

**WHAT YOU CANNOT PROVE 1: before 2000**

by

Harvey M. Friedman

Department of Mathematics

Ohio State University

December 19, 2005

<http://www.math.ohio-state.edu/%7Efriedman/>

Most of my intellectual efforts have focused around a single general question in the foundations of mathematics (f.o.m.). I became keenly aware of this question as a student at MIT around 40 years ago, and readily adopted it as the principal driving force behind my research.

1. General question, general conjectures.
2. The most abstract: general set theoretic statements.
3. The second most abstract: limited set theoretic statements.
4. The third most abstract: the projective hierarchy of sets of reals.
5. The fourth most abstract: Borel sets of reals.
6. The fifth most abstract: infinite sets of integers.
7. The sixth most abstract: finite combinatorics, with unbounded existence.
8. The most concrete: completely finite combinatorics.

**1. GENERAL QUESTION, GENERAL CONJECTURES.**

The currently standard formalization of mathematics came into general acceptance before 1930, and is known as ZFC = Zermelo Frankel set theory with the axiom of choice.

Enter the 1930s, the era of Kurt Gödel. Among his most astounding results are his two incompleteness theorems. They are very general, and assert the following when applied to ZFC.

G1. There exist sentences in the language of set theory which cannot be proved or refuted in ZFC (assuming that ZFC does not prove that ZFC is inconsistent).

G2. The consistency of ZFC is a sentence in the language of set theory, which cannot be proved in ZFC (assuming that ZFC is consistent). In fact, ZFC does not prove  $\text{Con}(\text{ZFC})$  if and only if ZFC is consistent.

Note that G2 immediately implies G1.

Both of these results are proved finitistically, without resorting to any kind of infinitary or set theoretic methods.

Barkley Rosser improved G1 to

GR. There exist sentences in the language of set theory which cannot be proved or refuted in ZFC (assuming that ZFC is consistent). In fact, these exist if and only if ZFC is consistent.

G1 is proved by the diagonalization method. GR is proved by a trickier form of the diagonalization method. G2 is proved by first applying the diagonalization method to obtain a sentence A not provable in ZFC (assuming ZFC is consistent). This is followed by a careful verification of a miraculous fact - A is equivalent to  $\text{Con}(\text{ZFC})$  - where this equivalence is provable in ZFC. Hence  $\text{Con}(\text{ZFC})$  is not provable in ZFC (provided ZFC is consistent).

Note that  $\text{Con}(\text{ZFC})$  is a statement concerning formal systems of set theory, which is of the utmost importance for f.o.m., but rather remote from normal mathematical activity. So we are lead to the general question, which has been an obsession of mine for over 40 years:

Q1. What kinds of mathematical questions cannot be settled in ZFC? I.e., neither proved nor refuted in ZFC. I.e., independent of ZFC.

After G1 and G2, Gödel tackled the most well known question in set theory prominently left open by Cantor - the continuum hypothesis, CH. This asserts that every set of real numbers is mappable onto the set of all real numbers, or embeddable into the set of all integers.

G3. CH is not refutable in ZFC (assuming ZFC is consistent).

The method used by Gödel to establish G3 is completely different than the methods he used to establish G1,G2. For G3, Gödel invented the method of inner models. He showed that every model of ZFC can be cut back to a model of ZFC + CH. This yields G3 via the completeness theorem for first order predicate calculus with equality - also due to Gödel! It is also possible to avoid the use of his completeness

theorem (as he does). The entire proof of G3 is given in a tiny fragment of ZFC.

Cohen provided the other half.

GC. CH is independent of ZFC (assuming ZFC is consistent).

For Cohen's half, he invented a third technique for showing independence from ZFC, called forcing. In particular, Cohen showed that every countable model of ZFC can be expanded to a model of not CH. This yields GC via the completeness theorem. The completeness theorem can be avoided (as Cohen does). The entire proof of GC is given in a tiny fragment of ZFC.

We now have three methods for proving independence from ZFC - two due to Gödel, and one due to Cohen. The last two of these methods was invented to show the independence of CH from ZFC.

There is a fourth method that has proved fruitful for showing independence from ZFC, which I use intensively. This will be described in Lecture 2.

