CONCRETE MATHEMATICAL INCOMPLETENESS

by

Harvey M. Friedman

Distinguished University Professor

Mathematics, Philosophy, Computer Science

Ohio State University

friedman@math.ohio-state.edu

University of Cambridge

Cambridge, England

November 8, 2010

minor revision: November 18, 2010

What This Is About:
The Search

When I was a student (long time ago), 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?

All of the examples of Concrete Incompleteness that we are going to talk about, come under the category of what we call **UNPROVABLE THEOREMS.**

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.

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

These will take the form of structural properties of kernels in digraphs.

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.

BORROWING FROM THE FUTURE

Are there clearly stated propositions of a concrete (especially discrete and finite) nature, from the existing literature, which cannot be proved or refuted from ZFC?

We believe that there is not such a proposition.

We will present some examples from the literature - and some that are implicit in the literature - that are discrete/finite, and cannot be proved or refuted in substantive **fragments** of ZFC. More later...

Accordingly, we look to the future. We identify what we believe to be inevitable future mathematical investigations that lead directly to such examples.

Boolean Relation Theory, and Kernel Structure Theory.

WHAT METHOD IS USED TO ESTABLISH UNPROVABILITY HERE?

Concrete Mathematical Incompleteness cannot be established through the usual methods for showing unprovability in set theory - via Gödel's constructible set construction, or Cohen's method of forcing.

Suppose we want to show sentence A is not provable in ZFC. Start by assuming A. Then construct a model of ZFC through a long series of gradual refinements. Thus:

ZFC + A proves that ZFC is consistent.

If ZFC proves A, then

ZFC proves ZFC is consistent.

However, Gödel shows that this is impossible (assuming ZFC is in fact consistent). Hence ZFC does not prove A.

Note that we have assumed that ZFC is consistent for this unprovability result. This is of course a necessary assumption.

HOW ARE LARGE CARDINALS USED TO PROVE CONCRETE THEOREMS?

Roughly as follows.

Start with your concrete problem in the integers or rationals.

Blow up the data to an enormous space of size a large cardinal.

Do large cardinal combinatorics to build a structure of size the large cardinal.

Build countable, or even finite, approximations to the enormous structure.

At the end, the large cardinal and large cardinal sized structures and constructions disappear.

In the relevant situations, we know that use of the large cardinals is unavoidable.

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.

These examples were originally from Borel measurable mathematics, and later in discrete and finite mathematics.

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 $A_1, A_2, \ldots$ from Z^+ to Z^+ such that

i. $A_1(n) = 2n$.

ii. $A_{i+1}(n) = A_iA_i \ldots A_i(1)$, 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.

Ackermann function is $A(n) = A_n(n)$. A(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 $f:N^k \rightarrow N^r$, 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 $f:N^k \rightarrow N$, 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 $f:N^k \rightarrow N$, 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.

If we require that $\max(f(x)) \leq \max(x)$, then we obtain the existence of a uniform upper bound on the $x_1,...,x_{k+1}$. This yields a finite statement that is not provable in Peano Arithmetic.

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 $A \cup. f[A^k] = N$.

Strictly dominating means $f(x_1,...,x_k) > x_1,...,x_k$. Also $\cup.$ 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 $A = N \backslash f[A^k]$.

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

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

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

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fQ \subseteq R \cup. gS.$$

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 $\cup.$ 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.

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

DIGRAPHS AND KERNELS

A digraph is a pair G = (V,R), where R $\subseteq$ V × V. The elements of V are the vertices, and the elements of R are the edges.

E is a kernel in G if and only if

i. No element of E is connect to any element of E.
ii. Every x $\in$ V\E is connected to an element of E.

A dag is a digraph with no cycles.

THEOREM. von Neumann. There is a unique kernel in every finite dag.

Extensive literature on kernels in digraphs. Dual notion is: dominators in digraphs.

DIGRAPHS ASSOCIATED WITH SETS OF RATIONALS

Now fix $A \subseteq Q$, where Q is the rationals.

We are interested in a basic family of digraphs associated with A. These are the digraphs (A^k,E), where $E \subseteq A^{2k}$ is order invariant.

We call these the A-digraphs.

We say that (A^k,E) is downward if and only if for all x E y, we have max(x) > max(y).

FACT. There exists $A \subseteq Q$ such that every downward A-digraph has a kernel. In fact, it suffices that A is well ordered. The kernel will be unique.

PROTOTYPE. There exists $A \subseteq Q$ such that every downward A-digraph has a kernel with a structural property.

THE UPPER SHIFT

The upper shift on Q is defined by

$$\mathrm{ush}(q) = q \text{ if } q < 0;\ q+1 \text{ if } q \geq 0.$$

Note the singularity at 0. The upper shift extends to vectors coordinatewise. The upper shift of a set of vectors is the set of the upper shifts of its elements.

AN UNPROVABLE THEOREM

UPPER SHIFT KERNEL THEOREM. There exists $0 \in A \subseteq Q$ such that every downward A-digraph has a kernel containing its upper shift.

SEMILINEAR KERNEL TEMPLATE

Let T:Q → Q. Then T extends to Q^k coodinatewise.

Rational semilinear subsets of Q^k are Boolean combinations of linear inequalities with rational coefficients.

SEMILINEAR KERNEL TEMPLATE. Let T:Q → Q be rational semilinear. There exists $0 \in A \subseteq Q$ such that every A-digraph has a kernel containing its diagonal image under T.

The Kernel Structure Theorem is the instance where T = ush (the upper shift).

We should be able to prove or refute each instance of this Template, with the help of a suitable large cardinal axiom.

FINITE FORM

UPPER SHIFT KERNEL THEOREM. There exists $0 \in A \subseteq Q$ such that every downward A-digraph has a kernel containing its upper shift.

FINITE UPPER SHIFT KERNEL THEOREM. Let $n \geq 1$. There exists finite $0 \in A \subseteq Q$ such that every downward A-digraph has an n-kernel containing its bounded upper shift. We can require that every element of A has norm at most $8n^2$.

We say that S is an n-kernel if and only if

i. No element of S is connected to an element of S.
ii. Every $x \in A^k \backslash S$ of norm $p \leq n$ is connected to an element of S of norm $\leq 8p^2$.

The bounded upper shift of S is the set of elements of its upper shift whose max is at most the max of some element of S.

This equivalent finite form is still just as unprovable.

WHAT ARE THE LARGE CARDINALS USED FOR BOOLEAN RELATION THEORY?
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.

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 (assuming SMAH is consistent) not in

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 KERNEL THEOREM?

k-SRP ordinals

Let λ be a limit ordinal. We say that $E \subseteq \lambda$ is stationary if and only if E meets every closed and unbounded subset of λ.

We say that a limit ordinal λ has the k-SRP if and only if every 2 coloring of its k element subsets is monochromatic on a stationary subset of λ.

The Upper Shift Kernel Theorem is provable in

SRP^+ = ZFC + "for all k there exists a k-SRP ordinal",

but (assuming SRP is consistent) not in

SRP = ZFC + $\{$there exists a k-SRP ordinal$\}_k$.

In fact, they are provable equivalent, in a weak fragment of ZFC, to the consistency of SRP.