DOES NORMAL MATHEMATICS NEED NEW AXIOMS?

by
Harvey M. Friedman*
Department of Mathematics
Ohio State University
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/

October 26, 2001
Lecture Notes

Abstract. We present a range of mathematical theorems whose proofs require unexpectedly strong logical methods, which in some cases go well beyond the usual axioms for mathematics.

****

There are a variety of mathematical results that can only be obtained by using more than the usual axioms for mathematics. For several decades there has been a gradual accumulation of such results that are more and more concrete, more and more connected with standard mathematical contexts, and more and more relevant to ongoing mathematical activity.

Probably the most well known mathematical problem that cannot be proved or refuted with the usual axioms (ZFC) is the continuum hypothesis - that every set of real numbers is either countable or of cardinality the continuum (Kurt Gödel and Paul Cohen).

But mathematicians have instinctively learned to hide from this kind of problem by focusing on relatively "concrete" subsets of complete separable metric spaces. In particular, the Borel measurable sets and functions in and between complete separable metric spaces proves to be a natural boundary.

By way of illustration,

"every Borel set of real numbers is either countable or of cardinality the continuum via a Borel measurable function"

is a well known theorem of descriptive set theory.

All problems discussed here live within this Borel measurable universe. Some are even further down in sets and functions on the integers.

1. Exotic High School Math. Warmup.
2. Ordinals in Freshman Calculus. Warmup.
3. Borel Measurable Selection.
4. Thin Set Theorem. Warmup.
5. Complementation Theorem. Warmup.
6. Disjoint Covers.
7. Boolean Relation Theory.
8. A Sketch.

1. EXOTIC HIGH SCHOOL MATH.

This problem was used a few years ago in Paul Sally's program for gifted high school students at U Chicago.

THEOREM 1.1. There is a longest sequence of 1's and 2's in which no block $x_i,...,x_{2i}$ is a subsequence of a later block $x_j,...,x_{2j}$. The longest length is 11.

Ex: 12221111111. The relevant blocks are 12, 222, 2211, 21111, 111111. None is a subsequence of any later one.

One of the students was able to give a correct proof of this.

THEOREM 1.2. There is a longest finite sequence of 1's, 2's, 3's, in which no block $x_i,...,x_{2i}$ is a subsequence of a later block $x_j,...,x_{2j}$.

The students couldn't prove this. The natural proof is very infinitary, and the longest length is gigantic. More detailed work gives a less infinitary proof, but all proofs must be somewhat exotic. More generally:

THEOREM 1.3. For all $k \geq 1$ there exists a longest finite sequence from $\{1,...,k\}$ in which no block $x_i,...,x_{2i}$ is a subsequence of any later block $x_j,...,x_{2j}$.

Theorem 1.3 can be proved using induction with 3 quantifiers over the positive integers, but not using induction with just 2 quantifiers over the positive integers.

As for bounds, let $n(k)$ be the longest length with k letters. Then $n(1) = 3$, $n(2) = 11$.

$n(3) > A_{7198}(158386)$, where $A_k(n)$ is the k-th function in the Ackermann hierarchy at n. A_1 = doubling, A_2 = base 2 exponentiation, A_3 = base 2 superexponentiation, etcetera.

See [Fr01].

2. ORDINALS IN FRESHMAN CALCULUS.

Here is a theorem in what used to be freshman calculus that is apparently new.

THEOREM 2.1. Let A,B be countable sets of real numbers. There is a one-one continuous function from A into B or there is a one-one continuous function from B into A.

This is the usual □/□ point-wise continuity notion.

The proof uses a countable ordinal analysis of the topology of countable sets of real numbers (or countable metric spaces).

There are several ways to indicate that the use of countable ordinals is necessary to prove Theorem 2.1.

THEOREM 2.2. There is no Borel function that takes a pair of countable sets of reals, given as infinite sequences, to a one-one continuous function from one into the other. There is no Borel function F: x □ {0,1} such that if F(x,y) = 0 then there is a one-one continuous map from rng(x) into rng(y), and if F(x,y) = 1 then there is a one-one continuous map from rng(y) into rng(x).

For those familiar with reverse mathematics, Theorem 2.1 is provably equivalent to ATR_0 over RCA_0.

See [Frxx].

3. BOREL MEASURABLE SELECTION.

Example: The function $(1-x^2)^{1/2}$ on [-1,1] is a selection for the unit circle on the set [-1,1]. It is also a selection for the unit circle.

Let S be a set of ordered pairs and A be a set. We say that f is a selection for S on A iff dom(f) = A and for all x □ A,

$(x,f(x)) \in S$. We say that f is a selection for S iff f is a selection for S on $\{x: (\exists y)((x,y) \in S)\} = dom(S)$.