Thus independence from ZFC touches fundamental problems in set theory. Subsequent work following Cohen showed that among the large backlog of open set theoretic problems, a considerable percentage are independent of ZFC.

Over the years, mathematicians have generally reacted by steering clear of difficult set theoretic questions, preferring to either ignore them or reduce their level of generality if set theoretic difficulties arise.

Set theoretic difficulties are generally perceived to be so remote from and sharply different than normal mathematical difficulties (topological, geometric, analytic, combinatorial, etcetera), that they should be separated.

In particular, the steering clear of set theoretic difficulties is generally regarded as an effective defensive move by the mathematical community with little or no real cost to mathematics.

Mathematicians will generally embrace the singular generality of set theoretically formulated results when the set theory involved is readily manageable. E.g., every

field has an algebraic closure. But if there were set theoretic difficulties in proving this for arbitrary fields, mathematicians would rather quickly focus on, say, countable fields. They would regard that extra generality as definitely not worth the cost.

But what about questions that are not overtly set theoretic? We make the following conjecture.

C1. Every mathematical question that is not heavily set theoretic, which has been raised in a published paper appearing in a refereed journal before today, the paper having been assigned an AMS classification number not in logic or set theory, can be settled in ZFC.

The closest exception that we know of to C1 lies in the realm of Borel measurable functions on the real line. This exception is almost explicit in the joint writings of the Paris analysts Debs and Saint Raymond. We will discuss these results in Lecture 2, as the proof of independence came after 2000.

Some decades ago, Borel measurable functions - particularly those at finite levels - were not considered to be set theoretic at all, and lied at the heart of real analysis.

However, times have changed, and the focus of mathematical activity has become more and more concrete. Normal mathematical activity has become even more focused on the finite, the discrete, and the well behaved continuous (or almost continuous), in contexts where continuous objects are readily approximable by finite objects.

The last part of Lecture 2 will focus on (nearly) the most concrete kind of finite statements involving infinitely many objects considered by mathematicians. This very recent work suggests the following conjecture:

C2. There is no inherent limitation to the construction of "natural" or "beautiful" mathematical statements that can be shown to be independent of ZFC (assuming ZFC does not prove its own inconsistency), except the obvious one: the statement must involve infinitely many objects.

In fact, we make the following extremely strong conjecture.

C3. There is a core finite combinatorial structure that emerges in a natural and uniform way in any nontrivial mathematical context, which cannot be handled within ZFC. Specifically, there is a natural, beautiful, and uniform way to seek more refined information in any nontrivial mathematical development involving infinitely many objects, where the resulting statements can be proved only by adding additional axioms to ZFC believed by set theorists to be consistent. This is because this core finite combinatorial structure is easily hidden in even the modest complexity inherent in any nontrivial mathematical development involving infinitely many objects.

In these two lectures, we will not only present statements independent of ZFC, but also statements independent of substantial fragments of ZFC. However, we will not discuss statements independent of only finite set theory (or Peano arithmetic), except in passing - finite set theory (or PA) does not represent substantial set theoretic methods. This will exclude any substantive discussion of historically important work by Goodstein, Paris/Harrington, myself, and others.

## **2. THE MOST ABSTRACT: GENERAL SET THEORETIC STATEMENTS.**

We begin with general set theoretic statements. These involve sets of unlimited cardinality. The oldest example is implicit in Cantor. Here is a particularly attractive form.

GST1. There exists an uncountable set  $A$  such that 1)  $A$  is not the union of fewer than  $A$  sets that are smaller than  $A$ ; 2) the power set of any set smaller than  $A$  is also smaller than  $A$ .

Note that this property holds for sets of cardinality  $0, \aleph_1$ , and for no finite cardinality  $\geq 1$ . Such an uncountable set must be awesomely enormous, as some simple investigations reveal.

In modern set theoretic terminology, GST1 is equivalent to the assertion "there exists a strongly inaccessible cardinal". GST1 asserts that the cardinality of  $A$  is a strongly inaccessible cardinal.

It is known that "there exists a strongly inaccessible cardinal" is not provable in ZFC, provided ZFC is

consistent. It is strongly believed that it is not refutable in ZFC, although it is known that the nonrefutability cannot be established by merely knowing that ZFC is consistent, or that ZFC does not prove that ZFC is inconsistent, etcetera.

