University of Pennsylvania
Department of Mathematics
Hans Rademacher Lectures
September 17 - 20, 2002
4:30 p.m., T-Th Sep 17-19
4:00 p.m., F Sep 20

All lectures in room A-6 of the David Rittenhouse Laboratory, first floor,
33-rd and Walnut Streets, Philadelphia.

DEMONSTRABLY NECESSARY USES OF ABSTRACTION

Harvey M. Friedman
University Professor
Ohio State University

RADEMACHER SERIES ABSTRACT.

There are many familiar theorems whose proofs use methods which are in some appropriate sense substantially more "abstract" than its statement. Some particularly well known examples come from the use of complex variables in number theory. Sometimes such abstraction can be removed - for example by the "elementary proof of the prime number theorem" - and sometimes no appropriate removal is known. The interest in removing abstraction typically varies, with no agreed upon criteria for appropriateness. E.g., the removal might sacrifice naturalness or intelligibility, or the result of the removal criticized as being merely a thinly disguised form of the original.

These Rademacher lectures focus on cases of demonstrable unremovability of abstraction, primarily (but not solely) in the context of discrete mathematics. These cases rely on a sharp, fully formalized, criteria for removal, where a proof of unremovability has been found. The issue of "natural" removal is finessed, as there is no removal, natural or otherwise.

More specifically, in each case we begin with a theorem whose known proofs use methods that are unexpectedly abstract relative to its statement. Next, we delineate flexible and comprehensive methods of lower abstraction. Then we present the result that the original theorem cannot be proved using only these methods of lower abstraction.

LECTURE 1. DEMONSTRABLY NECESSARY USES OF ABSTRACTION.

In the first lecture, we introduce all of the examples of demonstrable unremovability of abstraction under discussion. No formalisms will be presented. The identification of methods and their levels of abstraction will be given only at the informal mathematical level, without the use of axiomatic systems. The examples include

1. Minimization in norm of integral polynomials.
2. Termination of lexicographic descent in the natural numbers.
3. Hilbert basis theorem.
4. Degrees of algebraic approximations to sets.
5. Comparison of blocks within finite sequences of natural numbers.
6. Comparison in sequences of finite trees, and within large finite trees.
7. Graph minors in sequences of finite graphs.
8. Continuous comparison of countable sets of reals.
9. Borel diagonalization for infinite sequences of reals.
10. Borel selection/antiselection in symmetric Borel sets.
11. Borel selection in Borel sets.
12. 6561 cases of Boolean relation theory.

The climax of the series is item 12, where the demonstrably necessary level of abstraction is so immense that it is goes well beyond the usual accepted axioms for mathematics. This is despite the fact that the context is that of functions on the natural numbers.

LECTURE 2. POLYNOMIALS, TERMINATION, HILBERT BASES, DEGREES.

We will present an in depth discussion of the demonstrably necessary uses of abstract methods in the minimization in norm of integral polynomials, in the termination of lexicographic descent in the natural numbers, in the Hilbert basis theorem, and in the degrees of algebraic approximations to sets.

LECTURE 3. COMPARISON OF BLOCKS, TREES, GRAPHS, COUNTABLE POINTSETS.

We will present an in depth discussion of the demonstrably necessary uses of abstract methods in the comparison of blocks within finite sequences of natural numbers, in the comparison of terms in sequences of finite trees, in the comparison of subtrees within large finite trees, in graph minors within sequences of finite graphs, and in the continuous comparison of countable sets of reals.

LECTURE 4. BOREL DIAGONALIZATION, BOREL SELECTION, BOOLEAN RELATION THEORY.

We will present an in depth discussion of the demonstrably necessary uses of abstract methods in Borel diagonalization for infinite sequences of reals, in Borel selection/antiselection in symmetric Borel sets of reals, in Borel selection in Borel sets of reals, and finally in 6561 cases of Boolean relation theory. In this last case, the demonstrably necessary level of abstraction is so immense that it is goes well beyond the usual accepted axioms for mathematics. This is despite the fact that the context is that of functions on the natural numbers.

HANS RADEMACHER LECTURES
Philadelphia, Pennsylvania

LECTURE 1
DEMONSTRABLY NECESSARY USES OF ABSTRACTION

Harvey M. Friedman
The Ohio State University
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/
September 17, 2002

In order to prove a Theorem, we sometimes use ideas and constructions that are, in some sense, out of character with the statement of the Theorem. This is a perfectly normal situation. It is one of those things that makes mathematics so intriguing.

We are all familiar with cases where substantial machinery of an exotic nature seems to be needed to prove a comparatively mundane assertion: there are no positive integers x,y,z,n such that $x^{n+2} + y^{n+2} = z^{n+2}$.

But can we give examples where we can ***prove*** that all proofs of a given Theorem are comparatively exotic?

Before we can prove such a result, we need to be able to state it mathematically. Normally, finding an appropriate formulation is highly nontrivial. I will begin with a familiar example where this turns out to be utterly straightforward.

Imagine that you are working in an ancient mathematical context where numerical quantities can be added, subtracted, multiplied, divided, and compared in size. Then one day you encounter

$$x^2 = 2.$$

Or, in more rudimentary terms,

$$x \bullet x = 1+1.$$

The problem of the existence of a solution baffles everyone.

Then some clever person comes up with the following startling idea:

If an expression without division takes on both negative and positive values, then it takes on zero.

This intermediate value principle for polynomials is beyond the mathematics of the time, which consists of manipulations of equalities and inequalities. Eventually it becomes an accepted way of thinking about "numerical quantities", through a combination of introspection and utility.

Of course, the actual history is much more subtle than this. But in this case it is particularly easy to give a satisfactory formulation of the phenomena in question.

The ancient mathematical context is formalized by the usual ordered field axioms. The result is that

in some ordered fields, $x^2 = 2$ has no solution.

The additional principle used to prove existence has more than one formalization. An "expression" could mean a polynomial with or without variable coefficients.

The first interpretation suffices to prove the existence of a square root of 2.

However it does not give the existence of a square root of every nonnegative number. E.g., there is an ordered field containing all algebraic real numbers, and □, but without any square root of □.

The second interpretation yields the full ordered real closed field axioms.

Of course this is all very familiar, and in particular, no mathematical logic is needed to give a satisfactory formulation for a number of such situations, including many that arise from Euclidean geometry.

Nevertheless, we want to give a mathematical logic formulation, even if it is less informative than the preceding algebraic formulation.

1. Write down the ordered field axioms, not as algebraic conditions, but as a formal system in first order predicate calculus. Argue by example that this captures a significant kind of mathematical proof.

2. Show that $(\exists x)(x^2 = 2)$ cannot be proved in this formal system. This follows from the stronger result that there is an ordered field in which 2 has no square root.

3. Write down the above intermediate value principle and add it to the formal system. Show that $(\exists x)(x^2 = 2)$ can now be proved in this extended system.

In less elementary mathematical contexts, the mathematical logic viewpoint is typically required in order to have a chance of a successful formulation. At least as far as we know now.

In these lectures, we will adhere to the above plan 1-3.