We use for the reals with the usual topology.

THEOREM 3.1. Let $S \subseteq$ ^{2} be Borel and symmetric about the line $y = x$. Then S has a Borel selection on or $^2\backslash S$ has a Borel selection on .

This is closely related to an earlier theorem of D.A. Martin called Borel determinacy, involving infinite zero sum games.

Theorem 3.1 can be proved using uncountably many iterations of the power set operation, but not using only countably many iterations of the power set operation. See [Fr81].

Recent developments in Borel selection come from work of two analysts at University of Paris:

THEOREM 3.2. Let $S \subseteq$ ^{2} be Borel and $E \subseteq$ be Borel. If there is a Borel selection for S on every compact subset of E, then there is a Borel selection for S on E.

By Debs/Saint Raymond, Theorem 3.2 can be proved using large cardinal axioms. We proved that Theorem 3.2 cannot be proved in ZFC. There is a rather weak form of Theorem 3.2 that cannot be proved in ZFC.

THEOREM 3.3. Let $S \subseteq$ ^{2} be Borel. If there is a Borel selection for S on every compact set of irrationals, then there is a Borel selection for S on the irrationals.

Here is a continuous form which can be proved using uncountably many iterations of the power set operation, but not using only countably many iterations of the power set operation.

THEOREM 3.4. Let $S \subseteq$ ^{2} be Borel. If there is a continuous selection for S on every compact set of irrationals, then there is a continuous selection for S on the irrationals.

See [Fryy].

4. THIN SET THEOREM.

THEOREM 4.1. Thin Set Theorem. Let f be a multivariate function from **Z** into **Z**. There exists infinite A $\subseteq$ **Z** such that fA $\neq$ **Z**.

Here fA is the set of all values of f at arguments from A.

If you know the right branch of combinatorics, then this is not hard. Otherwise, you pretty much have to reinvent it.

We know that Theorem 4.1 cannot be proved constructively, even in dimension 2.

One precise way of saying this is the following.

THEOREM 4.2. There exists a computable f:$\mathbf{Z}^2$ $\to$ **Z** such that for all infinite computable A $\subseteq$ **Z**, fA = **Z**.

For those who know reverse math, TST is provable in ACA but not in ACA_0. TST in dimen-sion 2 is not provable in WKL_0.

Notice the logical form of TST. For any function of a certain kind there is a set of a certain kind such that some Boolean relation holds between the set and the image of the set under the function.

In fact, we do not even use the set. For any function of a certain kind there is a set of a certain kind such that some Boolean relation holds of the image of the set under the function. See [FS00] and [CGH].

5. THE COMPLEMENTATION THEOREM.

This can be viewed as a fixed point theorem. Let f be a multivariate function from **Z** into **Z**. We say that f is strictly dominating if and only if for all x $\in$ dom(f), |f(x)| > |x|. Here | | is the sup norm.

THEOREM 5.1. Complementation Theorem. Let f be a strictly dominating multivariate function from **Z** into **Z**. There exists infinite A $\subseteq$ **Z** such that fA = **Z**\A. Furthermore, there is a unique A $\subseteq$ **Z** such that fA = **Z**\A.

Suppose we have determined membership in A of all |x| < n.

For |x| = n, we inquire whether x ∈ f[A] thus far. If so, then x ∈ A. If not, then x ∉ A. Since f is strictly dominating, we never change our mind about x ∈ f[A].

There is obviously no leeway in this construction. Hence the uniqueness.

The structure of these unique fixed points is unclear, even in the case of one dimensional affine transformations, let alone higher dimensional transformations.

Note the logical form of the complementation theorem: For any function of a certain kind there is a set of a certain kind such that some Boolean relation holds between the set and the image of the set under the function.

6. DISJOINT COVERS.

The disjoint cover relation turns out to be an interesting Boolean relation between sets. We way that A is disjointly covered by B,C if and only if

i) A ⊆ B ∪ C;
ii) B ∩ C = ∅.

We write this as A/B,C.

Using this notation, we can restate the complementation theorem as follows.

COMPLEMENTATION THEOREM. Let f be a strictly dominating multivariate function from **Z** into **Z**. There exists infinite A ⊆ **Z** such that **Z**/A,fA.

We say that A ⊆ **Z** is bi-infinite if and only if A has infinitely many positive and infinitely many negative elements.

COMPLEMENTATION THEOREM? Let f be a strictly dominating multivariate function from **Z** into **Z**. There exists bi-infinite A ⊆ **Z** such that **Z**/A,fA.

