postulate in Euclidean geometry. These are also fixable. In many cases geometry has the much stronger kind of fixable Incompleteness - second order Incompleteness. Relationships between 1st/2nd order Incompleteness is worthy of several talks, mathematical and philosophical. We focus on 1st order incompleteness here.

Now let us turn to the discrete ordered ring axioms, DORA. This is very much like OFA except that we only think of integers - no reciprocal or division. This is also an elementary school system, with 0,1,+,-,x,<.

But instead of anything about reciprocal/division, we add

Nothing is strictly between 0 and 1.

Now consider this very basic statement

For all b there exists c such that c+c = b or c+c = b+1.

This is better known as "every number is even or odd". This statement is independent of DORA.

It's true in the ordered ring of integers, and false in the ordered polynomial ring in one variable over the integers.

Let's use the "logical" approach #2 for trying to fix this Incompleteness:

2*. Add to DORA: The least upper bound principle for all first order formulas.

GÖDEL. DORA + 2* still has Incompleteness.

In fact, there is no way to add further axioms to appropriately fix this Incompleteness.

DORA + 2* is essentially a rewrite of what is normally called PA = Peano Arithmetic. It is well known that PA is essentially equivalent to finite set theory = FST.

FST may be enough to prove or refute all finitary mathematical statements that have, as of 3/1/17, been published in accepted mathematical venues by mathematicians operating as mathematicians, as opposed to acting as f.o.m. provocateurs (like me).

E.g., it is widely believed that FLT = Fermat's Last Theorem is provable in FST, although this has not yet been firmly established.

This leaves open the possibility that f.o.m. investigators may be able to discover a finitary statement that is independent of FST, fully compatible with normal mathematical culture, and argue that the statement, although introduced by an f.o.m. provocateur, is *inevitable* over the realistically far out future of math. Note how such inevitably would answer objections that a provocateur was involved.

In fact, this is what has been happening. We now have a growing body of steadily more convincing examples of what I call CONCRETE MATHEMATICAL INCOMPLETENESS.

The early examples of such Concrete Mathematical Incompleteness at the FST level are Goodstein's Theorem (1944, 1982), Paris/Harrington Theorem (1977), Hydra Game (1982). There are some later examples at the FST level that are arguably more aligned with ordinary mathematical culture.

My current favorites at the FST or PA level are at 747: Incompleteness/2, 2/3/17, on the FOM Archives:

For x,y ∈ N^k, x <adj y if and only if x,y are each strictly increasing and (x_2,...,x_k) = (y_1,...,y_{k-1}).

x ≤c y if and only if each x_i ≤ y_i.

Ex: (3,5,8) <adj (5,8,9). (2,4,7) ≤c (2,5,8).

Obviously, x <adj y implies x ≤c y.

The interaction between these two binary relations on N^k, <adj and ≤c, is particularly interesting.

ADJACENT LIFTING. Every f:N^k → N^k has some x <adj y with f(x) ≤c f(y).

RECURSIVE ADJACENT LIFTING. Every recursive f:N^k → N^k has some x <adj y with f(x) ≤c f(y).

ELEMENTARY RECURSIVE ADJACENT LIFTING. Every elementary recursive f:N^k → N^k has some x <adj y with f(x) ≤c f(y).

POLYNOMIAL ADJACENT LIFTING. Every surjective polynomial P:N^k → N^k has some x ≤c y with P(x) <adj P(y).

- All four of these statements can only be proved by going slightly beyond FST (or PA or ACA_0).
- They can only be proved by using some seriously noticeable use of infinitistic methods that clearly go beyond the statements themselves.
- This represents Demonstrably Necessary Use of Machinery.

• However, to prove these statements, it is sufficient to use only a tiny tiny tiny tiny tiny tiny tiny fragment of the usual ZFC axioms for mathematics.