1. Minimization in norm of integral polynomials.

THEOREM 1.1. Every polynomial of several variables with integer coefficients achieves a value of least magnitude over the integers.

This clearly follows from the least number principle; i.e., any property that holds of a nonnegative integer holds of a least nonnegative integer.

One can see by example that most theorems living in the integers have constructive proofs.

From experience we see that constructivity is a significant, interesting, and natural condition on proofs.

There are some well known theorems in the integers (or algebraics) where no constructive proofs are known, and there is great interest in finding constructive proofs.

E.g., Roth’s theorem on approximability, and Falting’s proof of Mordell’s conjecture.

A well known development in mathematical logic provides powerful formalizations of constructive reasoning that corresponds well to informal ideas.

There is an array of results demonstrating that any theorem proved constructively must have certain algorithmic properties.

In the case of Theorem 1.1, if it is to be proved constructively, then it must have the following algorithmic property:

There must be an algorithm that produces a value of least magnitude over the integers of any given integral polynomial. However, by using the solution to Hilbert’s 10th problem (no algorithm for deciding the existence of solutions to Diophantine equations over the integers), there is no such algorithm.

THEOREM 1.2. Theorem 1.1 is not constructively provable.

It would be nice to have a supply of deeper theorems in the integers which we know cannot be proved constructively.

So far, we could be content with avoiding mathematical logic (proof theory), and think solely in terms of algorithms. However, there is another aspect of Theorem 1.1, which we take up in the second lecture, regarding the nature of the inductive argument that is involved. Mathematical logic is used for the formulation in an apparently essential way.

2. Termination of lexicographic descent in the natural numbers.

The lex ordering on N^k is the dictionary ordering.

THEOREM 2.1. Every sequence from N^k that is decreasing in the lex ordering terminates.

In the case k = 1, it is obvious that the sequence must stop, and the number of steps is at most the first term.

Things get interesting with $k = 2$. Here one argues by existential numerical induction. We will give a sense in which this is required.

For fixed k, we can also argue by existential numerical induction, but we repeating the argument roughly k times.

The full Theorem 2.1 is also proved by induction, but cannot be proved by existential numerical induction. It can be proved by universal/existential numerical induction.

The same results hold for the following sharper theorem. For x,y □ N^k, write x □$_c$ y iff for all i, x_i □ y_i.

THEOREM 2.2. Every infinite sequence from N^k has a finite initial segment such that every term is $\geq_c$ some term in that finite initial segment.

Here it is more difficult to be economical about axioms used in the proofs, but this has been done.

In lecture 2 we will discuss how to obtain finite versions with quantitative information.

3. Hilbert basis theorem.

For the purpose of logical analysis, one good formulation the Hilbert basis theorem is as follows.

THEOREM 3.1. Let $P_1,P_2,...$ be an infinite sequence of polynomials from the polynomial ring in k variables over a (countable) field. □ n such that all P's are ideal generated by $P_1,P_2,...,P_n$.

In an appropriate sense, HBT is equivalent to Theorem 2.2. The idea of the connection can be seen by the following simple construction.

For each x □ N^k let $\#(x)$ be the monomial in k variables, where the exponent of the i-th variable is the i-th coordinate of x. Let $x_1,x_2,...$ □ N^k, and consider the monomials $\#(x_1),\#(x_2),...$. By HBT, let every $\#(x_i)$ be ideal generated by $\#(x_1),...,\#(x_n)$. Then obviously every x_i is $\geq$ at least one of $x_1,...,x_n$.

We will discuss finite versions of the Hilbert basis theorem and associated quantitative information. The quantitative information is “exotic”.

We also consider sequences of algebraic sets and obtain the same results.

4. Degrees of algebraic approximations to sets.

The logically exotic nature of HBT and its finite forms generally does not spill over to results in commutative algebra/algebraic geometry.

Often using HBT is easiest, but hard work will avoid HBT and lead to decent estimates. E.g., the decomposition of algebraic sets into irreducible components. My impression is that there are some important situations where removal of HBT has not yet been achieved.

We have found a structural result which is proved using HBT, but where the quantitative information is exotic, as in the finite versions of HBT.

Let F be a field and $k \geq 1$. Let S □ $F[x_1,\ldots,x_k]$. The n-th algebraic approximation to S is the least superset of S of presentation degree □ n.

For any set S □ $F[x_1,\ldots,x_k]$, we look at the series of algebraic approximations $S[0] \supseteq S[1] \supseteq \ldots$. By HBT, this terminates. Of course, for algebraic S, this trivially terminates with S itself.

We say that S □ $F[x_1,\ldots,x_k]$ is rich iff $S[0] \supseteq\neq S]1] \ldots \supseteq\neq S[n] = S$, for some $n \geq 0$.

THEOREM 4.1. For each $k \geq 1$ and field F, there is a bound to the presentation degrees of the rich S □ $F[x_1,\ldots,x_k]$. In fact, there is a bound h(k) that depends only on k and not on F.

We have shown that the best possible bounds are exotic.

5. Comparison of blocks within finite sequences of natural numbers.

The block subsequence theorem involves a single finite string in k letters. The binary case is elementary. This challenge is given to gifted high school students in Paul Sally's program. At least one student solved it.

THEOREM 5.1. There is a longest finite string $x_1,\ldots,x_n$ in two letters such that no consecutive block $x_i,\ldots,x_{2i}$ is a subsequence of a later consecutive block $x_j,\ldots,x_{2j}$.

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

THEOREM 5.2. There is a longest finite string $x_1,\ldots,x_n$ in three letters such that no consecutive block $x_i,\ldots,x_{2i}$ is a subsequence of a later consecutive block $x_j,\ldots,x_{2j}$.

Theorem 5.2 merely states the existence of a natural number with a specific "testable" property. Nevertheless, the simplest way to prove this appears to involve not only infinite sequences but also defining infinite sequences by reference to all infinite sequences (impredicativity). In this context, such impredicativity can be avoided with considerable difficulty. However, there still has to be something exotic about the proof. The longest length is also exotic. The exotic nature of all proofs and the exotic nature of the longest length are closely related.

THEOREM 5.3. There is a longest finite string $x_1,\ldots,x_n$ in any given finite alphabet such that no consecutive block $x_i,\ldots,x_{2i}$ is a subsequence of a later consecutive block $x_j,\ldots,x_{2j}$.

As expected, the proof of Theorem 5.3 and the associated quantitative information is yet more exotic. This is explained in the third lecture.

6. Comparison in sequences of finite trees, and within large finite trees.

We use the partial ordering definition of finite trees.

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

Note that there is an obvious inf operation on the vertices of any finite tree.

J.B. Kruskal works with inf preserving embeddings between finite trees.

THEOREM 6.1. In any infinite sequence of finite trees, one tree is inf preserving embeddable into a later one.

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

THEOREM 6.2. 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 proof of Theorem 6.1 as well as the simplest known proof due to Nash-Williams, are exotic. NW introduced the impredicative “minimal bad sequence” argument. We showed that the construction of infinite sequences by reference to all in-finite sequences is unavoidable (impredicativity).