This is refutable. A way to fix this is to weaken **Z**/A,fA by using something smaller than **Z**. The natural way is to bring in a second function.

THEOREM? Let f,g be strictly dominating multivariate functions from **Z** into **Z**. There exists bi-infinite A ⊆ **Z** such that fA/A,gA.

This is also refutable. The problem is that A is on the left and right sides of /. This suggests bringing in a second set.

THEOREM. Let f,g be strictly dominating multivariate functions from **Z** into **Z**. There exist bi-infinite A,B ⊆ **Z** such that fA/B,gB.

The natural extension to three sets is this.

THEOREM. Let f,g be strictly dominating multivariate functions from **Z** into **Z**. There exist bi-infinite A,B,C ⊆ **Z** such that fA/B,gB and fB/C,gC.

Does this make a difference?

THEOREM? Let f,g be strictly dominating multivariate functions from **Z** into **Z**. There exist bi-infinite A,B,C ⊆ **Z** such that fA/C,gB and fB/C,gC.

This turns out to be refutable. However, we can fix this by modifying the strict domination condition.

We say that f is expansively trapped if and only if there exists p,q > 1 such that

$$p|x| \leq |f(x)| \leq q|x|$$

holds for all x ∈ dom(f).

PROPOSITION. Let f,g be expansively trapped multivariate functions from **Z** into **Z**. There exist bi-infinite A,B,C ⊆ **Z** such that fA/C,gB and fB/C,gC.

This Proposition is provable, but the proof uses large cardinals (Mahlo cardinals of finite order). It is not provable in ZFC.

Note the logical form of the Proposition:

For all multivariate functions f,g of a certain kind there exists sets A,B,C of a certain kind such that some Boolean

relation holds between the three sets and their six images under the two functions.

7. BOOLEAN RELATION THEORY.

We have noted the logical form of the thin set theorem and the complementation theorem (and also the Proposition). Here are two more examples of this form.

a. Let f be a multivariate continuous function from into . There exists an unbounded open set A such that fA ≠ . (True).
b. Every bounded linear operator on Hilbert space maps some nontrivial closed subspace into itself. (Open problem).

We now give a formal presentation of Boolean relation theory.

If f is a multivariate function of arity n and A is a set then $fA = \{f(x_1,...,x_n): x_1,...,x_n \in A\}$.

A BRT setting is a pair (V,K) where V is a set of multivariate functions, and K is a set of sets.

Ex: Let V be the set of all multivariate functions from N into N, and K be the set of all infinite subsets of N.

Ex: Let V be the set of all strictly dominating multivariate functions from N into N, and K be as above.

We now describe equational Boolean relation theory in (V,K). In its most elemental from, it consists of analyzing all statements of the form

For all f ∈ V there exists A ∈ K such that a given Boolean equation holds between A,fA.

A Boolean equation between elements of K is an equation between Boolean terms – i.e., using the Boolean operations of intersection, union, and complementation.

Complementation is defined using

the set of all elements
of sets in K and
values of functions in V

as the universal set. It can be readily seen that there are 16 Boolean equations between two sets that are formally distinct.

More generally, we can attempt to analyze all statements of the form

For all $f_1,...,f_k \in V$ there exists $A_1,...,A_n \in K$ such that a given Boolean equation holds between the (k+1)n sets

$A_1,...,A_n$
$f_1A_1,...,f_1A_n$
...
$f_kA_1,...,f_kA_n$.

It can be readily seen that there are $2^{2^{(k+1)n}}$ such Boolean equations that are formally distinct.

It appears that equational Boolean relation theory is interesting for any interesting pair (V,K) – and frequently quite nontrivial even for just a single function and a single set. There are a great many such interesting pairs (V,K) throughout mathematics.

The Thin Set Theorem is an example of inequational Boolean relation theory. Here inequations play the exact role that equations play in equational Boolean relation theory, where an inequation is simply the negation of an equation.

We can go further and consider propositional combinations of equations, and even compound terms like $f(A \cap gB)$. We have not investigated these more involved situations.

Let ET(**Z**) be the set of all expansively trapped multivariate functions from **Z** into **Z**. Let INF(**Z**) be the set of all infinite subsets of **Z**. Let BINF(**Z**) be the set of all bi-infinite subsets of **Z**.

The Proposition is a statement in equational BRT on (ET(**Z**), BINF(**Z**)) with two functions and three sets.

CONJECTURE 1. Every one of the 2^{512} statements in equational BRT on (ET(**Z**),BINF(**Z**)) with two functions and three sets is provable or refutable using Mahlo cardinals of finite order.

Because of the Proposition, clearly ZFC does not suffice. What about (ET(**Z**),INF(**Z**))?

