UNPROVABLE THEOREMS

by
Harvey M. Friedman
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/%7Efriedman/
Cal Tech Math Colloq
April 19, 2005

INTRODUCTION.

We discuss the growing list of examples of simply stated Theorems where it is known that there are no concrete proofs.

Here is our agenda.

A. In sufficiently long finite sequences from a finite set, certain blocks are subsequences of certain later blocks.
B. In sufficiently tall finite trees, certain truncations are embedded in certain taller truncations.
C. Multivariate functions on the integers have nonsurjective infinite restrictions.
D. Any two countable sets of reals are pointwise continously comparable.
E. Any permutation invariant Borel function from infinite sequences of reals into infinite sequences of reals maps some sequence into a subsequence.
F. For every symmetric Borel set in the plane, either it or its complement has a Borel selection.
G. Any Borel set in the plane that has a Borel selection on every compact set has a Borel selection.
H. For any two multivariate functions on the natural numbers of expansive linear growth there are three infinite sets which bear a certain Boolean relation with their images under the two functions. (Boolean relation theory).

1. BLOCK SUBSEQUENCE THEOREM.

The block subsequence theorem involves a single finite string in k letters. The following binary case is elementary, and a good challenge for gifted high school students.

THEOREM 1.1. There is a longest finite sequence $x_1,...,x_n$ in two letters such that no consecutive block $x_i,...,x_{2i}$ is a subsequence of a later consecutive block $x_j,...,x_{2j}$.

The longest length is 11, with 12221111111 and 21112222222 as the only examples.

THEOREM 1.2. There is a longest finite sequence $x_1,...,x_n$ in 3 letters where no consecutive block $x_i,...,x_{2i}$ is a subsequence of a later consecutive block $x_j,...,x_{2j}$.

Theorem 1.2 merely states the existence of a natural number with a specific testable property.

But the simplest known way to prove this involves not only infinite sequences but also defining infinite sequences using all infinite sequences (impredicativity). This is a weak use of the uncountable.

A logically more down to earth but more involved proof can be given for any number of letters. The most logically economical proof uses induction with an induction hypothesis that has three alternating quantifiers over the natural numbers. Two quantifiers does not suffice.

Coming back to the case of three letters, the exotic nature of all proofs is illustrated by the following lower bound on the length of the longest such finite string. In the case of two letters it is 11. In the case of three letters, it is greater than the 7198-th Ackermann function at 158,386.

The 3rd Ackermann function at 158,386 is already an exponential tower of 2's of height 158,386.

See my paper: Long finite sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

2. EMBEDDINGS OF FINITE TREES.

A tree is a finite poset with a least element (root), where the predecessors of any vertex are linearly ordered.

Note the obvious inf operation on the vertices of any finite tree.

J.B. Kruskal works with inf preserving embeddings between finite trees. I.e., h is a one-one map from vertices into vertices such that h(x inf y) = inf(h(x),h(y)). These are homeomorphic embeddings as topological spaces.

THEOREM 2.1. In any infinite sequence of finite trees, one tree is inf preserving embeddable into a later one.

J.B. Kruskal also considers finite trees whose vertices are labeled from a finite set (and more generally).

THEOREM 2.2. In any infinite sequence of finite trees with vertices labeled from a finite set, one tree is inf and label preserving embeddable into a later one.

Kruskal's, and the simpler Nash-Williams proof, are rather exotic. NW uses the "minimal bad sequence" argument, which represents a weak use of the uncountable:

Suppose there is an infinite sequence that forms a counterexample. Let T_0 be a tree of minimal size which starts such a counterexample. Let T_1 be a tree of minimal size such that T_0,T_1 starts such a counterexample. Continue in this way. This is the "minimal bad sequence".

Nash-Williams goes on to derive a contradiction from this minimal bad sequence.

We showed that, in an appropriate sense, all proofs must have this exotic nature. We also gave finite forms, and showed that all proofs of even these finite forms must have this exotic nature.

Here is one of our state of the art finite forms.