We gave a series of finite forms of Kruskal’s theorem.

The finite forms and associated quantitative information are also shown to be exotic.

These finite forms involve looking at long finite sequences of finite trees. As was the case with HBT, we got interested in structural information about a single sufficiently large finite tree.

THEOREM 6.3. In any sufficiently tall full tree labeled from a finite set, one truncation can be inf, label, and terminal preserving embeddable into a higher truncation.

We prove that this finite form and its associated quantitative information is as exotic as the finite forms involving finite sequences.

7. Graph minors in sequences of finite graphs.

Finite graphs are pairs (V,E), where for each element of E, we assign a set of vertices of cardinality 1 or 2 (incidence).

G is minor included in H iff G can be obtained from H by successively deleting a single edge, contracting a single edge, or removing an isolated vertex.

Minor inclusion is normally taken up to isomorphism.

Here is the graph minor theorem of Robertson/Seymour.

THEOREM 7.1. In any infinite sequence of finite graphs, one graph is minor included in a later graph.

At a critical place, the proof of Theorem 7.1 uses an iterated form of the infinite bad sequence argument. A single uniterated use of the infinite bad sequence argument is used to prove Kruskal's tree theorem. However, such iterations are known to be more powerful as the length of the iteration increases.

Before the graph minor theorem was proved, we proved a strengthening of Kruskal's theorem called the extended Kruskal theorem using a finitely iterated minimal bad sequence argument. We had also proved that, in an appropriate sense, these iterations are unavoidable.

We asked Robertson/Seymour to explicitly derive my EKT from their GMT.

Robertson/Seymour succeeded in doing this. Therefore the GMT is at least as exotic as the EKT.

We gave finite forms of EKT with associated numerical information.

Some of these were converted to finite forms of GMT, also with associated numerical information. The exotic nature of EKT and GMT is retained.

8. Continuous comparison of countable sets of reals.

The following is in the classical folklore.

THEOREM 8.1. For any two closed sets of real numbers, one is continuously embeddable into the other.

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

Theorem 8.1 can be made to follow from the following main case:

THEOREM 8.2. For any two countable closed sets of real numbers, one is continuously embeddable into the other.

The following is also from the classical folklore.

THEOREM 8.3. 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 8.4. 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.

Here is the most rudimentary form of this result.

THEOREM 8.5. For any two sets of rational numbers, one is continuously embeddable into the other.

All of these results must, in an appropriate sense, use arguments involving arbitrary countable ordinals.

We will take this up later, including a way of saying "must" using descriptive set theory rather than mathematical logic.

9. Borel diagonalization for infinite sequences of reals.

Here is one form of Cantor's theorem.

THEOREM 9.1. 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 sequence, from the point of view of descriptive set theory.

THEOREM 9.2. There is a Borel measurable function F:¬• □ ¬ such that for all x □ ¬•, F(x) is not a coordinate of x.

The construction of F is by diagonalization, and there is every reason to believe that the value of F depends on the order in which the arguments are given.

THEOREM 9.3. There is no Borel measurable function F:¬• □ ¬ obeying rng(x) = rng(y) □ F(x) = F(y), such that for all x □ ¬•, F(x) is not a coordinate of x.

Or put positively,

THEOREM 9.4. Let F:¬$^\bullet$ □ ¬ be Borel measurable, where for all x,y □ ¬$^\bullet$, rng(x) = rng(y) □ F(x) = F(y). There exists x □ ¬$^\bullet$ such that F(x) is a coordinate of x.

The proof uses a Baire category argument on the highly nonseparable space ¬$^\bullet$, where ¬ is given the discrete topology. In fact, we discuss a family of such results in lecture 4, including results to the effect that the nonseparable arguments cannot be replaced by separable arguments.

The necessary use of machinery becomes much more dramatic when we consider Borel equivalence relations on ¬. I.e., equivalence relations E □ ¬ □ ¬ on ¬ which are Borel measurable.

THEOREM 9.5. Let E be a Borel equivalence relation on ¬. Let F:¬$^\bullet$ □ ¬ be Borel, where if x,y □ ¬$^\bullet$ have E-equivalent coordinates then F(x),F(y) are E-equivalent. Then there exists x □ ¬$^\bullet$ such that F(x) is E-equivalent to a coordinate of x.

In order to prove Theorem 9.5, we must not only use ¬, but also S(¬), SS(¬), SSS(¬), SSSS(¬), and even more than this. We must use all countably transfinite iterations of the power set operation.

10. Borel selection/antiselection in symmetric Borel sets.

Necessary uses of countably transfinite iterations of the power set operation are rather dramatic, and we have been interested in trying to relate this to standard situations in classical analysis. We have been able to do this in the context of Borel selection.

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 ¬ if and only if for all x □ ¬, (x,f(x)) □ E.

Here is some background regarding selection.

THEOREM 10.1. There is a Borel set E □ ¬ □ ¬ such that i) for all x □ ¬ there exists y □ ¬ such that (x,y) □ E; ii) there is no Borel selection for E on ¬. However, if i) holds then there is a Lebesque measurable selection for E on ¬ (for Borel E).

THEOREM 10.2. Let E ¬ ¬ be a symmetric Borel set. Then E or ¬\E has a Borel selection on ¬.

The proof of Theorem 10.2 uses all countable transfinite iterations of the power set operation in a demonstrably essential way.

The number of iterations needed corresponds to the level of E in the Borel hierarchy.

We proved Theorem 10.2 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 usual ZFC axioms. In 1968 we proved that every proof of Borel determinacy must use all countably transfinite iterations of the power set operation. In 1974, Martin proved Borel determinacy using exactly all such.

In 1981 we also proved that Theorem 10.2 requires use of all countably transfinite iterations of the power set operation.

11. Borel selection in Borel sets.

We recently became acquainted with a series of joint papers of two functional analysts Debs and Saint Raymond of U. Paris concerning selection theorems (they use different terminology).

We need a more general notion of selection. Let S be a set of ordered pairs, A a set. f is a selection for S on A iff dom(f) = A and (x A) (x,f(x)) S.

THEOREM 11.1. Let S ¬ ¬ be Borel 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 11.1 using BD 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 11.1.

The following result is also implicit in Debs/Saint Raymond.

PROPOSITION 11.2. Let S □ ¬ x ¬ and E □ ¬ 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.

We say “Proposition” instead of “Theorem” because Debs/Saint Raymond use an axiom that goes beyond ZFC to prove this. What they use is still fairly innocent as far as extensions of ZFC go. This will be discussed in the fourth lecture.

We have shown that Proposition 11.2 cannot be proved in ZFC.

12. 6561 cases of Boolean relation theory.

We have discovered a general class of mathematical problems which make good sense in a great variety of contexts, but which present 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

$$fA = \{f(x_1,...,x_k): k \text{ is the arity of } f \text{ and } x_1,...,x_k \text{ □ } A\}.$$

We find it very convenient to suppress the arity of f and use the notation fA.

Let f be a multivariate function from N into N. We say that f is strictly dominating if and only if

$$\text{for all } x \text{ □ } \mathrm{dom}(f),\ f(x) > \max(x).$$

Here are two simple examples of Boolean relation theory.

