UNPROVABLE THEOREMS

by
Harvey M. Friedman
Distinguished University Professor
Mathematics, Philosophy, Computer Science
Ohio State University
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/

Boston Mathematics Colloquium
delivered at MIT
October 8, 2009

It’s great to be back here!

I was a math student 1964-67, and remember taking courses here in 2-190, and in 2-290!

I started as a Freshman and finished with a Ph.D. MIT decided to get rid of me early!

I don’t remember if I got as high as 2-390, but I distinctly remember taking my first logic course - as a Freshman - with Hartley Rogers, in Fall 1964 - here in 2-190. Or was it in 2-290?

The textbook was Elliot Mendelson’s, Introduction to Mathematical Logic, still a good textbook today.

I knew that logic was supposed to be the basis of all thinking (maybe a bit naive considering, e.g., the political world).

I remember asking Hilary Putnam - then a Professor in the Philosophy Department here - “how does logic begin?” Our meeting was outside Walker Memorial Cafeteria. I’m still pondering that one.

And I remember talking about recursion theory inside my thesis advisor’s fancy new sports car. The proud owner was Gerald Sacks, then at MIT.

What This Is About:
The Search

When I was a student way back in 1964, I was fascinated by the drama created by the great legendary figure Kurt Gödel (died 1978):

there are mathematical statements that cannot be proved or refuted using the usual axioms and rules of inference of mathematics.

Furthermore, Gödel showed that this cannot be repaired, in the following sense:

even if we add finitely many new axioms to the usual axioms and rules of inference of mathematics, there will remain mathematical statements that cannot be proved or refuted.

These startling results are taught in the usual mathematical logic curriculum. One common way of proving these results provides no examples.

So what about the examples? I.e., examples of such ***INCOMPLETENESS***?

STANDARD EXAMPLES OF INCOMPLETENESS

1. That "the usual axioms and rules of inference for mathematics does not lead to a contradiction".
   I.e., "ZFC does not have a contradiction" is neither provable nor refutable in ZFC.

2. That "every infinite set of real numbers is either in one-one correspondence with the integers or in one-one correspondence with the real line".
   I.e., "the continuum hypothesis of Cantor" is neither provable nor refutable in ZFC.

These and related examples appear in the mathematical logic curriculum.

Note that these examples are very much associated with abstract set theory, and unusually far removed in spirit and content from traditional down to earth mathematics.

I was very aware of this disparity, even as a student, which was reinforced in conversations with other students and Professors.

For several decades I have been seeking examples of a new "down to earth" kind. This has been an ongoing process. Recently, there has been some particularly clear progress. I will highlight the main events up through now.

WHAT IS AN UNPROVABLE THEOREM?

The title of the talk mentions “Unprovable Theorems”.

These are a particularly important kind of statement neither provable nor refutable in ZFC (the usual axioms and rules of inference of mathematics).

An Unprovable Theorem is a theorem that is

i. proved using a by now well studied hierarchy of additional axioms for mathematics called the “large cardinal hierarchy”.

ii. cannot be proved (or refuted) with only the usual axioms for mathematics.

The highlight of this talk is the presentation of some examples of Unprovable Theorems of a radically new kind.

They will take the form of Fixed Point Theorems in a discrete setting. We will also present elegant finite approximations.

DOES THIS TALK HAVE ANYTHING TO DO WITH THE AXIOM OF CHOICE?

Many mathematicians think that if somebody is talking about Unprovability, they are talking about an axiom of choice (AxC) issue.

This talk has nothing to do with AxC for the following interesting reason.

THEOREM (Gödel). If a reasonably concrete sentence can be proved using the AxC, then it can also be proved without using the AxC.

Since we are talking exclusively about reasonably - and often very - concrete sentences, the axiom of choice is entirely irrelevant.

In any case, we will always assume that the axiom of choice is available to be used.

This talk has everything to do with how big a dose of infinite thinking that we need to use.

HOW DO PREVIOUS UNPROVABLE THEOREMS DIFFER FROM NORMAL MATHEMATICS?

I have addressed this question earlier. I want to repeat what I said in more specific terms.

Previous examples of Unprovable Theorems have one or more of the following features.

1. They are about formal systems for doing mathematics. If reformulated in terms of usual mathematical objects, they become hopelessly artificial.