250 page Introduction to a book draft at https://u.osu.edu/friedman.8/foundational-adventures/boolean-relation-theory-book/

covering the state of Concrete Mathematical Incompleteness through BRT = Boolean Relation Theory.

• From below FST to around "uncountably many uncountable cardinalities", a very substantial fragment of ZFC.
• Variety of Concrete Mathematical Incompleteness at various levels.
• Also BRT, the predecessor of Emulation Theory, the latest rage. Both transcend ZFC.
In existing cases of Concrete Mathematical Incompleteness, P, we have the following:

P is shown, over an appropriately weak system, to be *provably equivalent* to the consistency (or consistency variant) of an unexpectedly strong system T.

Assuming T is "OK", this establishes the independence of P from T.

• If P is refutable from T then T proves its own inconsistency (or variant), so T not OK.
• If P is provable from T then T proves its own consistency. By Gödel, T is inconsistent, and so T is definitely not OK.

Before diving in to Emulation Theory, I want to mention a few more results in Concrete Mathematical Incompleteness - ones that don't really challenge ZFC, but nonetheless represent a wide range of important levels of Incompleteness. And it may even threaten to touch your own mathematical interests. I would certainly like to hear about that!

IN ANY LONG ENOUGH SEQUENCE $x_1,\ldots,x_n$ FROM {1,2,3}, SOME $(x_i,\ldots,x_{2i})$ IS A SUBSEQUENCE OF SOME LONGER $(x_j,\ldots,x_{2j})$.
IN ANY LONG ENOUGH SEQUENCE $x_1,\ldots,x_n$ FROM {1,...,k}, some $(x_i,\ldots,x_{2i})$ IS A SUBSEQUENCE OF SOME LONGER $(x_j,\ldots,x_{2j})$.

• Second is provable in 3-quantifier induct-ion, but not in 2-quantifier induction.
• Size for the first is > 7198th Ackermann function at 158,386 = $A_{7198}(158,386)$.
• Any proof of the first in EFA = exp function arithmetic, needs > $A_{7198}(158,385)$ symbols, a bit much. Same for SEFA.
• This is an ULTRA FINITE INCOMPLETENESS.

IN EVERY INFINITE SEQUENCE OF FINITE TREES, SOME TREE IS HOMEOMORPHICALLY EMBEDDABLE INTO A LATER TREE.
IN EVERY INFINITE SEQUENCE OF FINITE GRAPHS, SOME GRAPH IS MINOR INCLUDED IN A LATER GRAPH.

• First requires construction of a sequence of integers using all sequences of integers.
• Second requires infinite iteration of the above.
• Such constructions were rejected by Poincare and Weyl as circular and useless.
• Today they are widely accepted, as they lie well within ZFC.
• Same even for very computable sequences.

FOR ANY TWO COUNTABLE SETS OF REAL NUMBERS, THERE IS A ONE-ONE POINTWISE CONTINUOUS FUNCTION FROM ONE INTO THE OTHER.

• Proof requires a transfinite induction of length ω_1, similar to Cantor's Transfinite Decomposition of closed sets of reals.
• Statement not "Borel true". I.e., no Borel function taking two countable sets of reals (as infinite sequences) and returning such a function (again as an infinite sequence).
• No Borel function taking two countable sets of reals and returning an indication of a direction (forward or backward) for the pointwise continuous function.

EVERY BOREL $F:I^\infty \to I^\infty$, INVARIANT UNDER PERMUTATIONS (IN SEVERAL SENSES), MAPS SOME SEQUENCE TO A SUBSEQUENCE.

EVERY SHIFT INVARIANT BOREL $F:K \to K$ (IN VARIOUS SENSES) MAPS SOME x TO $(x_1,x_4,x_9,x_{16},...)$.

- Not provable in countable set theory, but just beyond. First proofs: Cohen's forcing.
- Proof of first conveniently converts to a Baire category argument, applied to a necessary nonseparable(!) topology.
- Specifically to I^∞, where the interval I is given the DISCRETE(!) topology.
- Not provable in SEPARABLE MATHEMATICS.