1. For all strictly dominating f there exists infinite A □ N such that fA = N\A.

2. For all strictly dominating f,g there exists infinite A,B,C □ N such that C □ fA = C □ gB = fA □ gB = ∅.

Statement 1 is called the Complementation Theorem and plays a special role in BRT. We leave the proof of both statements to the audience.

The first example involves only one function and one set. We have called this “baby BRT”. We do not know of any interesting concrete contexts where BRT with one function and one set leads to severe logical difficulties.

The second example 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 if and only if there exist c,d > 1 such that for all but finitely many $x \in \mathrm{dom}(f)$,

$$c|x| \leq f(x) \leq d|x|$$

where |x| is the maximum coordinate of the tuple x.

We use $X \cup. Y$ for $X \cup Y$ together with the commitment that X,Y are disjoint. E.g.,

$$X \cup. Y \subseteq Z \cup. W$$

means

$$X \cup Y \subseteq Z \cup W \wedge X \cap Y = \emptyset \wedge Z \cap W = \emptyset.$$

PROPOSITION 12.1. For all f,g of expansive linear growth, there exist infinite $A,B,C \subseteq N$ such that

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

We have given a proof of Proposition 12.1 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, a little less potent large cardinals than are used in the proof do not suffice.

It is clear that Proposition 12.1 has a particularly simple structure compared to a typical statement in Boolean relation theory.

In fact, the two clauses in Proposition 12.1 have the form

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

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 using the same large cardinal axioms that we use to prove Proposition 12.1. Obviously, we need the large cardinal axioms since 12.1 is among the 6561.

Furthermore, the logical difficulties associated with Proposition 12.1 are not dependent on the wildness of arbitrary multivariate functions from N into N or arbitrary infinite subsets of N. The logical difficulties remain even if we restrict the functions and sets to concrete countable families. These matters will be discussed in the fourth lecture.

We think that BRT is mathematically interesting enough that mathematicians will want to develop it, despite the necessary rethinking of the foundations for mathematics. This remains to be seen.

LECTURE 2
POLYNOMIALS, TERMINATION, HILBERT BASES, DEGREES

Harvey M. Friedman
The Ohio State University
http://www.math.ohio-state.edu/~friedman/
September 18, 2002

In the remaining three lectures, we discuss the 12 topics from the first lecture in order.

The unavoidably exotic nature of the proof methods become successively clearer and stronger from lecture 2 to lecture 4. In this lecture, the exotic nature is at times quite subtle, involving the nature of induction statements and constructivity. However, you should find the associated numerical information more dramatic.

1. Minimization in norm of integral polynomials.

THEOREM 1.1. Every polynomial of several variables with integer coefficients achieves a value of least magnitude over the integers.

This is an obvious consequence of the least number principle - any property that holds of a nonnegative integer holds of a least nonnegative integer.

The nonconstructive nature of the obvious proof is apparent: let n be any value. If it is not least, then pass to a lower value. Keep going on at most n times till you get to the least value. But you can't tell when you have arrived at the least value, or how to get to a lower value.

There is a purely algorithmic way of looking at the nonconstructivity. The logical form of the statement is

(□n)(□m)(□r)(A(n,m,r,s)).

Here n,m,r range over nonnegative integers. The n codes the given polynomial of several variables. The m,r code vector arguments.

A(n,m,r,s) asserts that for the P coded by n, $|P(r')| \geq |P(m')|$, where r codes the vector r' and m codes the vector m'. This is typical of how coding is used to sort out logical issues.

According to any reasonable idea of constructivity, if a statement of the form □□□ or even □□□... is provable constructively, then there must be an algorithm which produces an instance of the first existential quantifier given an instance of the first universal quantifier.

In our case, this is just a computable f:N □ N such that

(□n)(□r)(A(n,f(n),r)).

I.e. an algorithm which, when presented with an integral polynomial P, produces an argument where P achieves a value of least magnitude.

It is a bit more convenient to use the following consequence of this. Namely, an algorithm which, when presented with an integral polynomial P, produces a value of P of least magnitude.

Hilbert’s 10th problem asks for an algorithm that decides whether an integral polynomial has a zero over the integers. This was answered negatively by Matiyasevich, J. Robinson, Davis, Putnam.

Suppose there is an algorithm which, when presented with an integral polynomial P, produces a value of P of least magnitude over **Z**. Then we get an algorithm which, when presented with an integral polynomial P, decides whether P has a zero, since P has a zero over **Z** iff any value of P over **Z** of least magnitude is 0. Thus there is no such algorithm.

This establishes the nonconstructivity of Theorem 1.1 from the algorithmic point of view. However, there is a well understood proof theoretic approach to constructivity. We will give some details in the case of formal arithmetic.

The system PA (Peano Arithmetic) may be familiar, but perhaps not HA (Heyting Arithmetic). HA is the constructive form of PA.

In all systems of logic discussed here, we use connectives □,□, ,□ ,□ , quantifiers □,□, variables, and =. The usual axioms and rules of logic are understood. In the case of PA, we use 0,S,+,•,=. The axioms are:

1. □S(x) = 0, S(x) = S(y) □ x = y.
2. x+0 = 0, x+(S(y)) = S(x+y).
3. x•0 = 0, x•(S(y)) = x•y + x.
4. (□[x/0] □ (□x)(□ □ □[x/S(x)])) □ □, where □ is any formula in the language.

PA is a very strong system, and it is believed that all core mathematical theorems to date that are appropriately expressed in finite terms can be proved in PA. We discuss some exceptions involving trees, graphs in lecture 3 (are they in the "core"?).

HA is the same as PA except that we use the axioms and rules of constructive (intuitionistic) logic. This amounts to dropping the law of excluded middle, or, equivalently, dropping the rule that allows the deduction of A from a contradiction from □A. Fortunately, constructive logic is rather robust and unmistakable.

There are some very pleasing well known facts about PA vs. HA.

1. Every □ statement provable in PA is provable in HA.
2. Every □□ statement provable in PA is provable in HA.
3. If (□x)(□y)(□(x,y)) is provable in HA then there is a recursive f:N □ N such that (□x)(□(x,f(x)).
4. If (□x)(□y)(□(x,y)) is provable in HA then there is an algorithm f such that (□x) (□(x,f(x)) is provable in HA.

We say that a formula is in class $n \geq 0$ if and only if it starts with □ n quantifiers and is followed by a formula with bounded quantifiers only.

For each $n \geq 0$, write PA_n for PA where the induction scheme is for class n formulas.

With some effort, PA_n is equivalent to:

i) using □□... of length n in the induction scheme;
ii) using □□... of length n in the induction scheme;
iii) using either of the above in the least number principle scheme instead of the induction scheme.

It is now clear that Theorem 1.1 is provable in PA_1.

PA_0 is too weak for many purposes. PA_0 is more robust if we introduce exponentiation into the language. Thus we add axiom

3.5. $x^0 = S(0)$, $x^{S(y)} = x^y \bullet x$.

