UNPROVABLE THEOREMS IN DISCRETE MATHEMATICS

Harvey M. Friedman
Department of Mathematics
Ohio State University
friedman@math.ohio-state.edu
www.math.ohio-state.edu/~friedman/
April 26, 1999

An unprovable theorem is a mathematical result that can-not be proved using the com-monly accepted axioms for mathematics (Zermelo-Frankel plus the axiom of choice), but can be proved by using the higher infinities known as large cardinals. Large car-dinal axioms have been the main proposal for new axioms originating with Gödel.

Gödel's famous incompleteness theorems from the 1930's demonstrate the possibility of unprovable theorems in dis-crete and finite mathematics.

Known examples in discrete and finite mathematics have been hopelessly unsatisfactory from the point of view of a mathe-matician. (Disguised statments about formal set theories; Diophantine equations too long to write down in base 10 in 1000 years, ad hoc concoctions, etc.).

This is not to be confused with various important undecidability results concerning the impossibility of giving algorithms for solving an infinite family of problems.

E.g., the algorithmic undecid-ability of the class of Diophantine equations with a solution over the integers.

(Incidentally, this is open over the rationals).

Here we are talking about specific individual assertions of substantive mathematical content, in discrete or finite mathematics, which can only be proved by going well beyond the usual axioms for mathematics.

Before getting into discrete and finite mathematics, I want to discuss some of the original examples from the 1980’s where large infinite sets are used in fairly concrete mathe-matics - at least fairly concrete for an analyst. The startling point is that these uses of large infinities are demonstrably necessary - we know that they simply cannot be removed.

Cantor's famous diagonaliza-tion theorem can be stated as follows. For any $\mathbf{x} \in I$ there exists $y \in I$ which not a term in $\mathbf{x}$. We call such a y a diag-onalizer for $\mathbf{x}$. We want to investigate how a diagonalizer for $\mathbf{x}$ can be obtained from $\mathbf{x}$.

First of all, it is easy to see that a diagonalizer cannot be obtained continuously, where we give I the usual infinite product topology (which is also separable).

The Borel measurable subsets of a topological space form the least σ algebra containing the open sets. The Borel meas-urable functions from one space into another are the functions under which inverse images of open sets are Borel measurable.

It is well known that we can obtain diagonalizers by a Borel measurable function. I.e., there is a Borel measurable function F such that for all $\mathbf{x} \in I$, $F(\mathbf{x})$ is a diagonalizer for $\mathbf{x}$.

In such a construction, the y chosen may depend not only on the terms in $\mathbf{x}$ but the order in which they appear in $\mathbf{x}$.

So it is natural to ask: can diagonalizers be chosen Borel measurably and dependent only on the set of terms?

The answer is no (Borel diagonalization theorem).

THEOREM 1. Let $F:I \to I$ be Borel measurable. Assume that for all $\mathbf{x},\mathbf{y} \in I$, if x and y have the same terms (are perm-utations of each other; are finite permutations of each other) then $F(\mathbf{x}) = F(\mathbf{y})$. Then there exists x such that $F(\mathbf{x})$ is a term in $\mathbf{x}$.

The following elegant variant is one of very many, and assumes the general flavor of a fixed point theorem:

THEOREM 2. Let $F:I \to I$ be Borel measurable. Suppose for all $\mathbf{x},\mathbf{y} \in I$, if $\mathbf{x}$ and $\mathbf{y}$ are subsequences of each other then $F(\mathbf{x})$ and $F(\mathbf{y})$ are subsequences of each other. Then there exists $\mathbf{x}$ such that $F(\mathbf{x})$ is a subsequence of $\mathbf{x}$.

Theorem 1 is proved by a basic application of the Baire cate-gory theorem for the space $\mathbf{I}$, where this time I is given the DISCRETE topology $\mathbf{I}$. Any Borel measurable $F:I \to I$ will be a

Borel measurable F:**I** → I. By using an appropriate 0-1 law, we see that F must be constant off of a meager set in the **I** topology. The conclusion follows immediately.

The Borel diagonalization theorem lives squarely in the realm of discrete mathematics, and so one would not expect to be using the normally useless discrete topology on I. Yet the significant point is that one can suitably formalize "separable mathematics" or "inherently countable mathematics" and show that all three forms of the Borel diagonalization theorem cannot be proved there. The proof of Theorem 2 is trickier, but with the same underlying idea.

We mention two additional Borel diagonalization theorems that share the same logical features - i.e., necessary use of nonseparable mathematics.