EVERY BOREL SUBSET OF $\Re^2$, SYMMETRIC ABOUT $y = x$, CONTAINS OR IS DISJOINT FROM THE GRAPH OF A BOREL FUNCTION FROM $\Re$ INTO $\Re$.

- Requires uncountably many uncountable cardinalities, quite a strong fragment of ZFC.
- Essentially equivalent formulation: Proof requires uncountably many transfinite iterations of the power set operation.

We now jump to EMULATION THEORY.

According to Nautilus Magazine, this is going to be used to blow up mathematics! Whoops, I shouldn't have said that.

EMULATION THEME. FOR ANY OBJECT OF A CERTAIN KIND, SOME MAXIMAL EMULATION (OF THE SAME KIND) EXHIBITS SPECIFIED SYMMETRY.

- S is an emulation of E if it resembles it in a specified way.
- Maximal emulation is an emulation which if enlarged, stops being an emulation.
- Symmetry typically requires invariance under transformations.

Of course, we want a context where everything has some maximal emulation. It suffices to have union of emulations be emulations. This will happen if emulation is finitely based.

Looking a bit out in the future, there is a more general formulation:

EMULATION THEME*. FOR CERTAIN NATURAL PARTIAL ORDERINGS, EVERY POINT HAS A MAXIMAL SUCCESSOR EXHIBITING SPECIFIED SYMMETRY.

For this, we generally want the partial orderings to be closed under sups.
A lesson to be learned from Emulation Theory of the future? - maybe everybody, no matter how ugly, can make maximal general improvement of themselves, while also being beautiful in specific ways.

Emulation Theory provides a particular context for this Emulation Theme, which is now a growing rich theory with plenty of open questions and thematic projects. Some of these results demonstrably require using far more than the usual ZFC axioms for mathematics.

- Emulation Theory (here) lives in $Q[0,1]^k$.
- Q[0,1] is the closed unit interval in the rationals Q.
- Objects of Emulation Theory are the subsets of $Q[0,1]^k$.

We need to explain emulations and the symmetry. We start with the symmetry, as it has very deep roots in abstract set theory.

DEFINITION 1. We say that $S \subseteq Q[0,1]^2$ is drop equivalent at (x,y),(x',y) if and only if for all z < y, (x,z) in S iff (x',z) in S.

Let's draw a picture for drop equivalence.

```
 _______________
|               |
|    A   B      |
|    |   |      | S ⊆ Q[0,1]^2 is drop
|    |   |      | equivalent at A,B defined
|____|___|______| below:
```

This rectangle is $Q[0,1]^2$ with points A = (x,y), B = (x',y). We have set $S \subseteq Q[0,1]^2$ in the background. As we drop from A and B, we want each point below A to lie in S iff the corresponding point below B lies in S.

Does every $S \subseteq Q[0,1]^2$ exhibit such symmetry?

THEOREM 1. There exists $S \subseteq Q[0,1]^2$ where drop equivalence holds only trivially. I.e., S is drop equivalent at (x,y),(x',y) if and only if $x = x' \vee y = 0$.

We can repair Theorem 1 at some cost.

THEOREM 2. Every $S \subseteq Q[0,1]^2$ is drop equivalent at some (x,y),(x',y), $x \neq x' \wedge y > 0$, if we replace Q[0,1] by some other dense linear ordering with endpoints 0,1. These replacements can be of any uncountable cardinality but not countable.

So far we are not threatening ZFC. However!

THEOREM 3. Every $S \subseteq Q[0,1]^2$ is drop equivalent at some (x,x),(x',x), $0 < x < x'$, provided we replace Q[0,1] by some gigantic dense linear ordering with endpoints 0,1. The size required here is far beyond anything that can be proved to exist in ZFC.

```
 _______________
|               |
|          A  B |
|          |  | |
|          |  | |
|__________|__|_|
```

Here A is on the diagonal.