THEOREM 2.3. Let T be the full k splitting tree with labels 1,...,r which is sufficiently tall relative to k,r. There is an inf preserving label preserving terminal preserving embedding from some truncation of T into a taller truncation of T.

By a truncation of T, we mean the subtree of vertices at or below a certain height.

The growth rate associated with this finite form corresponds exactly to the necessarily exotic nature of its proof.

See my paper

Internal finite tree embeddings, in: Reflections on the Foundations of Mathematics: Essays in honor of Solomon

Feferman, ed. Wilfried Sieg, Richard Sommer, Carolyn Talcott, Lecture Notes in Logic, Association for Symbolic Logic, pp. 62-93, AK Peters, 2002.

We extended this work to the graph minor theorem (Robertson/Seymour). We show that all proofs are yet more exotic, involving arbitrary finite iterations of the minimal bad sequence argument. There are also some finite forms.

3. NONSURJECTIVE RESTRICTIONS.

The following result of ours is deeply connected with the infinite Ramsey theorem.

THIN SET THEOREM. Let $f:N^k \to N$. There exists infinite $A \subseteq N$ such that $f[A^k] \neq N$.

TST can be derived from the infinite Ramsey theorem, but it is not known if the infinite Ramsey theorem can be derived from it. However, we do know that there is no constructive proof of TST even for k = 2, and any proof must be about as exotic as he proof of the infinite Ramsey theorem.

This is the simplest example of what we call inequational Boolean relation theory. BRT will be discussed later in the talk.

See the paper

Free Sets and Reverse Mathematics, by Cholak, Guisto, Hirst, and Jockusch, to appear in Reverse Mathematics, ed. Simpson, ASL. Available at
http://www.nd.edu/~cholak/papers/vitae.html

4. CONTINUOUS COMPARISON OF COUNTABLE SETS OF REALS.

The following is in the classical folklore.

THEOREM 4.1. For any two closed sets of real numbers, one is continuously embeddable into the other.

The proof necessarily uses the Cantor-Bendixson countably transfinite decomposition of closed sets.

Theorem 4.1 follows from the following main case:

THEOREM 4.2. For any two countable closed sets of real numbers, one is continuously embeddable into the other.

This also uses the transfinite decomposition of countable closed sets.

The following is also from the classical folklore.

THEOREM 4.3. For any two countable compact metric spaces, one is continuously embeddable into the other.

By a more careful argument, we have shown the following.

THEOREM 4.4. For any two countable sets of real numbers, one is continuously embeddable into the other. For any two countable metric spaces, one is continuously embeddable into the other.

Even for countable sets of rationals, we know that, in various appropriate senses, we must use transfinite induction of arbitrary countable well ordered lengths.

See my paper

Metamathematics of comparability, to appear in Reverse Mathematics, ed. Simpson, Lecture Notes in Logic, ASL. Available at http://www.math.ohio-state.edu/%7Efriedman/

5. PERMUTATION INVARIANT BOREL FUNCTIONS.

Here is one form of Cantor's theorem.

THEOREM 5.1. For any infinite sequence of real numbers, some real number is not a coordinate of the sequence.

There is a reasonable way of getting a real number that is off the given sequence, from the point of view of descriptive set theory.

THEOREM 5.2. There is a Borel measurable function F: $\square$ such that for all x $\square$, F(x) is not a coordinate of x.

The construction of F is by diagonalization, and we expect that the value of F depends on the order in which the arguments are given.

THEOREM 5.3. Every permuta-tion invariant Borel function from into maps some infinite sequence to a coordinate.

Permutation invariance makes sense for F: . One notion is that if x,y are permutations of each other then F(x),F(y) are permutations of each other. Another is that F(π(x)) = π(F(x)) for all permutations π. The results hold under a variety of related notions.

THEOREM 5.4. Every permutation invariant Borel function from into maps some infinite sequence into an infinite subsequence.

The proofs use a Baire category argument on the highly nonseparable and exotic space , where is given the DISCRETE topology.

This is a highly nonseparable argument for a separable result. We know that there is no separable argument. The necessary use of the uncountable here is substantially stronger than what we have encountered up till now.