2. They involve uncountable objects of a pathological nature. If the Unprovable Theorem is specialized to objects of limited pathological nature, then it becomes a Theorem of ZFC.

For more than 40 years, I have been developing examples of Unprovable Theorems which do not have these features.

The ongoing research has been driven by the issue of the quality of the examples.

WHAT FEATURES DRIVE THE QUEST FOR NEW UNPROVABLE THEOREMS?

We seek the following features.

1. The Unprovable Theorem should involve only objects of the most concrete and familiar kind from normal mathematics.

2. The Unprovable Theorem should be simple to state, and be free of ad hoc features - as is characteristic of good normal mathematics.

3. The Unprovable Theorem should have an intrinsic interest on its own, or part of a clearly stated and well motivated systematic investigation.

The examples we present today represent a substantial breakthrough with regard to these criteria over what we were able to do even earlier in 2009.

They now take the form of Fixed Point Theorems in a discrete setting.

WHAT IS THE FUTURE OF THIS SEARCH FOR UNPROVABLE THEOREMS?

1. To uncover the most basic and fundamental combinatorial structures that are behind these new Unprovable Fixed Point Theorems.

2. To realize these combinatorial structures naturally in a variety of well studied contexts in algebra, geometry, and analysis.

3. To obtain Unprovable Theorems that fit well into standard algebra, geometry, and analysis.

4. To craft the demonstrably necessary tools from beyond ZFC for general use throughout normal mathematics.

If we don't do this, our successors will.

WHAT ARE SOME EARLIER EXAMPLES OF WEAKLY UNPROVABLE THEOREMS?

Over the years, we have developed a number of Weakly Unprovable Theorems, in this sense:

Although the Theorems can be proved in ZFC, they use portions of ZFC that are unexpectedly large compared to their statements.

LONG FINITE SEQUENCES FROM A FINITE ALPHABET

Is there a longest finite sequence $x_1,...,x_n$ from {1,2} such that a certain pattern is avoided?

PATTERN TO BE AVOIDED. $x_i,...,x_{2i}$ is a subsequence of $x_j,...,x_{2j}$, where $i < j \leq n/2$.

E.g., (2,1,2) is a subsequence of (1,2,2,2,1,1,1,2).

ANSWER: Yes. n = 11. Gifted high school students in Paul Sally's summer program can sometimes prove this.

Is there a longest finite sequence $x_1,...,x_n$ from {1,2,3} such that this pattern is avoided?

ANSWER: Yes. I gave a lower bound for n in

Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

$n(3) > A_{7198}(158386)$

where A_p is the p-th Ackermann function from Z^+ to Z^+.

WHAT IS THE ACKERMANN HIERARCHY OF FUNCTIONS?

There are many versions that differ slightly. Most convenient: functions $A_1, A_2, ...$ from Z^+ to Z^+ such that
i. $A_1(n) = 2n$.
ii. $A_{i+1}(n) = A_i A_i ... A_i(1)$, where there are n A_i's.

We make some derivations.

$A_k(1) = 2$. $A_k(2) = 4$.

$A_2(n) = 2^n$. $A_3(n)$ is an exponential stack of n 2's.

$A_3(3) = A_2A_2A_2(1) = A_2(4) = 16$. $A_3(4) = A_2(A_3(3)) = A_2(16) = 2^{16} = 65{,}536$.

$A_4(3) = A_3A_3A_3(1) = A_3(4) = 2^{16} = 65{,}536$.

$A_4(4) = A_3A_4(3) = A_3(65{,}536)$, which is an exponential stack of 2's of height 65,536.

$A_5(5)$ = hard to "see".

Recall $n(3) > A_{7198}(158386)$.

LONG FINITE SEQUENCES FROM A FINITE ALPHABET

Is there a longest sequence $x_1,...,x_n$ from {1,...,k} avoiding this pattern?

ANSWER: Yes, for any $k \geq 1$. However n(k), as a function of k, grows faster than all multiply recursive functions. The Ackermann function is a 2-recursive function.

This Theorem can be proved using just Induction (Peano Arithmetic).

It can be proved in 3 quantifier induction but not in 2 quantifier induction. This is an example of a Weakly Unprovable Theorem. See

Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

Also: $n(4) > AA...A(1)$, where there are $A_5(5)$ A's.