PROPOSITION'. Let f,g be expansively trapped multivariate functions from **Z** into **Z**. There exists infinite A,B,C $\subseteq$ **Z** such that fA/C,gB, fB/C,gC, and A $\cap$ fC = $\emptyset$.

This is provable using Mahlo cardinals of finite order but not in ZFC.

CONJECTURE 2. Every one of the 2^{512} statements in equational BRT on (ET(**Z**),INF(**Z**)) with two functions and three sets is provable or refutable using Mahlo cardinals of finite order.

We have given a complete analysis of equational and inequational BRT on (ET(**Z**),INF(**Z**)) and (ET(**Z**),BINF(**Z**)) with only one function and one set. Here it suffices to use only the very weak system ACA to prove or refute all statements that arise.

Note that the Proposition consists of two disjoint cover conditions in (ET(**Z**),BINF(**Z**)) with two functions and three sets.

In a slightly different context we have succeeded in analyzing all such statements with two disjoint cover conditions, using Mahlo cardinals of finite order.

8. A SKETCH.

PROPOSITION*. Let f,g be integral piecewise polynomials obeying $|f(x)|,|g(x)| \geq 2|x|$. There exist bi-infinite A,B,C such that fA/C,gB and fB/C,gC.

We have shown that this also cannot be proved in ZFC.

Begin by blowing up the discrete ordered ring **Z** by a well ordered set of indeterminates of large cardinal length. This results in an enormous discrete ordered ring **R**.

Verify that the relation $|x| > 2|y|$ in **R** is well founded. Transfinite recursion is then applied to this well founded relation in order to construct the unique set A $\subseteq$ **R** such that **R**/A,gA. This is the same as the proof of the Complementation Theorem, only here we are in a transfinite context rather than **Z**.

It is easily seen that the indeterminates and their negatives all lie in A.

We then form the chain indexed by natural numbers

$\pm I = I_0 \subset I_1 \subset \ldots \subset A \subset \mathbf{R}$

'minimally', where each $fI_j/I_{j+1},gI_{j+1}$.

For any choice of $\pm I' \subset \pm I$, we can canonically form the chain indexed by natural numbers

$\pm I' = I_0' \subset I_1' \ldots \subset A \subset \mathbf{R}$

'minimally', where each $fI_j'/ I_{j+1}',gI_{j+1}'$, and each $I_j' \subset I_j$.

We carefully choose $I' \subset I$ of order type ω according to large cardinal combinatorics. Each resulting I_j' will have order type $\mathbf{Z}$.

Much more is true. For all j, the indeterminates appearing in I_j' have order type ω, and the degrees and integer coefficients of elements of I_j' are bounded.

It then follows that we can stick the chain

$\pm I' = I_0' \subset I_1' \subset I_2'$

back into $\mathbf{Z}$ and we are done. In fact, we get rather concrete bi-infinite sets $A \subset B \subset C \subset \mathbf{Z}$ such that $fA/B,gB$, $fA/B,gC$, $fA/C,gB$, $fA/C,gC$, $fB/C,gC$.

9. A BIG PLAN: VARYING PARAMETERS.

THE PLAN: Let T be any interesting simply stated mathematical theorem. Place T in a simple logical form, after identifying appropriate concepts. Then choose parameters in the logical form to vary, so as to create a classification problem with only finitely many instances.

The resulting classification problem is expected to be deep, interesting, and, with some frequency, doable by and only by going far beyond the usual axioms for mathematics.

Boolean relation theory is just the special case of varying the parameter: Boolean form. We look forward to varying sensible arithmetic, algebraic, geometric, and analytic parameters.

REFERENCES

[CGH] P. Cholak, M. Giusto, J. Hirst, Free Sets and Reverse Mathematics, http://www.nd.edu/~cholak/papers/vitae.html.

[Fr81] On the necessary use of abstract set theory, Advances in Mathematics 41 (1981), 209-280.

[Fr01] H. Friedman, Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

[Frxx] H. Friedman, Metamathematics of comparability, http://www.math.ohio-state.edu/~friedman/

[Fryy] H. Friedman, Selection for Borel relations, http://www.math.ohio-state.edu/~friedman/

[Frzz] H. Friedman, Boolean relation theory notes, http://www.math.ohio-state.edu/~friedman/

[Frww] H. Friedman, Lecture notes on baby Boolean relation theory, http://www.math.ohio-state.edu/~friedman/

[FS00] H. Friedman, S.G. Simpson, Issues and problems in reverse mathematics, in: Computability Theory and Its Applications, Contemporary Mathematics, volume 257, 2000, 127-144.

*This research was partially supported by NSF Grant DMS-9970459.