The necessarily exotic nature of the proof is much more dramatic when we consider Borel equivalence relations on . I.e., equivalence relations E which are Borel measurable.

THEOREM 5.5. Let F: be a Borel function that respects the Borel equivalence relation E. Then F maps some sequence to a subsequence up to E.

In order to prove this, we must not only use in a set theoretic way, but also $\wp(\ )$, $\wp\wp(\ )$, $\wp\wp\wp(\ )$, etc., and even more than this. We must use all countably transfinite iterations of the power set operation.

See my paper

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

6. BOREL SELECTION AND SYMMETRIC BOREL SETS.

Let E . We say that E is symmetric iff (x,y) E (y,x) E.

We say that f is a selection for E on iff for all x ,
(x,f(x)) E.

Here is some background regarding selection.

THEOREM 6.1. Let E be a Borel set in the plane such that every vertical cross section is nonempty. There is a Lebesgue measurable selection for E on , but maybe not be a Borel selection for E on .

The proof of 6.1 is **not** exotic. However consider the following.

THEOREM 6.2. Let E be a symmetric Borel set in the plane. Then E or \E has a Borel selection on .

The proof of 6.2. uses all countable transfinite iterations of the power operation in a demonstrably essential way. The number of iterations of the power set operation needed corresponds to the level of E in the Borel hierarchy.

We proved Theorem 6.2 using a theorem of infinite game theory due to Donald Martin, called Borel determinacy. This theorem was first proved by Martin in the mid 1960's using large cardinals going way beyond the ZFC axioms. In 1968 we proved that any proof of Borel determinacy must use all countably transfinite iterations of the power set operation.

In 1974, Martin proved Borel determinacy using exactly all countably transfinite iteration of the power set operation. This is exactly what is necessary and sufficient here.

See my paper

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

7. BOREL SELECTION IN BOREL SETS.

There is a series of joint papers by Debs and Saint Raymond concerning selection theorems (they use different terminology).

THEOREM 7.1. Let S be a Borel set in the plane and E be Borel with empty interior. If there is a continuous

selection for S on every compact subset of E, then there is a continuous selection for S on E.

A proof of Theorem 7.1 using Borel determinacy is implicit in Debs/Saint Raymond. We have shown that if we use only a transfinite iteration of the power set operation up to a single countable ordinal, then we cannot prove Theorem 7.1.

The following is also implicit in Debs/Saint Raymond.

PROPOSITION 7.2. Let S be a Borel set in the plane. If there is a Borel selection for S on every compact subset of E, then there is a Borel selection for S on .

"Proposition" indicates that Debs/Saint Raymond use an axiom that goes beyond ZFC. We have shown that Proposition 7.2 is independent of ZFC.

See my paper

Selection for Borel relations, in: Logic Colloquium '01, Lecture Notes in Logic, ed. Baaz, S. Friedman, Krajicek, ASL, p. 151-169, 2005.

8. 6561 CASES OF BOOLEAN RELATION THEORY.

We have discovered a general class of mathematical problems which makes good sense in a great variety of contexts, but which presents severe logical difficulties even in concrete contexts.

Boolean Relation Theory (BRT) concerns the Boolean relations between sets and their images under multivariate functions.

More specifically, let f be a multivariate function and A be a set. We define

$fA = \{f(x_1,...,x_k)$: k is the arity of f and $x_1,...,x_k \in A\}$. I.e., if the arity of f is k then

$$fA = f[A^k].$$

It is very convenient to suppress the arity of f and use the notation fA.

Let $f:N^k \to N$. We say that f is strictly dominating iff for all $x \in dom(f)$, $T(x) > max(x)$.

Here are two simple examples of equational Boolean relation theory.

1. For all strictly dominating f there exists infinite $A \subseteq N$ such that $N = A \dot\cup fA$. I.e., $A = N \setminus fA$. Or A,fA partitions N.

2. For all strictly dominating f,g there exists infinite $A,B,C \subseteq N$ such that $C \cap fA = C \cap gB = fA \cap gB = \emptyset$.