There are much stronger well known statements of this general kind - i.e., the existence of a set with a basic set theoretic property that depends only on its cardinality:

GST2. There exists a nonempty set  $A$  such that there is a countably additive measure on all subsets of  $A$  that takes on only the values 0 and 1, where points have measure 0, and  $A$  has measure 1.

GST2 is one of many equivalent formulations of "there exists a measurable cardinal". This property obviously fails for nonempty countable sets  $A$ . Basic work in the 1940s shows that the least cardinality  $\aleph_1$  of such a set  $A$  is a strongly inaccessible cardinal, and also that there are lots of strongly inaccessible cardinals below  $\aleph_1$ . Thus GST2 not only implies GST1, but is much stronger from many points of view.

The set theory community expresses great confidence in the consistency of ZFC, and equally great confidence in the consistency of ZFC + "there exists a strongly inaccessible cardinal". However, with ZFC + "there exists a measurable cardinal", confidence abounds, but it is subdued.

A natural hierarchy of statements such as GST1 and GST2 has emerged from the set theory community, and it is called the hierarchy of large cardinal hypotheses. The weakest natural large cardinal hypotheses that have emerged are at the level of GST1. GST2 is generally viewed as a medium large cardinal hypothesis, with many interesting levels strictly between GST1 and GST2. As we move up from GST2, we move into the region of large large cardinal hypotheses, where confidence in consistency is visibly restrained.

**Who cares?** What good are such amorphous abstract monstrosities postulated by the likes of GST1 and GST2?

Stay tuned to Lecture 2, which concentrates on the relevance of something like GST1.1 in surprisingly concrete contexts.

### 3. THE SECOND MOST ABSTRACT: LIMITED SET THEORETIC STATEMENTS.

In limited set theoretic statements, the cardinality of the objects under consideration are bounded at the outset, or can be demonstrated to be bounded.

The most well known of such highly set theoretic statements is the continuum hypothesis (CH), which states:

CH. Every set of real numbers is either mappable onto the set of all real numbers, or embeddable into the set of all integers.

As mentioned before, Godel and Cohen proved the independence of CH from ZFC (assuming ZFC is consistent).

The heavily set theoretic nature of CH is readily identifiable by the use of arbitrary sets of real numbers, and arbitrary functions on the real numbers. These sets and functions are **NOT** required to be presentable in the forms that are so common in ordinary mathematical activity.

Specifically, the sets and functions in CH are not required to be presented sequentially.

Borel measurable functions are required to be presented sequentially - for finite level Borel measurable functions, the sequential presentations are particularly explicit.

The Borel sets in complete separable metric spaces form the least family of subsets containing the open sets, and closed under taking countable unions, countable intersections, and complements.

The Borel functions between two complete separable metric spaces can be defined in two equivalent ways. One is that the inverse image of every open set is Borel. The other is that they form the least family of functions containing the continuous functions, and closed under pointwise limits of sequences of functions.

These definitions naturally give rise to hierarchies of length  $\aleph_1$ . But they can be cut off at  $\aleph_1$ , resulting in the finitely Borel sets and functions. Generally speaking,

phenomena appearing at some level already appear at levels at most 2 or 3.

What happens if we Borelize CH?

CHB. Every Borel set of real numbers is either Borel mappable onto the set of all real numbers, or Borel embeddable into the set of all integers.

CHB is provable in a tiny fragment of ZFC.

There is a rather substantial literature on a variety of set theoretic statements involving arbitrary sets and functions on the real line (or in complete separable metric spaces). A great many of these statements have been shown to be independent of ZFC (generally, but not always, assuming only that ZFC is consistent). These results use the forcing method of Cohen in elaborate ways.

Here is a typical such result (although atypically brilliant!), going back to the 1970s, due to Richard Laver.

A set of reals  $S$  is said to be strongly measure zero if and only if for any sequence  $\epsilon_1, \epsilon_2, \dots$  of positive reals, there exists a sequence  $I_1, I_2, \dots$  of intervals covering  $S$ , where each  $I_n$  has length less than  $\epsilon_n$ .