Don't get excited yet! This is an example of Mathematical Incompleteness that is closely related to well known developments in large cardinal theory. The statement is intensely set theoretic, and the literature already has plenty of Mathematical Incompleteness in the highly set theoretic realm.

Yes, this is much simpler than the typical set theoretic independence result that you find. But I needed to make such simplifications in the set theory realm as a preliminary step toward the main events.

DIGRESSION - THE SMALLEST LARGE CARDINAL

We state this just using linear orderings. It is usually stated more esoterically.

A linear ordering D is inaccessible iff

i. D has a limit point.
ii. Every function from the power set of any given proper initial segment of D, into D, stays within some proper initial segment of D.

Without i, we can use the positive integers. Without ii, we can use the positive integers with ∞ at the top.

THEOREM 4. Suppose there are two inaccessible cardinalities. Then "there exists an inaccessible linear ordering" is independent of ZFC.

- Inaccessibles ~ Grothendieck Universes.
- Large Cardinals required for Emulation Theory are far more ferocious.
- Emulation Theory gets to the essence of Theorem 3 while staying in Q[0,1]!

REPEATING:

THEOREM 3. Every $S \subseteq Q[0,1]^2$ is drop equivalent at some $(x,x),(x',x)$, $0 < x < x'$, provided we replace $Q[0,1]$ by some gigantic dense linear ordering with endpoints 0,1. The size required is far beyond anything proved to exist in ZFC.

The large cardinals involved in Theorem 3 are treated in

H. Friedman, Subtle Cardinals and Linear Orderings, Annals of Pure and Applied Logic, Volume 107, Issues 1-3, 15 January 2001, Pages 1-34. https://u.osu.edu/friedman.8/files/2014/01/subtlecardinals-1tod0i8.pdf

PROTOTYPE 1. For subsets of $Q[0,1]^2$, some MAXIMAL EMULATION is drop equivalent at some $(x,x),(x',x)$, $0 < x < x'$.

Thus we don't use any old subset of $Q[0,1]^2$, but rather some sort of associate.

• Maximal Emulations, yet to be defined, allow rationals to be moved around in order preserving ways.
• Order is used on Q[0,1], and NOTHING more. • This allows for a SIMPLIFICATION here. We can say what x,x' are IN ADVANCE.
• We use the friendly numbers 1/2,1.

PROTOTYPE 2. For subsets of $Q[0,1]^2$, some MAXIMAL EMULATION is drop equivalent at $(1,1/2),(1/2,1/2)$.

The above is the Lead Statement in Emulation Theory for dimension 2 - once I tell you what maximal emulations are.

DEFINITION 2. $x,y \in Q^k$ are order equivalent iff their coordinates have the same relative order. I.e., for all $1 \leq i,j \leq k$, $x_i < x_j$ iff $y_i < y_j$. S is a 1-emulation of $E \subseteq Q[0,1]^2$ iff $S \subseteq Q[0,1]^2$ and E,S have the same elements up to order equivalence.

EXERCISE. Every subset of $Q[0,1]^2$ has a maximal 1-emulation. In fact, it is unique.

MAXIMAL EMULATION DROP/1. MED/1. For subsets of $Q[0,1]^2$, some maximal 1-emulation is drop equivalent at (1,1/2),(1/2,1/2).

But MED/1 is actually very easy to prove.

- Maximal 1-emulations are very simple.
- Every maximal 1-emulation is merely a union of equivalence classes under order equivalence on $Q[0,1]^2$.
- Easy exercise that every such union is automatically drop equivalent at (1,1/2),(1/2,1/2).

But that is merely 1-emulation.

DEFINITION 3. S is an r-emulation of $E \subseteq Q[0,1]^2$ if and only if S^r,E^r have the same elements up to order equivalence of 2r-tuples.

The idea behind r-emulation is that E,S have the same r fold interactions between elements, from a strictly order theoretic point of view.