Let K be the Cantor space {0,1} with the usual compact topology. Let s:K → K be the shift map, where s(x) is obtained from x by chopping off the first term of x. For x ∈ K let $x^{(2)} = (x_1,x_4,x_9,x_{16}...)$.

THEOREM 3. Let F:K → K be Borel measurable. Assume that for all x ∈ K, F(sx) = F(x). Then there exists x such that $F(x) = x^{(2)}$.

Let T be the usual circle group.

THEOREM 4. There is a continuous f:T → T which agrees somewhere with: every Borel measurable F:T → T that satisfies F(2x) = F(x).

EMERGING GENERAL THEME: For certain interesting classes of functions X and Y, some element of X agrees somewhere with every element of Y.

Not yet systematically explored.

I now want to mention a Borel theorem whose proof necessarily employs much larger sets. We say that S ⊆ IxI is symmetric if and only if (x,y) ∈ S ↔ (y,x) ∈ S.

THEOREM 5. Every symmetric Borel measurable subset of the unit square (or KxK) contains or is disjoint from the graph of a Borel measurable (or con-tinuous) function.

The proof (which relies heavily on work of D.A. Martin on infinite games) necessary uses uncountably many uncountable cardinalities! However monstrous such cardinalities are, they are still well within ZFC.

But now we come to a Borel theorem that can only be proved by using infinities going way beyond ZFC.

UNPROVABLE THEOREM 6. Let F be a Borel measurable function from the space of sequences of finitely generated groups into finitely generated groups which is isomorphically invariant. Then F maps all of the infinite subsequences of some argument into a value that is embeddable into a term of that argument. We now turn to discrete and finite mathematics.

The connections with large infinities are more delicate and have taken longer to develop.

The next Theorem captures the essence of recursion on N.

Let N be the set of nonnegative integers. $F:N^k \to N$ is strictly dominating iff for all $x_1,...,x_k \in N$, $F(x_1,...,x_n) > x_1,...,x_n$. For $A \subseteq N$, we write $F[A]$ for the forward image of F on A^k.

THEOREM 7. Let $k \geq 1$ and $F:N^k \to N$ be strictly dominating. There exists $A \subseteq N$ such that $A = N\backslash F[A]$ (or equivalently, $F[A] = N\backslash A$). Furthermore A is unique and A is infinite.

We construct A by induction. Suppose we have determined membership in A for all $i \in [0,n)$. We place n in A if and only if n is not the value of F at integers already placed in A. By the strict dominance of F, these placements remain correct later on.

Obviously there is no leeway in how we can construct A, so that A is unique. And clearly A must be infinite since if A were finite, both A and F[A] would be finite, contradicting that their union is all of N.

Write $A \Delta B$ for $A\backslash B \cup B\backslash A$. We can restate Theorem 7 (without uniqueness) as follows:

THEOREM 7′. Let $k \geq 1$ and $F:N^k \to N$ be strictly dominating. There exists an infinite $A \subseteq N$ such that $N \Delta A \Delta F[A]$.

We now present an elaboration of Theorem 7'. We write A+A for $\{x+y: x,y \in A\}$.

THEOREM 7''. Let $k,n \geq 1$ and $F:N^k \to N$ be strictly dominating. There exists infinite sets $A_1 \subseteq ... \subseteq A_n \subseteq N$ such that for all $1 \leq i < n$, $A_i+A_i \subseteq A_{i+1} \subseteq F[A_{i+1}]$.

Theorem 7'' is a completely trivial weakening of Theorem 7'; just set all of the A's to be the A from Theorem 7'. However, take a look at this:

UNPROVABLE THEOREM 8. Let $k,n \geq 1$ and $F:N^k \to N$ be strictly dominating. There exists infinite sets $A_1 \subseteq ... \subseteq A_n \subseteq N$ such that for all $1 \leq i < n$, $A_i+A_i \subseteq (A_{i+1} \cap F[A_{i+1}])\backslash A_1$.

We have shown that 8 can only be proved by using axioms going well beyond the usual axioms of mathematics (ZFC). These axioms are called large cardinal axioms, and in this case they are what are called "Mahlo cardinals of finite order."

These cardinals are far larger than strongly inaccessible cardinals - which correspond to Grothendieck's "universes," which Grothendieck and other algebraists sometimes postulate for convenience. But in down to earth algebraic settings, it is well known that they are a luxury that can be easily dispensed. with. In contrast, here we show the demonstrable unremovability of such monsters - in fact monsters that are far more imposing than even Grothendieck's "universes" or strongly inaccessible cardinals.