Borel's Conjecture (1919). Strongly measure zero is equivalent to countable.

This is the same Emile Borel as in "Borel sets and Borel functions".

*Borel's Conjecture is independent of ZFC. It implies the negation of CH, but is not implied by the negation of CH. These results use only the consistency of ZFC.*

Again, we can Borelize this statement.

*"Every Borel set of real numbers that is strongly measure zero is countable" is provable using a tiny fragment of ZFC.*

Not all important limited set theoretic statements live in subsets of complete separable metric spaces.



Let  $\wp$  be the power set operation. From the set theoretic point of view, the real line and complete separable metric spaces amount to taking  $\wp^\omega$ , where  $\omega$  is the set of all set theoretic natural numbers (the first limit ordinal in the sense of von Neumann).

Sets of real numbers live in  $\wp^\omega$ , and we can form  $\wp^\omega \wp^\omega \dots \wp^\omega$ , any finite number of times. This is incredibly gargantuan from the point of view of ordinary mathematical activity.

However, this is nothing compared to what is available in ZFC, and thus we regard this as limited set theory.

In particular, in ZFC, we have the axiom of replacement, and so we can form the entire sequence

$$\omega, \wp\omega, \wp\wp\omega, \wp\wp\wp\omega, \wp\wp\wp\wp\omega, \dots$$

and therefore the union of this sequence. Then we continue. We can continue this way throughout all of the von Neumann ordinals.

Of particular interest at the level of  $\wp\wp\wp\omega$ , or  $\wp^\omega$ , is the existence of a probability measure on the unit interval:

PMI. There is a countably additive measure on all subsets of  $[0,1]$ , where points have measure 0 and  $[0,1]$  has measure 1.

Even though PMI is a limited set theoretic statement, in some ways it behaves like an unlimited set theoretic statement, because of this result of Solovay from the 1960s:

ZFC + PMI is consistent if and only if ZFC + "there exists a measurable cardinal" is consistent (Solovay). However, these two hypotheses do not imply each other.

#### **4. THE THIRD MOST ABSTRACT: THE PROJECTIVE HIERARCHY OF SETS OF REALS.**

The projective hierarchy of sets of reals starts off at the bottom with the Borel subsets of  $\mathbb{R}^n$ ,  $n \geq 1$ .

At the next level of the projective hierarchy, we have the so called A and CA sets. The A sets (analytic sets) are the projections

$$\{(x_1, \dots, x_n) : (\exists y \in \mathbb{R}) ((x_1, \dots, x_n, y) \in S)\}$$

where  $S$  is a Borel subset of  $\mathbb{R}^{n+1}$ .

The CA sets (coanalytic sets) are the complements of analytic sets.

It is classical that

Borel is properly included in A (or CA).  
 $A \cap CA = \text{Borel}$ .

Analytic sets are much more abstract than Borel sets, in the following sense. In order to determine membership/nonmembership of the real number  $x$  in a Borel set, only countably many questions have to be answered regarding  $x$ , each question calling for a comparison of  $x$  with a given rational number. This takes the form of a countably branching decision tree.

On the other hand, in order to determine membership of  $x$  in an analytic set, countably many questions have to be answered regarding  $x$  to establish membership. However, no countably many questions are generally sufficient to establish nonmembership. Furthermore, there is no way to know in advance the schedule of questions even to establish membership (i.e., there is no appropriate countably branching decision tree).

Then comes PCA and CPCA sets. These are projections of CA and sets, and complements of PCA sets.

This process is normally continued through all finite levels. The sets of reals that appear somewhere are called the projective sets of reals. It is classical that the hierarchy does not collapse.

A handful of basic questions naturally arise concerning properties of projective sets. Generally speaking, such properties are provable about Borel sets, but cannot be proved at the PCA and CPCA levels and higher; sometimes they can be proved at the A and CA levels.

i. Do uncountable sets have perfect subsets? This is provable for Borel sets, and even analytic using a tiny fragment of ZFC. But "every uncountable coanalytic set has a perfect subset" is independent of ZFC. Also "every uncountable projective set has a perfect subset" is independent of ZFC.

ii. Are the sets Lebesgue measurable? Trivial for Borel sets, and provable for analytic and coanalytic sets using a tiny fragment of ZFC. But "every PCA set is Lebesgue measurable" is independent of ZFC. Also "every projective set is Lebesgue measurable" is independent of ZFC.

iii. Are the new projections at each level equally complicated? E.g., "any two analytic sets that are not Borel are in one-one correspondence via a Borel bijection of the reals". This is independent of ZFC. There is an obvious analog higher up in the projective hierarchy.