This does not change PA_n, $n \geq 1$, or what we said in i) - iii). To avoid confusion, we write EFA (exponential function arithmetic) for PA_0 using exponentiation.

THEOREM 1.2. Theorem 1.1 is provable in PA_1 but not in EFA and not in HA. In fact, EFA proves that Theorem 1.1 is equivalent to PA_1.

CONJECTURE. All celebrated number theory to date is provable in EFA, even constructively.

It is at least believed that the existing proofs of all celebrated number theory need only minor modification to conform to PA.

But no proof of Falting's theorem (Mordell's conjecture) within HA is known. That would yield effective bounds. No proof of Roth's theorem on rational approximations in HA is known either, because that would yield effective bounds. No proof of Roth's theorem in EFA is known since there is a crucial induction whose induction statement has an unbounded quantifier.

2. Termination of lexicographic descent in the natural numbers.

For $k \geq 1$, $x,y \in N^k$, write $x <_{lex} y$ iff at the first coordinate at which x,y differ, x is less than y.

THEOREM 2.1. Every sequence from N^k that is decreasing in the lex ordering terminates.

We discuss what is needed to prove Theorem 2.1 by adding to PA and HA, a symbol for an unknown function $F:N \to N$. Call this PA(F), HA(F), $PA_n(F)$, $HA_n(F)$, EFA(F). These are nice, robust systems.

Take Theorem 2.1 as "if F is an infinite sequence from N^k that is decreasing in the lex ordering until it reaches zero, then it reaches zero".

THEOREM 2.2. Theorem 2.1 for $k = 1$ is provable in EFA(F). For any fixed $k \geq 2$, it is provable in $HA_1(F)$ but not in EFA(F).

But what about the full Theorem 2.1 for all k?

THEOREM 2.3. Theorem 2.1 is provable in $HA_2(F)$ but not in $PA_1(F)$.

A sharper theorem of this character is as follows. For $x,y \in N^k$, write $x \leq_c y$ iff for all i, $x_i \leq y_i$.

THEOREM 2.4. Every infinite sequence from N^k has a finite initial segment such that every term is $\geq_c$ some term in that finite initial segment.

It is trickier to be economical about the proof of Theorem 2.4.

The following can be obtained from a paper of Steve Simpson.

THEOREM 2.5. Theorem 2.4 for each fixed k is provable in $PA_1(F)$. Theorem 2.4 is provable in $PA_2(F)$ but not in $PA_1(F)$. Even for k = 1, Theorem 2.4 is not provable in HA(F). The equivalence of Theorems 2.1 and 2.4 can be proved in $PA_1(F)$.

The exotic nature of Theorems 2.1 and 2.4 become clearer as we move to finite forms and associated finite information.

THEOREM 2.6. For all $k \geq 1$ there is a longest sequence $x_1 >_{lex} x_2 >_{lex} ... >_{lex} x_n$ from N^k such that each $\max(x_i)$ □ i.

To prove this, fix $k \geq 1$. The space of all infinite sequences from N^k with these two properties forms an infinite finitely branching tree. There are no infinite paths by Theorem 2.1. Hence the tree is finite, and we are done.

Theorem 2.6 is a □□ statement in arithmetic.

THEOREM 2.7. Theorem 2.6 is provable in HA_2 but not in PA_1.

We now discuss the associated numerical information in Theorem 2.6.

We introduce (a version of) the Ackermann hierarchy of functions. We define strictly increasing functions $A_k:Z^+$ □ Z^+, where $k \geq 1$, as follows. $A_1(n) = 2n$, $A_{k+1}(n) = A_kA_k...A_k(1)$, where there are n A_k's.

$A_2(n) = 2^n$, $A_3(n)$ is an exponential tower of 2's of height n. The Ackermann function is $A(n) = A_n(n)$.

$A_3(1) = 2$. $A_3(2) = 4$. $A_3(3) = 16$. $A_3(4) = 2^{16} = 65,536$. $A_3(5) = 2^{65,536}$. $A_4(1) = 2$. $A_4(2) = A_3A_2(1) = A_3(2) = 4$. $A_4(3) = A_3A_4(2) = A_3(4) = 2^{16} = 65,536$. $A_4(4) = A_3A_4(3) = A_3(65,536)$, which is an exponential tower of 2's of height 65,536.

$A_4(4)$ is ridiculously large, but not incomprehensibly so. However, if we go much further, then a profound level of incomprehensibility emerges. These higher levels of largeness blur. We think of $A_5(5)$ as incomprehensibly large. We us it as a kind of benchmark.

Recall:

THEOREM 2.6. For all $k \geq 1$ there is a longest sequence $x_1 >_{lex} x_2 >_{lex} ... >_{lex} x_n$ from N^k such that each $\max(x_i)$ □ i.

Let h(k) = longest length.

THEOREM 2.8. In Theorem 2.6, h(k) is roughly the Ackermann function. I.e., there is a small c such that for all k, $A(k-c) \leq h(k) \leq A(k+c)$.

3. Hilbert basis theorem.

One common way of formulating the Hilbert basis theorem is this. We say that a ring R is Noetherian iff for all x_1,x_2, ..., there exists n such that all x's are ideal generated by $x_1,...,x_n$.

THEOREM 3.1. If R is a (countable) Noetherian ring then so is R[x].

However, this is too innocent a formulation in order to illustrate our theme, with exotic finite forms and associated numerical information.

For our purposes, we consider the following formulation of the Hilbert basis theorem.

THEOREM 3.2. Let $P_1,P_2,...$ be an infinite sequence of polynomials from the polynomial ring in k variables over a (countable) field. There exists n such that all P's are ideal generated by $P_1,P_2,...,P_n$.

Let us review a proof of this form of HBT.

Order the monomials in k variables lexicographically. First let Q_1,Q_2, ... enumerate all polynomials ideal generated by the P's. For each i, look at the leading monomial M_i of Q_i. Apply Theorem 2.4 to the sequence $M_1,M_2,...$, obtaining n such that all M's are multiples of at least one of $M_1,...,M_n$. This gives us m such that the leading coefficient of every Q is a multiple of the leading coefficient of at least one of $Q_1,...,Q_m$. Then every Q is ideal generated by $Q_1,...,Q_m$, using iterated division with remainder.

As indicated in the first lecture, we can derive Theorem 2.2 from Theorem 3.2 by considering sequences of monomials.

THEOREM 3.3. Theorems 2.4 and 3.2 are provably equivalent in EFA(F).

We now consider the following immediate consequence of Theorem 3.2. It should be viewed as a form of the standard application of HBT to decreasing chains of algebraic sets.

THEOREM 3.4. Let $P_1,P_2,...$ be an infinite sequence of polynomials from the polynomial ring in k variables over a (countable) field. There exists n such that every simultaneous zero of $P_1,...,P_n$ is a zero of all P's.

It is harder to show that Theorem 3.4 implies Theorem 2.4. The construction of the P's is trickier. of course, this implication cannot be done at all if we assume that the P's represent irreducible algebraic sets, by Krull's theorem for chains of prime ideals. So we are immersed in reducible algebraic sets.