Of course, 8 is rather spec-ialized, and needs to be placed in a thematic context. We have been proposing a theory of solvability of Boolean equations. The idea is to embed 8 into a general class of problems; in particular, to view it as simply one instance of solvability of a general kind of Boolean equation.

To describe this promising approach, let us return to Theorem 7'.
THEOREM 7'. Let $k \geq 1$ and $F:N^k \to N$ be strictly dominating. There exists an infinite $A \subseteq N$ such that $N \subseteq A \subseteq F[A]$.

We can view this as follows:

GIVEN: Let R(A,B) be a formal Boolean relation between two subsets A,B of N.

DECIDE: For all $k \geq 1$ and strictly dominating $F:N^k \to N$, there exists an infinite $A \subseteq N$ such that $R(A,F[A])$.

The point is that $N \subseteq A \subseteq B$ counts as a formal Boolean relation between $A,B \subseteq N$. Specifically, a Boolean rela-tion is taken as the assertion that some combination of union, intersection, and complementation is N.

All Boolean relations can be written as a finite list of one or more of these basic Boolean relations:
i) inclusions of the form $\alpha \subseteq \beta$, where α is an intersection of one or more variables, and β is the union of one or more variables;
ii) the union of one or more variables = N;
iii) the intersection of one or more variables = $\emptyset$.

We can give a complete anlysis of which R - in list form - makes the statement true.

In an appropriate sense, all true problem instances follow formally from Theorem 7′. And if we were to use all F, and not just the strictly dominat-ing F, then all true problem instances would be formally trivial.

GIVEN: Let $n \geq 1$ and $R(A_1,...,A_{2n})$ be a formal Boolean relation between subsets of N.
DECIDE: For all $k \geq 1$ and strictly dominating $F:N^k \to N$, there exists infinite $A_1 \subseteq ... \subseteq A_n \subseteq N$ such that $R(A_1,...,A_n,F[A_1],...,F[A_n])$.

We again give a complete analysis of which R in list form makes this statement true.

And again, in an appropriate sense, all true problem in-stances follow formally from Theorem 7′. Again, if we were to use all F, then all true problem instances would be formally trivial.

GIVEN: Let $n \geq 1$ and $R(A_1,...,A_{3n})$ be a formal Boolean relation between subsets of N.
DECIDE: For all $k \geq 1$ and strictly dominating $F:N^k \to N$, there exists infinite $A_1 \subseteq ... \subseteq A_n \subseteq N$ where $R(A_1,..,A_n,F[A_1]$ $,...,F[A_n],A_1+A_1,...,A_n+A_n)$.

We conjecture that there is an exponential time algorithm which, with the help of Mahlo cardinals of finite order, provably solves this problem.

We already know that there is no algorithm which, without the help of such cardinals, provably solves this problem.

We make the following finite obstruction conjecture. This conjecture asserts that any R that makes the following finite problem true also makes the previous infinite problem true.

GIVEN: Let $n \geq 1$ and $R(A_1,...,A_{3n})$ be a formal Boolean relation between subsets of N.
DECIDE: For all $k,r \geq 1$ and strictly dominating $F:N^k \to N$, there exists $A_1 \subseteq ... \subseteq A_n \subseteq N$, each with at least r elements, such that $R(A_1,..,A_n, F[A_1],...,F[A_n],A_1+A_1,..,A_n+A_n)$.

Specifically, we conjecture that the finite obstruction conjecture can be proved with the help of Mahlo cardinals of finite order, but not without. We already know that the finite obstruction conjecture cannot be proved without the help of Mahlo cardinals of finite order. But can it be proved with their help?

We now turn to the "greedy" construction of finite graphs. The term "greedy" is from the theory of algorithms, where so many constructions proceed so that at each stage, some aspect is optimized among all possible choices.

A digraph G is a pair (V,E), where V = V(G) is a finite set and $E = E(G) \subseteq VxV$. V is the set of vertices and E is the set of edges. (No multiple edges allowed).

If (x,y) is an edge, then we say that y is a target of x.

We say that G' is a point extension of G if and only if

i)$V(G')\backslash V(G) = \{x\}$ for some x;
ii) the edges in G are exactly the edges in G' that connect vertices in G;
iii) in G', x is not a target of any vertex.

Thus in G', all of the new edges point from the new vertex x to a vertex in G.

We write G'/G for the new part of G' over G, whose vertices V are x together with the tar-gets of x, and whose edges are those edges in G' that connect these vertices.

A digraph construction se-quence (dgc) is a finite or infinite sequence of digraphs $G_1,G_2,...$ such that each G_{i+1} is a point extension of G_i.