There is an interesting aspect to this phenomena. There are two rival extensions of ZFC that settle all such questions about the projective hierarchy - but in opposite ways!

The first axiom is the so called Gödel axiom of constructibility - which Gödel may have subscribed to at one point, but sharply repudiated later in print. (For the later Gödel, there is right and a wrong for set theoretic sentences, no matter how unlimited).

This axiom, written  $V = L$ , settles not only all such questions about the projective hierarchy (negatively), but also CH (positively), PMI (negatively), and all related questions about sets of limited size. In addition, we know that  $V = L$  is independent just from the consistency of ZFC. However,  $V = L$  does not settle the existence of a strongly inaccessible cardinal and related questions, although it does settle the existence of a measurable cardinal (negatively).

The second axiom is a natural strengthening of the existence of measurable cardinals. It is called "the existence of Woodin cardinals". Measurable cardinals will suffice for questions about  $A$ ,  $CA$ , and  $PCA$  (sometimes  $CPCA$ ), but not higher. The questions about the projective hierarchy are settled positively. However CH, PMI, and related questions about sets of limited size remain independent. It does settle the existence of a strongly

inaccessible cardinal and, in fact, the existence of a measurable cardinal (positively), but there is also a hierarchy of yet stronger principles of a related kind, in unlimited set theory, that remain independent.

In contrast to  $V = L$ , the consistency of the existence of Woodin cardinals must be taken on faith - just as is the case with the existence of measurable cardinals.

The set theorists usually are adamant about rejecting  $V = L$  in favor of the existence of Woodin cardinals, and regard the seemingly "complete" treatment of the projective hierarchy given by  $V = L$  as FALSE - whereas the opposite seemingly "complete" treatment of the projective hierarchy given by Woodin cardinals as TRUE. It is the main vindication put forth by contemporary set theorists of the study of large cardinals.

My own view is that the projective hierarchy is so far removed from normal mathematics, that even if we accept the previous paragraph in the sense intended by the set theorists, this development does not come close to satisfactorily establishing the importance or relevance of large cardinals to mathematics.

We want demonstrably necessary uses of large cardinals in concrete mathematical contexts - the more concrete the better.

## **5. THE FOURTH MOST ABSTRACT: BOREL SETS OF REALS.**

We have already discussed Borel sets and functions on the reals (and complete separable metric spaces), and contrasted them with the higher levels of the projective hierarchy.

The most striking independence result from ZFC in the realm of Borel sets was obtained after 2000, and will be discussed in Lecture 2. It grew out of work of the Paris analysts Debs and Saint Raymond.

The independence results before 2000, in the realm of Borel sets, were most convincing at important levels significantly below ZFC. We discuss some of these now.

The lowest level that we consider in this section is countable set theory. This amounts to simply eliminating

the power set axiom from ZFC. We can, optionally, also add "every set is countable" to ZFC\P. We can also view ZFC\P as "separable mathematics".

In ZFC\P, we cannot construct  $\mathbb{R}$  or  $\mathbb{P}$  as a set. However, we can speak of elements of  $\mathbb{R}$  and elements of  $\mathbb{P}$ . We can develop a complete treatment of the Borel sets and functions on the reals (and complete separable metric spaces) well within ZFC\P.

We begin with one form of Cantor's theorem that the reals are uncountable.

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 (Borel theory).

THEOREM 5.2. There is a Borel function  $F: \mathbb{R}^{\mathbb{N}} \rightarrow \mathbb{R}$  such that for all  $x \in \mathbb{R}^{\mathbb{N}}$ ,  $F(x)$  is not a coordinate of  $x$ .

The construction of  $F$  is by diagonalization. We would expect that  $F(x)$  depends on the order of the arguments of  $x$ .