Fix the dimension k and an infinite field F. Let T be a finite tree with at least one vertex, where every path excluding the root is of length □ k, and where the vertices other than the root are labeled with different elements of the field F. We call these the k-good trees.

The algebraic meaning of a vertex at the i-th level above the root with label c is the equation $x_i = c$. The algebraic meaning of a path is the conjunction of the algebraic meaning of the vertices along that path other than the root. The algebraic meaning of the tree T is the disjunction of the algebraic meanings of the paths of T.

Take [T] to be this union of intersections. Rewrite as intersection of unions. Each union is the zero set of a polynomial obtained by multiplying the relevant x_i-c. [T] becomes an algebraic subset of F^k, given by polynomials of degree □ #T = the number of terminal vertices of T.

We need to have a sufficient criterion for [T] to properly contain [T'].

LEMMA 3.5. Let T,T' be k-good trees. Suppose T' is obtained from T by adding one or more children to a terminal vertex. Or suppose T' is obtained from T by deleting one of the children of a vertex that has at least two children (and of course all vertices above the one deleted). Then [T] properly contains [T'].

Now all we have to do is to deal with the combinatorics of these two tree operations.

There is a nice way of assigning ordinals < $\square^k$ to k-good trees. For each terminal node x of height $1 \square i \square k$, assign the ordinal $\square^{i-1}$. Now take the sum of the ordinals assigned to the terminal nodes, in decreasing (≥) order. This is ord(T).

The two tree operations lower ordinal. Also, ord(T) is onto the ordinals < $\square^k$. Even more is true and useful. Given □ < ord(T), there exists T' obtained from T by successive applications of the two tree operations in some combination, such that ord(T') = □.

Recall that the lexicographic ordering used in Theorems 2.1 and 2.4 is just $\square^k$.

We have just provided a way of assigning an algebraic set to ordinals < $\square^k$ so that if the algebraic set decreases then the ordinal lowers.

THEOREM 3.6. Theorem 3.4 and 2.4 are provably equivalent in EFA(F).

We now come to finite forms. In $F[x_1,\ldots,x_k]$, the degree of an ideal means the least d such that the ideal is generated by its elements of degree □ d.

THEOREM 3.7. Let k ≥ 1 and F be a field. There is a bound on the length of chains of ideals $I_1 \square\neq \ldots \square\neq I_n \square F[x_1,\ldots,x_k]$, where each I_j is of degree □ j. Furthermore, the bound can be taken to depend on k only, and not on F.

Seidenberg proved Theorem 3.7, and more generally with any bounds on the degrees of the ideals. He called it the constructive form of Hilbert's basis theorem. In particular, he considered:

THEOREM 3.8. Le k,c ≥ 1 and F be a field. There is a bound on the length of chains of ideals $I_1 \square\neq \ldots \square\neq I_n \square F[x_1,\ldots,x_k]$, where each I_j is of degree □ j+c. Furthermore, the bound can be taken to depend on k,c only, and not on F.

Seidenberg established a primitive recursive bound only for k □ 2, and doubted whether one exists for k = 3.

In fact, there is a nice proof of Theorems 3.7, 3.8, using the compactness theorem for predicate calculus. The proof of Theorem 3.8 for each k ≥ 1 is naturally formalized in a system called RCA_0 + WKL_0, for which there is a metatheorem to the effect that every □□ sentence provable there has a primitive recursive realization. PA_1 is the major source of power of RCA_0 + WKL_0. Thus we can put Seidenberg's doubt to rest using machinery from mathematical logic.

The lower bounds for Theorems 3.7, 3.8 involving the Ackermann hierarchy are clear since the derivations of the finite forms of lex descent discussed earlier is easy.

Seidenberg did not consider Theorems 3.7, 3.8 for descending chains of algebraic sets:

THEOREM 3.9. Let k ≥ 1 and F be a field. There is a bound on the length of chains of algebraic sets $A_1 \supsetneq \ldots \supsetneq A_n$ □ $F[x_1,\ldots,x_k]$, where each A_i is of presentation degree □ i. Furthermore, the bound can be taken to depend on k only, and not on F.

We can show that the lower bounds in Theorem 3.9 are (roughly) at least those for our finite form of lex descent using the above way of assigning algebraic sets to ordinals.

4. Degrees of algebraic approximations to sets.

The logically exotic nature of HBT and its finite forms generally does not spill over to its applications to commutative algebra/algebraic geometry. Often HBT is the simplest way to obtain a result, but harder work will avoid HBT and lead to decent estimates.

For example, the decomposition of algebraic sets into irreducible components has a treatment with decent bounds, avoiding HBT. My impression is that there are some important situations where removal of HBT has not yet been achieved.

One should look further into the possible role of exotic functions in algebraic geometry and commutative algebra.

The idea is to recognize that sequences of algebraic sets or ideals, even if of finite length, are too arbitrary. Instead, one wants any such sequence to come out of more ordinary data; e.g., as a construction that is used in a proof.

Along these lines, the unique decomposition of algebraic sets into irreducible components is just perfect, except that HBT is completely avoided in favor of explicit arguments, and the associated numerical information is the opposite of exotic.

Digression on Hilbert functions.

The theory of Hilbert functions and Hilbert polynomials has a certain exotic combinatorial underpinning. We have uncovered a simple fact about Hilbert functions which relates to the Ackermann function.

A polynomial in $F[x_1,...,x_k]$ is called homogenous if and only if all of its monomials are of the same degree.

Let M be an ideal in $F[x_1,..., x_k]$. We define M_n to be the set of all homogenous polynomials in M of degree n.

The Hilbert function of $F[x_1,...,x_k]/M$ is the function H:N □ N defined by

H(n) = the dimension of $F[x_1,...,x_k]/M_n$ as a vector space over F, which is the same as

P(k,n) minus the dimension of M_n as a vector space over F,

where P(k,n) is the number of k-tuples of nonnegative integers whose sum is n. It is well known that P(k,n) is a polynomial of degree k-1 with rational coefficients.

THEOREM 4.1. (Hilbert). $HF(M_n)$ agrees with a unique polynomial of degree □ k-1 with rational coefficients for all sufficiently large n. This unique polynomial is called the Hilbert polynomial of $F[x_1,...,x_k]/M$.

Let us call the k dimensional Hilbert functions the Hilbert functions of the $F[x_1,...,x_k]$ /M, where M is an ideal in $F[x_1,...,x_k]$. These functions depend only on k and not on the field F.

Various characterizations of these functions have been established, mainly due to Macauley.

Let us define the k dimensional Hilbert function agreement sets as those sets of the form $\{n: f(n) = g(n)\}$, where f,g are k dimensional Hilbert functions.

THEOREM 4.2. For all $k \geq 1$ there is a finite subset of N which is not a k dimensional Hilbert function agreement set. The least size of such a set, as a function of k, grows like the Ackermann function.

End of Digression on Hilbert functions.

We now propose a structural theorem about algebraic S □ $F[x_1,\ldots, x_k]$.

The n-th algebraic approximation to S is the least algebraic superset of S of presentation degree □ n. This always exists, even if S is not algebraic.