$A(n) = A_n(n)$.

COUNTABLE SETS OF REALS AND RATIONALS

After you teach pointwise continuity of functions from a set of reals into the reals, you can state the following theorem.

COMPARABILITY THEOREM. If A,B are countable sets of real numbers, then there is a one-one pointwise continuous function from A into B, or a one-one pointwise continuous function from B into A.

This was well known from the early 20th century if A,B are countable and closed.

Despite the elementary statement, my proof uses transfinite induction on all countable ordinals. I proved that this is required. See

Metamathematics of comparability, in: Reverse Mathematics, ed. S. Simpson, Lecture Notes in Logic, vol. 21, ASL, 201-218, 2005.

Transfinite induction on all countable ordinals is required even if for just sets of rationals A,B.

HOW DO WE SAY MATHEMATICALLY THAT TRANSFINITE INDUCTION ON ALL COUNTABLE ORDINALS IS REQUIRED?

There are good proof theoretic ways of saying this, but here is a mathematical way. Experience shows that if we have a Theorem of the form

*) $(\forall x \in X)(\exists y \in X)(R(x,y))$

where X is a complete separable metric space and R is a Borel relation, and if the proof is "normal", then there is a Borel function $H:X \to X$ such that

**) $(\forall x \in X)(R(x,H(x)))$.

A huge number of Theorems of analysis can be put in form *), where **) holds for some Borel H.

The Comparability Theorem can be put in form *), via infinite sequences of reals (R^∞). Yet there is no Borel H with **).

$f(x_1,...,x_k) \leq f(x_2,...,x_{k+1})$

THEOREM A. For all $k,r \geq 1$ and $f:N^k \to N^r$, there exist distinct $x_1,...,x_{k+1}$ such that $f(x_1,...,x_k) \leq f(x_2,...,x_{k+1})$ coordinatewise.

THEOREM B. For all $k \geq 1$ and $f:N^k \to N$, there exist distinct $x_1,...,x_{k+2}$ such that $f(x_1,...,x_k) \leq f(x_2,...,x_{k+1}) \leq f(x_3,...,x_{k+2})$.

THEOREM C. For all $k \geq 1$ and $f:N^k \to N$, there exist distinct $x_1,...,x_{k+1}$ such that $f(x_2,...,x_{k+1}) - f(x_1,...,x_k) \in 2N$.

For f given by an algorithm, A,B,C are statements in the language of Peano Arithmetic (PA).

We have shown that A,B,C cannot be proved in PA for (even very efficiently) computable functions f. For any fixed k, the can be proved in PA for computable f.

HOMEOMORPHIC EMBEDDINGS BETWEEN FINITE TREES

We use finite rooted trees. Each forms a topological space, with a notion of homeomorphic embedding between them. For our purposes, this is almost the same as an inf preserving one-one map from vertices into vertices.

J.B. KRUSKAL. In any infinite sequence of finite trees, one is homeomorphically embeddable in a later one.

Kruskal's proof and all subsequent proofs use uncountable sets. in particular, an infinite sequence of finite trees is constructed with reference to all such.

We proved that this is necessary. In fact, necessary even for very computable infinite sequences. See

Internal finite tree embeddings, in: Lecture Notes in Logic, volume 15, 62-93, 2002, ASL.

There are stronger results related to the Graph Minor Theorem of Robertson and Seymour. See

(with N. Robertson and P. Seymour), The Metamathematics of the Graph Minor Theorem, AMS Contemporary Mathematics Series, vol. 65, 1987, 229-261.

BOREL SETS IN THE PLANE AND ONE DIMENSIONAL BOREL FUNCTIONS

In any topological space, the Borel sets form the least σ algebra of sets containing the open sets. For uncountable Polish spaces (complete separable metric spaces), this leads to a hierarchy of Borel sets of length ω_1. However, most delicate issues arise at the finite levels, or even at the third level.

THEOREM. (Using a result of D.A. Martin from Infinitely Long Game Theory). Every Borel set in $\Re^2$, symmetric about the line y = x, contains or is disjoint from the graph of a Borel function from $\Re$ into $\Re$.