THEOREM 5.3. Every permutation invariant Borel function from  $\mathbb{R}^{\mathbb{N}}$  into  $\mathbb{R}$  maps some infinite sequence to a coordinate.

Permutation invariance makes sense for  $F: \mathbb{R}^{\mathbb{N}} \rightarrow \mathbb{R}$ . 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  $F(\pi(x)) = \pi(F(x))$  for all permutations  $\pi$  of  $\mathbb{N}$ . The following result holds under a variety of related notions.

THEOREM 5.4. Every permutation invariant Borel function from  $\mathbb{R}^{\mathbb{N}}$  into  $\mathbb{R}$  maps some infinite sequence into an infinite subsequence.

We proved Theorems 5.3 and 5.4 by going just beyond ZFC\P, and showed that they were not provable in ZFC\P. Certainly, the use of  $\mathbb{P}$  is more than sufficient to prove Theorems 5.3 and 5.4.

We now give an example at a much higher level. Recall that in ZFC, we can iterate  $\mathbb{P}$  infinitely often, starting at  $\mathbb{N}$ ,

and then take the limit. We can continue transfinitely, obtaining what is called the cumulative hierarchy of sets.

The level we are going to represent is by iterating the power set through all countable ordinals, just shy of putting them all together.

Let  $E \subseteq \mathbb{R}^2$ . We say that  $E$  is symmetric iff  $(x,y) \in E \iff (y,x) \in E$ . We say that  $f$  is a selection for  $E$  on  $\mathbb{R}$  iff for all  $x \in \mathbb{R}$ ,  $(x,f(x)) \in E$ .

Here is an old classical result. It is proved in a tiny fragment of ZFC.

**THEOREM 5.5.** 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  $\mathbb{R}$ . However, there may not be a Borel selection for  $E$  on  $\mathbb{R}$ .

Now consider this.

**THEOREM 5.6.** Let  $E$  be a symmetric Borel set in the plane. Then  $E$  or its complement has a Borel selection on  $\mathbb{R}$ .

Theorem 5.6 can be proved using all countably transfinite iterations of the power set operation, but not without.

The proof of Theorem 5.6 relies heavily on earlier work of D.A. Martin in infinite game theory (Borel determinacy).

We will return to the Borel realm in Lecture 2 with some post 2000 work concerning Borel selection that is independent of ZFC.

## **6. THE FIFTH MOST ABSTRACT: INFINITE SETS OF INTEGERS.**

The most striking independence results from ZFC in the realm of infinite sets of integers appear in the substantially developed post 2000 work on "Boolean Relation Theory", the title of my forthcoming research monograph.

Here we will discuss some pre 2000 highlights that represent rather modest levels of independence - at least by the standards of this talk.

It is an accepted part of ZFC to allow sets of natural numbers to be formed based on quantifying over all sets of natural numbers - including the one being formed.

This is well known to be akin to the least upper bound principle for the real line, as opposed to the convergence of Cauchy sequences, or the existence of convergent subsequences of bounded infinite sequences.

Poincare and Weyl railed against the use of such a principle on the general grounds of circularity. Recall that in 1902, Russell had obtained his famous paradox via a set formation principle that bears at least some resemblance to this.

Current conventional wisdom is that the "circularity" Poincare and Weyl disavowed is not vicious like the one Russell identified, and it sits well within a tiny fragment of ZFC.

We showed that a number of basic results require this principle, including two that are celebrated existing theorems in infinitary combinatorics.

The first is due to J.B. Kruskal. A tree is a finite poset with a least element called the root, where the predecessors of every vertex are linearly ordered.

There is an obvious inf operation on the vertices of any finite tree.

Kruskal works with inf preserving embeddings between finite trees. I.e.,  $h$  is a one-one map from vertices into vertices such that  $h(x \text{ inf } y) = \text{inf}(h(x), h(y))$ .

Note that these  $h$  are homeomorphic embeddings as topological spaces.

Kruskal's Tree Theorem. In any infinite sequence of finite trees, one tree is inf preserving embeddable into a later tree.

The second example is a theorem of Robertson and Seymour called the graph minor theorem.