If □n is replaced by n then we get the same definition. For algebraic S, we have $S[0] \supseteq S[1] \supseteq \ldots \supseteq S[d] = S$, where $\deg(S) = d$.

We call S rich iff the S[i], 0 □ i □ d, are distinct. This is the same as: for all 0 □ i □ d, $\deg(S[i]) = i$.

Note that this series fits squarely into Theorem 3.9 about bounds on lengths of chains of algebraic sets. So

THEOREM 4.3. For all $k \geq 1$ and field F, there is a bound to the degrees of the rich algebraic subsets of $F[x_1,\ldots,x_k]$. The bound can be taken to depend on k and not on F.

From what we saw earlier, upper bounds given by the Ackermann function.

The lower bounds are also approximately the Ackermann function, with a more involved construction. The lower bounds are exotic even if only finite rich sets in finite fields are considered.

LECTURE 3
COMPARISON OF BLOCKS, TREES, GRAPHS, COUNTABLE POINTSETS

Harvey M. Friedman
The Ohio State University
http://www.math.ohio-state.edu/~friedman/
September 19, 2002

In this third lecture, the levels of abstraction in the proof methods are more exotic than in the second lecture. In the fourth lecture, they are far more exotic still.

5. Comparison of blocks within finite sequences of natural numbers.

Let us start with the following simple problem, which Paul Sally uses in his gifted high school program.

THEOREM 5.1. There is a longest finite sequence $x_1,x_2,...,x_n$ from {1,2} in which no consecutive block $x_i,...,x_{2i}$ is a subsequence of any later consecutive block $x_j,...,x_{2j}$.

Let us call this property of finite sequences property *.

One can easily show that the longest length of a sequence from {1,2} with property * is 11, and that the only examples are 12221111111 and 21112222222. One of the gifted high school students was able to show this.

THEOREM 5.2. There is a longest finite sequence from {1,2,3} with property *.

This is no longer a gifted high school theorem. The simplest known proof of this is truly exotic compared with the statement. With some considerable trouble, it can be replaced with a considerably less exotic proof, but still rather exotic compared to the statement.

We sketch this simplest known proof, which uses the Nash Williams minimal bad sequence argument in this context.

First we shift context to infinite sequences of finite sequences.

THEOREM 5.3. Let $k \geq 1$ and $x_1,x_2,...$ be an infinite sequence of finite sequences from {1,...,k}. There exists $i < j$ such that x_i is a subsequence of x_j.

Suppose this is false. Call an infinite sequence bad if it is a counterexample. Let x_1 be of least length so that it starts an infinite bad sequence. Let x_2 be of least length so that x_1,x_2 starts a bad sequence. Continue in this way, getting a “minimal” bad sequence $x_1,x_2,...$. There is an infinite subsequence $x_{i1},x_{i2},...$, all of which start with the same number. Note that $x_{i1}',x_{i2}',...$ is bad, where the primes mean "chop off the first term" (no x can be empty). Hence $x_1,...,x_{i1 -1},x_{i1}',x_{i2}',...$ is also bad. But x_{i1}' is shorter than x_{i1}, contradicting the choice of x_{i1}. QED

We now prove that there is a longest finite sequence from {1,2,3} with property *.

Suppose there are arbitrarily long such. Build the finitely branching tree of such. Let $x_1,x_2,...$ be an infinite branch, which therefore has property *. Consider the infinite sequence

x_1,x_2

x_2,x_3,x_4

x_3,x_4,x_5,x_6

...

By Theorem 5.3, one is a subsequence of a later one. This contradicts property *.

Obviously we did not use that there are only three letters.

THEOREM 5.4. (Block subsequence theorem). For all $k \geq 1$, there is a longest finite sequence $x_1,....,x_n$ in k letters in which no consecutive block $x_i,...,x_{2i}$ is a subsequence of a later consecutive block $x_j,...,x_{2j}$.

In order to tame the proof of the block subsequence theorem, we need to tame Theorem 5.3. I.e., we need to replace the minimal bad sequence argument with something more concrete.

The sharpest way to do this is to effectively assign (names for) ordinals < ω^{ω^k} to finite bad sequences from {1,...,k+1}, where if one is extended to another, then the corresponding ordinal decreases (due to Simpson).

THEOREM 5.5. The block subsequence theorem is provable in PA_3.

This is because PA_3 suitably handles the ordinal ω^{ω^ω}. For each fixed k, PA_2 suitably handles the ordinal ω^{ω^k}.

We have shown how to reverse this process in order to show how ω^{ω^ω} can be suitably handled in EFA + the block subsequence theorem.

Using well known information from the proof theory of fragments of PA, we obtain

THEOREM 5.6. The block subsequence theorem is not provable in PA_2.

Back to the block subsequence theorem with 3 letters. To obtain an exotic lower bound, we make some rather special arguments for this context.

We begin with a somewhat long finite bad sequence $x_1,...,x_{2p}$ from {1,2,3} such that for all 1 □ i □ p, the block $x_i,...,x_{2i}$ has a 1, and the last p terms are 133...3. We were able to create one of these so called "special" sequences $x_1,...,x_{216}$ by hand.

The long bad sequence from {1,2,3} has the form $x_1,...,$ x_{216},y, where y is a long sequence of 2's 3's.

None of the first relevant 108 blocks will be subsequences of later relevant blocks, since they have a 1 in them.

This applies to many of the next 108 relevant blocks since they have so many 3's in them, and we won't ever have so many consecutive 3's, and the first term of y is 2.

We use $23^{25}2$ as markers that occur at successively incrementally greater spacing apart, where what goes in between these markers is of critical importance.
These "in between" blocks of 2's, 3's have exactly 8 3's.

A series of technical Lemmas show that the resulting sequence has property * if no in between block is a subsequence of any later in between block.

So we just have to create a very long sequence of incrementally length growing sequences of finite 2's, 3's with exactly 8 3's, no one of which is a subsequence of a later one.

This is a much easier combinatorial challenge, and one can create $A_7(184)$ of them in this context.

THEOREM 5.7. The longest length of a bad sequence from {1,2,3} is > $A_7(184)$.

"7" was derived from the length 216 of the special sequence, which acts as a seed.

Randall Dougherty wrote some software that looks for special sequences. He was able to find one of length 187,196. Plugging this into our machinery, we obtain:

THEOREM 5.8. The longest length of a bad sequence from {1,2,3} is > $A_{7198}(158,386)$.

For those not here yesterday, the Ackermann hierarchy of functions is defined by

$A_1(n) = 2n$, $A_{k+1}(n) = A_kA_k... A_k(1)$, where there are n A_k’s. Define $A(n) = A_n(n)$. A(4) is an exponential stack of 2’s of height 65,536. A(5) is incomprehensibly large.

As for an upper bound, we haven’t work this out, but are confident that A(A(5)) is a crude upper bound.

If we consider 4 letters, then the numbers grow considerably more exotic. The longest length is greater than AA...A(1), where there are A(5) A’s.

Let J(k) be the longest length of a sequence with property * in k letters.

Then J grows faster than all multiply recursive functions. By comparison, the Ackermann function is a puny little doubly recursive function.