We proved that it is necessary and sufficient to use uncountably many iterations of the power set operation. For finite level Borel sets in $\Re^2$, it is necessary and sufficient to use infinitely many iterations of the power set operation. See

On the Necessary Use of Abstract Set Theory, Advances in Math., Vol. 41, No. 3, September 1981, pp. 209-280.

BOOLEAN RELATION THEORY

Boolean Relation Theory concerns Boolean relations between sets and their images under functions. This leads to Unprovable Theorems. There is a book draft on my website - Boolean Relation Theory and Incompleteness.

The two starting points of BRT are the ZFC theorems

THIN SET THEOREM. For all $f:N^k \to N$, there exists infinite $A \subseteq N$ such that $f[A^k] \neq N$.

COMPLEMENTATION THEOREM. For all strictly dominating $f:N^k \to N$, there is a unique $A \subseteq N$ such that $A \,\dot{\cup}\, f[A^k] = N$.

Strictly dominating means $f(x_1,...,x_k) > x_1,...,x_k$. Also $\dot{\cup}$ is disjoint union.

We restate as a Fixed Point Theorem:

COMPLEMENTATION THEOREM. For all strictly dominating $f:N^k \to N$, there is a unique $A \subseteq N$ such that $A = N \setminus f[A^k]$.

There are some mildly exotic features of proofs, more so with the Thin Set Theorem.

BOOLEAN RELATION THEORY

Let ELG be the set of all $f:N^k \to N$, $k \geq 1$, where there exist $c,d > 1$ such that

$$cmax(x) \leq f(x) \leq dmax(d)$$

holds for all but finitely many $x \in N^k$.

TEMPLATE. For all f,g in ELG, there exists infinite $A,B,C \subseteq N$ such that

$$X \,\dot{\cup}\, fY \subseteq V \,\dot{\cup}\, gW$$
$$P \,\dot{\cup}\, fQ \subseteq R \,\dot{\cup}\, gS.$$

where the letters X,Y,V,W,P,Q,R,S are among the letters A,B,C. fE is $f[E^k]$, where $dom(f) = N^k$, and $\dot{\cup}$ means "disjoint union".

There are $3^8 = 6561$ instances of the Template. All but 12 are provable/refutable in a very weak fragment of ZFC. The 12 are provable using strongly Mahlo cardinals of finite order, but not in ZFC.

$$A \,\dot{\cup}\, fA \subseteq C \,\dot{\cup}\, gB$$
$$A \,\dot{\cup}\, fB \subseteq C \,\dot{\cup}\, gC.$$

STRICTLY DOMINATING ORDER INVARIANT RELATIONS

$SDOI(Q^k)$ forms the class of binary relations on Q^k that we use for the Unprovable Fixed Point Theorem.

These are rather concrete - there are only finitely many such $R \subseteq Q^k \times Q^k = Q^{2k}$.

$OI(Q^k)$ is the class of order invariant $R \subseteq Q^k \times Q^k = Q^{2k}$. I.e., membership in R (as a 2k tuple) depends only on the relative order of the coordinates.

$SD(Q^k)$ is the class of strictly dominating $R \subseteq Q^k \times Q^k$. I.e., where $R(x,y) \rightarrow \max(x) < \max(y)$.

$SDOI(Q^k) = OI(Q^k) \cap SD(Q^k)$.

The $R \in OI(Q^k)$ have nice canonical presentations as a finite set of 2k tuples from $\{1,...,2k\}$ whose set of coordinates forms an initial segment of $1,...,2k$.

The $R \in SDOI(Q^k)$ have canonical presentations meeting the obvious requirement.

EASY FIXED POINT THEOREM

Let cube(A) be the least V^k containing A.

TRIVIAL FIXED POINT THEOREM. For all $R \in SDOI(Q^k)$, some $A = cube(A) \setminus R[A]$. (Set $A = \emptyset$).

For $A \subseteq Q^k$, $X \subseteq Q$, let cube(A,0) be the least V^k such that $A \subseteq V^k \wedge 0 \in V$.

BABY FIXED POINT THEOREM. For all $R \in SDOI(Q^k)$, some $A = cube(A,0) \setminus R[A]$. (Set $A = \{(0,...,0)\}$).