Let  $G, H$  be graphs (undirected, with loops and multiple edges allowed). We say that  $G$  is minor included in  $H$  if and

only if  $G$  can be obtained (up to isomorphism) from  $H$  by applying the following operations zero or more times in  $H$ : contracting edges to a point, removing edges, and removing vertices.

Graph Minor Theorem. In any infinite sequence of finite simple graphs, one graph is minor included in a later graph.

We showed that in an appropriate sense, the use of the principle in question must be applied arbitrarily many finite times, in order to prove the graph minor theorem. Just one application is sufficient for the Kruskal tree theorem.

## 7. THE SIXTH MOST ABSTRACT: FINITE COMBINATORICS, WITH UNBOUNDED EXISTENCE.

In finite combinatorics, all data is entirely finite. Most commonly, we assert that any given finite object of a certain kind has a specific property, where that property may or may not be algorithmically checkable.

The most well known illustrative examples come from number theory.

$\square^0_1$ . A specific Diophantine equation, or family of Diophantine equations, has no integral (rational) solution. The Riemann hypothesis. Goldbach's conjecture.

$\square^0_2$ . All Diophantine equations of a certain form have at least one (infinitely many) integral (rational) solution. The twin prime conjecture.  $e + \square$  is irrational (transcendental).

$\square^0_2$ . A specific Diophantine equation has at most finitely many solutions.  $e + \square$  is rational (algebraic).

$\square^0_3$ . All Diophantine equations of a certain form have at most finitely many solutions (Faltings). Certain algebraic numbers can be approximated by rationals in certain ways with finitely many exceptions (Roth).

Normally mathematics strives to be  $\square^0_1$ . Thus when a  $\square^0_2$  theorem is proved, people want to provide an upper bound for the existential quantifier (in terms of the outermost universal quantifier), thereby putting the theorem into  $\square^0_1$



form. When a  $\Sigma^0_2$  theorem is proved, people want to provide an example of the existential quantifier in front, again rendering it in  $\Sigma^0_1$  form. Similarly, when a  $\Sigma^0_3$  theorem is proved, people want to provide an upper bound for the existential quantifier (in terms of the outermost universal quantifier), which still renders it in  $\Sigma^0_1$  form.

Thus in finite combinatorics, we have the classical finite Ramsey theorem.

FINITE RAMSEY THEOREM. Let  $n$  be sufficiently large relative to  $k, r, m \geq 1$ . Any coloring of the unordered  $k$  tuples from an  $n$  element set, with at most  $m$  colors, has an  $r$  element monochromatic set. I.e., an  $r$  element set all of whose unordered  $k$  tuples have the same color.

Obviously FRT as stated is  $\Sigma^0_2$ . Ramsey himself gave upper bounds on  $n$  as a function of  $k, r, m$ . They are iterated exponential, with the stack of size roughly  $k$ . This converts FRT to form  $\Sigma^0_1$ . Ramsey also gave lower bounds of the same character.

Of course, the finite Ramsey theorem is way below our radar screen in terms of independence.

Up to very recently, all of the remotely mathematically natural sentences about finite objects that have been shown to be independent of even relatively weak systems such as finite set theory, are  $\Sigma^0_2$  or  $\Sigma^0_3$ . One actually sees that the independence is tied up with the enormous size of any realization of the existential quantifier. In such cases, it is known that one cannot exhibit a bound in the usual sense, rendering them in  $\Sigma^0_1$  form.

At our threshold level of independence, the examples are our various finite forms of Kruskal's tree theorem and the graph minor theorem.

Kruskal's tree theorem was proved by Kruskal in more general form using labeled vertices. In particular, we can use vertices labeled from a finite set.

FINITE KRUSKAL TREE THEOREM (one of many). Let  $T$  be the full  $k$  splitting tree with labels  $1, \dots, r$  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  $T$ .

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

The above theorem also requires the construction of sets of natural numbers by means of quantification over all sets of natural numbers - the principle that Poincare and Weyl objected to.

The growth rate associated with this finite form corresponds exactly to its level of independence.

### **8. THE MOST CONCRETE: COMPLETELY FINITE COMBINATORICS.**

Completely finite combinatorics is required to be in  $\square_1^0$  form.

By far the most significant independence results are very recent, and will be presented in Lecture 2.