For any set X let DG(X) be the set of digraphs all of whose vertices lie in X. We consider "weight" functions $w:DG(X) \to N$.

We seek to minimize weights of new parts. A w-minimal dgc is a dgc $G_1,G_2,...$ from DG(X) where each G_{i+1} is such that for no point extension G_{i+1}' of G_i ***with the same vertices as G_{i+1},*** is $w(G_{i+1}'/G_i) < w(G_{i+1}/G_i)$.

The following is obvious:

THEOREM 9. Let $G \in DG(X)$ and $v_1,v_2,...$ be a sequence of distinct elements of $X\backslash V(G)$ of length $0 \leq n \leq$. Let $w:DG(X) \to N$. There exists a w-minimal dgc of length 1+n starting with G, where the new vertices are $v_1,v_2,...$.

We need to consider some structural properties of digraphs.

Let $[N]^k$, $k \geq 1$, be the set of all k element subsets of N. Let $G \in DG([N]^k)$. We say that x is a summit in G if and only if $x \in V(G)$ and every vertex y that x points to in G has $max(y) \leq max(x)$.

Let $x,y \in [N]^k$. We say that x is entirely lower than y if and only if every element of x is < every element of y.

THEOREM 10. Let $k,p \geq 1$ and $w:DG([N]^k) \to N$ have finite range. There exists a w-minimal dgc of finite length, starting with any element of $DG([N]^k)$, such that in the final digraph, all k element subsets of some p element set appear as summits with the same number of targets.

We prove Theorem 10 with the help of infinitely many uncountable cardinals. We conjecture that these are required. Now, look at this:

UNPROVABLE THEOREM 11. Let $k,p \geq 1$ and $w:DG([N]^k) \to N$ have finite range. There exists a finite w-minimal dgc of finite length, starting with any ele-ment of $DG([N]^k)$, such that in

the final graph, all k element subsets of some p element set appear as summits with the same entirely lower targets.

It is necessary and sufficient to use subtle cardinals of finite order to prove 11. These cardinals are somewhat bigger than the ones we have been talking about earlier.

There is a more abstract way to state the conclusion of 11.

UNPROVABLE THEOREM 11'. Let $k,p \geq 1$ and $w:DG([N]^k) \to N$ have finite range. There exists a w-minimal dgc of finite length, starting with any element of $DG([N]^k)$, such that in the final digraph, there are p summits of any collective order type with the same entirely lower targets.

In fact, this requires the same large cardinals even if p is set to 2.

Finally, we discuss the issue of removing all mention of infinite objects from these unprovable theorems. This corresponds to going from discrete mathematics to finite mathematics.

For 11 (or 11') this is simply a matter of introducing finite parameters in the most straightforward way:

UNPROVABLE THEOREM 12. Let $n >> k,p,r \geq 1$ and $w:DG([1,n]^k) \to [r]$. There exists a w-minimal dgc of finite length, starting with any element of $DG([1,n]^k)$, such that in the final digraph, all k element subsets of some p element set are summits with the same entirely lower targets.

Here the w-minimal dgc are defined as before except that all terms must lie in $dom(w) = DG([1,n]^k)$. By a compactness or Konig tree argument, 12 is equivalent to 11.

An appropriate elimination of infinite objects in 8 is more delicate. Recall 8:

UNPROVABLE THEOREM 8. Let $k,n \geq 1$ and $F:N^k \to N$ be strictly dminating. There exists infin-ite sets $A_1 \supseteq ... \supseteq A_n \subseteq N$ such that for all $1 \leq i < n$, $A_i+A_i \subseteq (A_{i+1} \cup F[A_{i+1}])\backslash A_1$.

The approach we take is to strengthen the inclusion relation. Thus for $A,B \subseteq N$, we write $A \subseteq_d B$ if and only if $A \subseteq B$ and for all $n \geq 0$, $|B \cap [1,n]| \leq |A \cap [1,n]|^d$.

UNPROVABLE THEOREM 8'. Let $t >> k,n,r \geq 1$ and $F:[1,t]^k \to N$ be strictly dminating. There exists finite sets $A_1 \subseteq_{k\hat{}2} ... \subseteq_{k\hat{}2} A_n$

□ N, with at least r elements, such that for all $1 \leq i < n$, $A_i + A_i \subseteq (A_{i+1} \cup F[A_{i+1}]) \setminus A_1$.

We can show that it is necessary and sufficient to use subtle cardinals of finite order in order to prove 8'.

We can even go further and bound t as a function of k,n,r in terms of iterated exponentiation. The resulting asser-tion is purely universal and provably equivalent to 8'.