EASY FIXED POINT THEOREM. For all $R \in SDOI(Q^k)$, some $A = cube(A,0,1,...) \setminus R[A]$. (Arrange $A = \{0,1,...\}^k \setminus R[A]$).

Let $R \in SD(Q^k)$. Define A by induction. Suppose membership has been decided for all x with $max(x) < n$, $n \geq 0$. Let $max(x) = n$. Put x in A if and only if $x \notin R[A \cap (-\infty,n)^k]$. Then for all $x \in N^k$, $x \in A$ iff $x \notin R[A]$, as required. For $A = N^k \setminus R[A]$, A is unique.

WELL ORDERED FIXED POINT THEOREM. Let $X \subseteq Q$ be well ordered. For all $R \in SDOI(Q^k)$, some $A = cube(A,X) \setminus R[A]$. (Arrange $A = B^k \setminus R[A]$).

THE UNPROVABLE UPPER SHIFT FIXED POINT THEOREM

The upper shift of $x \in Q^k$ is obtained by adding 1 to all nonnegative coordinates of x.

The upper shift of $A \subseteq Q^k$ is the set of upper shifts of elements of A.

UPPER SHIFT FIXED POINT THEOREM. For all $R \in SDOI(Q^k)$, some $A = cube(A,0)\backslash R[A]$ contains its upper shift.

This is an Unprovable Theorem.

THEOREM. There exists $R \in SDOI(Q^k)$ such that there is no $A = Q^k\backslash R[A]$.

FINITE APPROXIMATIONS

For all $R \in SDOI(Q^k)$, there exist finite $A_1,A_2,... \subseteq Q^k$ such that for all $i \geq 1$, $A_{i+1} = cube(A_{i+1},0)\backslash R[A_{i+2}]$ contains $A_i \cup us(A_i)$.

For all $R \in SDOI(Q^k)$, there exist finite $A_1,...,A_k \subseteq Q^k$ such that for all $1 \leq i \leq k-2$, $A_{i+1} = cube(A_{i+1},0)\backslash R[A_{i+2}]$ contains $A_i \cup us(A_i)$.

For all $R \in SDOI(Q^k)$, there exist finite $A_1,...,A_k \subseteq Q^k$ such that for all $1 \leq i \leq k-2$, $A_{i+1} = cube(A_{i+1},0)\backslash R[A_{i+2}]$ contains $A_i \cup us(A_i)$, where the numerators and denominators of the rationals used in the A's have magnitudes at most (8k)!.

It is provable in a weak fragment of ZFC that these sequential forms are equivalent to the original form.

Look how concrete the third formulation is. It is in what is called Π^0_1 form.

WHAT ARE THE LARGE CARDINALS USED FOR BOOLEAN RELATION THEORY AND FOR THE UPPER SHIFT FIXED POINT THEOREM? strongly inaccessible cardinals not enough!

An (von Neumann) ordinal is the set of its predecessors, and a (von Neumann) cardinal is an ordinal not equinumerous with any predecessor.

We later give a purely order theoretic treatment of those used for the Upper Shift Fixed Point Theorem.

κ is a strong limit cardinal iff for all $\alpha < \kappa$, $\mathrm{card}(\wp(\alpha)) < \kappa$.

κ is a regular cardinal iff κ is not the sup of a subset of κ of cardinality $< \kappa$.

κ is an inaccessible cardinal iff κ is a regular strong limit cardinal $> \omega$.

ZFC does not suffice to prove the existence of a strongly inaccessible cardinal.

Grothendieck Topoi (strong kind).

WHAT ARE THE LARGE CARDINALS USED FOR BOOLEAN RELATION THEORY?

strongly k-Mahlo cardinals

κ is a strongly 0-Mahlo cardinal iff κ is a strongly inaccessible cardinal.

κ is a strongly n+1-Mahlo cardinal iff κ is a strongly n-Mahlo cardinal such that every closed and unbounded subset of κ has an element that is a strongly n-Mahlo cardinal.

The 12 exotic cases in Boolean Relation Theory are provable in

SMAH+ = ZFC + "for all k there exists a strongly k-Mahlo cardinal",

but not in any consistent fragment of

SMAH = ZFC + {there exists a strongly k-Mahlo cardinal}.