EXERCISE. Every subset of $Q[0,1]^2$ has a maximal r-emulation. If $r \geq 2$, not necessarily unique.

MAXIMAL EMULATION DROP/2. MED/2. For subsets of $Q[0,1]^2$, some maximal r-emulation is drop equivalent at (1,1/2),(1/2,1/2).

What is the status of MED/2? Is it provable in ZFC?

- We prove MED/2 using the existence of an uncountable set, well within ZFC.
- Suspect countable set theory or ZFC\P is not enough.

We now go to THREE DIMENSIONS!

MAXIMAL EMULATION DROP/3. MED/3. For subsets of $Q[0,1]^3$, some maximal r-emulation is drop equivalent at (1,1/2,1/3),(1/2,1/3,1/3).

Here we require: for all $p < 1/3$, $(1,1/2,p) \in S \leftrightarrow (1/2,1/3,p) \in S$. I.e., drop vertically from points (1,1/2,1/3),(1/2,1/3,1/3) in the cube $Q[0,1]^3$ down to the base $z = 0$.

- Our proof of MED/3 uses the large cardinals mentioned before with Theorem 3.
- We think it likely that MED/3 is not provable in ZFC.
- The claim we are making is that

MAXIMAL EMULATION DROP/4. MED/4. For subsets of $Q[0,1]^k$, some maximal r-emulation is drop equivalent at (1,1/2,...,1/k),(1/2,...,1/k,1/k).

is provably equivalent, over WKL_0, to Con(SRP), SRP = ZFC + $\{$there exists a k-SRP ordinal$\}_k$. Thus MED/4 is independent of ZFC.

Low dimension situation should clarify in 2017. MED/4 still involves countably infinite objects. The given subset of $Q[0,1]^k$ can be taken to be finite, but the maximal emulation cannot. We naturally demand more concreteness. Emulation Theory addresses this in two different ways.

- The Implicit Way. Use Math Logic Machinery to uniformly convert statements of a form similar to MED/4 into equivalent statements involving only finite objects.
- The Explicit Way. Dig in deeper and say similar things of similar simplicity, involving only finite objects.

THE IMPLICIT WAY

The logical form of MED/4 (using only finite given sets, which is equivalent) is such that it is an easy undergraduate math logic exercise to reformulate it as asserting that an effectively given list of sentences in first order predicate calculus with equality each have a countable model.

By Gödel's Completeness (not Incompleteness) Theorem, MED/4 is equivalent to a statement involving proofs in predicate calculus, with only finite objects. The explicitly finite statement thus obtained is in Π^0_1 form.

There is an important feature of Π^0_1 sentences such as FLT, called provable falsifiability. We know, a priori, that if a given Π^0_1 statement is false then it can in principle be verified to be false.

In fact, under a careful treatment, provable falsifiability is equivalent to being implicitly Π^0_1.

However, the Π^0_1 forms obtained by this general method lose their purely mathematical character. So we can, and do, want more.

THE EXPLICIT WAY

We discovered a new approach recently. Let's examine MED/4 again:

MED/4. For subsets of $Q[0,1]^k$, some maximal r-emulation is drop equivalent at (1,1/2,...,1/k),(1/2,...,1/k,1/k).

PROTOTYPE. For finite subsets of $Q[0,1]^k$, some finite weakly maximal r-emulation is drop equivalent at (1,1/2,...,1/k),(1/2, ...,1/k,1/k).

I won't get into this further here.

Emulation Theory is now interacting with the nearly largest large cardinal hypotheses using new ideas approaching compatibility with ordinary mathematical culture.

We'll stop and invite you to follow Emulation Theory progress and other topics on the FOM email list at

FOM Information Page http://www.cs.nyu.edu/mailman/listinfo/fom
FOM Archives
http://www.cs.nyu.edu/pipermail/fom/

IT APPEARS THAT MATH HAS SURVIVED THIS TALK!