1 is called the Complementation Theorem and plays a special role in BRT.

We leave the proof of both statements to the audience.

2 involves two functions and three sets. Here we know of interesting concrete contexts where BRT with two functions and three sets leads to severe logical difficulties.

Let f be a multivariate function from N into N. We say that f is of expansive linear growth iff there exist $c,d > 1$ such that for all but finitely many $x \in dom(f)$,

$$c\ max(x) \le f(x) \le d\ max(x).$$

We use $X \dot\cup Y$ for $X \cup Y$ if X,Y are disjoint; undefined otherwise.

PROPOSITION 8.1. For all f,g of expansive linear growth, there exist infinite $A,B,C \subseteq N$ such that

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

We have given a proof of Proposition 8.1 using certain large cardinals that go well beyond the usual axioms of ZFC. We have also shown that ZFC alone does not suffice. In fact, we know exactly what large cardinals are required.

It is clear that Proposition 8.1 has a particularly simple structure compared to a typical statement in BRT. In fact, the two clauses in Proposition 8.1 have the form

$$X \dot\cup fY \subseteq Z \dot\cup gW$$
$$S \dot\cup fT \subseteq U \dot\cup gV$$

where X,Y,Z,W,S,T,U,V are among the three letters A,B,C. This amounts to a particular set of instances of Boolean relation theory of cardinality $3^8 = 6561$.

We have been able to show that all of these 6561 statements are provable or refutable very explicitly, with ONE exception (up to symmetry): Proposition 8.1.

Furthermore, there is a finite obstruction phenomena to the effect that if we replace "infinite" by "arbitrarily large finite" then we get the same classification.

Finite obstruction can be proved very explicitly for all cases except 8.1 (up to symmetry). For 8.1, using "arbitrarily large finite" makes 8.1 easily provable.

What if we require that f,g are concretely given – e.g., integral piecewise linear (finitely many pieces). Then 8.1 can be proved with the same large cardinals, and still require them.

NOTE: At present, we have carried this out for these two cases:

a. f,g are defined by cases using addition, multiplication, exponentiation, and round up subtraction and division, and of expansive linear growth.

b. f,g are integral piecewise linear (finitely many pieces), with nonnegative coefficients, and strictly dominating.

What if we also require that the sets A,B,C be explicitly given? For b, we can require that A,B,C be finite unions of integral piecewise linear images of infinite geometric progressions. A related requirement can be made for a. Then 8.1 again corresponds to the same large cardinals.

The large cardinals in question are the Mahlo cardinals of finite order – formulated in around 1905!

For a proof of 8.1 using these cardinals, see my paper

Equational Boolean Relation Theory, available at http://www.math.ohio-state.edu/%7Efriedman/

9. HOW ARE LARGE CARDINALS USED?

We will give a brief explanation of how they are used to prove Proposition 8.1. It is considerably easier to explain this if we assume that f,g are integral piecewise linear functions with nonnegative coefficients.

Let N* be the free Abelian semigroup on a well ordered set of generators of type α, where α is a large cardinal. We take 1 to be the first generator. N* is naturally linearly ordered. In fact, N* is naturally well ordered.

Clearly the integral piecewise linear f,g with nonnegative coefficients have canonical extensions f*,g* to N*.

The well foundedness of N* enables us to use a transfinite form of the Complementation theorem. In particular, we can construct a unique set $W \subseteq N^*$ such that $N^* = W \cup g^*W$.

With some care, we then build a tower $A \subseteq B \subseteq C \subseteq W$, such that

$$A \cap f^*A \subseteq C \cap g^*B$$
$$A \cap f^*B \subseteq C \cap g^*C.$$

This lives in the transfinite, and so may not be embeddable back into N. However, using the combinatorics of large cardinals, we can arrange not only that C is of order type α, but the set of all generators used to represent elements of C has order type α, and also that the representation of elements of C have lengths bounded by a fixed integer. Then we know that we can embed C back into $N \times Z$, completing the proof of 8.1 - in the case of strictly dominating integral piecewise linear functions with nonnegative coefficients.