In fact, they are provably equivalent, in a weak fragment of ZFC, to the 1-consistency of SMAH.

WHAT ARE THE LARGE CARDINALS USED FOR THE UPPER SHIFT FIXED POINT THEOREM?

k-subtle cardinals

k-large ordinals

We say that $f:\alpha^k \to \alpha$ is regressive iff for all $0 < \beta_1,\ldots,\beta_k < \alpha$, $f(\beta_1,\ldots,\beta_k) < \min(\beta_1,\ldots,\beta_k)$.

α is k-large iff for all $f:\alpha^k \to \alpha$, there exist $1 < \beta_1 < \ldots < \beta_{k+1}$ such that $f(\beta_1,\ldots,\beta_k) = f(\beta_2,\ldots,\beta_{k+1})$.

The k-large ordinal hierarchy is a simplified form of the k-subtle cardinal hierarchy.

The Upper Shift Fixed Point Theorem is provable in

SUB+ = ZFC + “for all k there exists a k-large ordinal”,

but not in any consistent fragment of

SUB = ZFC + {there exists a k-large ordinal}$_k$.

In fact, it is provable equivalent, in a weak fragment of ZFC, to the consistency of SUB.

WHAT ARE THE LARGE CARDINALS USED FOR THE UPPER SHIFT FIXED POINT THEOREM?
k-critical linear orderings

We say that a linear ordering $(X,<)$ is k-critical iff
i. it has no endpoints.
ii. for all regressive $f:X^k \to X$, there exists $b_1 < \ldots < b_{k+1}$ such that $f(b_1,\ldots,b_k) = f(b_2,\ldots,b_{k+1})$.

THEOREM. The following are provably equivalent in ZFC.
i. For all k, there exists a k-subtle cardinal.
ii. For all k, there exists a k-large ordinal.
iii. For all k, there exists a k-critical linear ordering.

The Upper Shift Fixed Point Theorem is provable in

ZFC + "for all k there is a k-critical linear ordering"

but not in any consistent fragment of

ZFC + $\{$there is a k-critical linear ordering$\}_k$.

See: *Subtle Cardinals and Linear Orderings, Annals of Pure and Applied Logic Volume 107, Issues 1-3, 15 January 2001, Pages 1-34.*

A TEMPLATE

Recall

UPPER SHIFT FIXED POINT THEOREM. For all R ∈ SDOI(Q^k), some A = cube(A,{0})\R[A] contains its upper shift.

Note that the upper shift is the coordinatewise lifting of the one dimensional upper shift us:Q → Q.

Let M be any system of finitely many partial piecewise linear functions from Q into Q with rational coefficients. For A ⊆ Q^k, write M[A] for the image of A under the coordinatewise lifting of the components of M.

TEMPLATE. Let M be as given. Is it the case that for all R ∈ SDOI(Q^k), there exists A = cube(A,{0})\R[A] containing M[A]?

CONJECTURE. Every instance of the Template is refutable in a weak fragment of ZFC, or provable in SUB+.

This Template is subject to finite approximations analogous to those for the Upper Shift Fixed Point Theorem.

WHAT ABOUT THE STRONGEST LARGE CARDINAL HYPOTHESES?

We can extend conveniently to correspond to the strongest of the large cardinal hypotheses.

Let $A,B \subseteq Q^k$. A sharply contains B iff A contains B, and every lower cross section of B is a lower cross section of A. Lower cross sections of A are sets of the $\{(c,x_2,\ldots,x_k) \in A: x_2,\ldots,x_k < c\}$, $c \in Q$.

$Q^{k\leq}$ is the set of all $x \in Q^k$, where each coordinate is $\leq$ the next. A is B on C means $A \cap C = B \cap C$.

SHARP UPPER SHIFT THEOREM. For all $R \in SDOI(Q^k)$, some A is $cube(A,\{0\})\backslash R[A]$ on $Q^{k\leq}$, and sharply contains its upper shift.

The above corresponds to what is called the huge cardinal hierarchy.

Let $h:Q \to Q$, where $h(x) = (x+1)/2$ if $x \in [0,1]$; x if $x < 0$; undefined otherwise.

Using both the upper shift and h pushes it higher than I1 but lower than I2. Finite approximations are palatable, but present opportunities for substantial simplifications.