6. Comparison in sequences of finite trees, and within large finite trees.

A poset is a pair (D,□) where D is a nonempty set and □ is a reflexive transitive relation obeying

(x □ y □ y □ x) □ x = y.

A tree is a poset T = (V,□) where there is a minimum element called the root, and where for each x □ T, {y: y □ x} is linearly ordered by □.

The elements of V = V(T) are called the vertices of T. A tree is said to be finite if it has finitely many vertices.

For finite trees, we define the inf operation on V, where x inf y is the greatest z such that z □ x □ z □ y.

Let T_1 and T_2 be finite trees. h is an inf preserving embedding from T_1 into T_2 iff

i) h:V(T_1) □ V(T_2) is one-one;
ii) for all x,y □ V(T_1), h(x inf y) = h(x) inf h(y).

Here is the most rudimentary form of J.B. Kruskal's theorem.

THEOREM 6.1. In any infinite sequence of finite trees, one tree is inf preserving embeddable into a later tree.

The Nash Williams infinite bad sequence argument was invented to give the simplest proof known of Theorem 6.1.

Before we prove this, there is a Lemma needed due to Graham Higman. The simplest proof of this Lemma also uses the minimal bad sequence argument, although it can be avoided in favor of something less exotic. However, the minimal bad sequence argument for the main body of the proof of Kruskal's theorem is largely unavoidable (it can be tamed a little bit).

A quasi ordering is a reflexive transitive relation. A wqo (well quasi ordering) is a quasi ordering □ such that in any infinite sequence from its field, one term is □ a later term.

Theorem 6.1 can be restated: The finite trees ordered by one-one inf preserving embeddability form a wqo.

Let Q be a wqo. Write FIN(Q) for the quasi ordering of all finite subsets from Q, where A □* B iff there exists one-one h:A □ B such that for all x □ A, x □* h(x).

THEOREM 6.2. (Higman's Theorem). If Q is a wqo then FIN(Q) is a wqo.

We first need a general fact about wqo's, which is an easy application of Ramsey's theorem for pairs.

LEMMA. If (Q,□) is a wqo then every infinite sequence from Q has an infinite increasing (□) subsequence.

To prove Higman's theorem, let Q be a wqo, and suppose FIN(Q) is not a wqo. Let x_1 □ FIN(Q) be of least cardinality that starts an infinite bad sequence in FIN(Q). Let x_2 be of least cardinality such that x_1,x_2 starts an infinite bad sequence in FIN(Q). Continue in this way, getting a minimal bad $x_1,x_2,...$ in FIN(Q).

Look at the first terms of the x's. By the general fact, there is an infinite sub-sequence $x_{i1},x_{i2},...$ whose first terms are increasing in Q. Hence $x_{i1}',x_{i2}',...$ is bad, where the primes indicate throwing away an element from each (none of the x's can be empty). Therefore $x_1,...,x_{i1-1},x_{i1}',x_{i2}',...$ is also bad in FIN(Q). Since x_{i1}' is of lesser cardinality than x_{i1}, we have a contradiction.

Now we prove KT.

THEOREM 6.1. (Kruskal's theorem). In any infinite sequence of finite trees, one tree is inf preserving embeddable into a later tree.

Suppose there is an infinite bad sequence T_1,T_2, ... of finite trees. Let T_1 have the least number of vertices such that it starts an infinite bad sequence of finite trees. Let T_2 have the least number of vertices such that T_1,T_2 starts an infinite bad sequence of finite trees. Continue in this way to form a minimal bad sequence $T_1,T_2,...$ of finite trees.

If we chop off the root of a finite tree, we get a finite set of trees. Let V be the union of all trees obtained in this way from the T's. We claim that this set V of trees is a wqo.

To see this, suppose there is an infinite bad sequence in V. Let this be $S_1,S_2,...$, where the S's come from successively later T's, and where S_1 comes from T_i. Then $T_1,...,T_{i-1},S_1,S_2,...$ is an infinite bad sequence of trees, with S_1 smaller than T_i. This is a contradiction.

So V is a wqo. By Higman's Lemma, FIN(V) is a wqo. Now go back to $T_1,T_2,...$ and chop off the roots, getting a sequence $T_1',T_2',...$ from FIN(V). Let T_i' □* T_j'. Then T_i is inf preserving embeddable into T_j, which is the desired contradiction. QED

The exotic nature of the proof of Kruskal's theorem is much stronger than the necessary uses of induction in the second lecture.

We will discuss how we classify the power of such proof methods later.

But first we discuss the finite forms of Kruskal's theorem. Our original ones correspond to the ones we gave for lexicographic descent, and the first way we did this with the Hilbert basis theorem. We look at finite sequences with bounded growth rate.

THEOREM 6.3. Let $k \geq 1$ and $T_1,...,T_n$ be a sufficiently long finite sequence of finite trees, where each T_i has at most $k+i$ vertices. There exist $i < j$ such that T_i is inf preserving embeddable into T_j.

To prove this, let $k \geq 1$ and assume false. Form the finitely branching tree of finite bad sequences subject to the inequality. (Use a concrete representation of finite trees so that isomorphic finite trees are identical). This tree is infinite by hypothesis. Hence it has an infinite path, which forms an infinite bad sequence of fnite trees. This contradicts Kruskal's theorem. QED

Note that Theorem 6.3 is a purely finite statement. To greatly understate the truth, Theorem 6.3 is unprovable in Peano Arithmetic.

Theorem 6.3 is not the first example of a serious finite theorem that is unprovable in PA. The first came out of Ramsey theory, which we discuss later. However, Theorem 6.3 is incomparably more exotic than those first examples, in the sense of being unprovable in far stronger systems and also having far higher associated finite information.

We found a structural theorem about a single large finite tree that is equally exotic.

A full finite tree is a finite tree whose terminal vertices have the same height, where all nonterminal vertices have the same valence.

An r-labeled tree is a tree together with a mapping of the vertices into $\{1,...,r\}$.

THEOREM 6.4. Let $k,r \geq 1$ and T be a sufficiently tall full finite r-labeled tree of valence k. Then some truncation of

T is inf, label, and terminal preserving embeddable into a higher truncation of T.

We have shown that Theorem 6.4 is unprovable in PA, and also much stronger systems, even for $k = 2$.

Theorems 6.3, 6.4 also have exotic associated finite information.

7. Graph minors in sequences of finite graphs.

Finite graphs are pairs (V,E), where for all x E, we assign a set of vertices of cardinality 1 or 2.

G is minor included in H iff G can be obtained from H by successively deleting a single edge, contracting a single edge, or removing an isolated vertex.

Minor inclusion is normally taken up to isomorphism. Here is the graph minor theorem of Robertson/Seymour.

THEOREM 7.1. In any infinite sequence of finite graphs, one graph is minor included in a later graph.

At a critical place, the proof of Theorem 7.1 uses an iterated form of the infinite bad sequence argument. We used a single infinite bad sequence argument for Kruskal's tree theorem (the second one used for Higman's Theorem can be avoided).

Such iterations are known to be more powerful as the iteration length increases.

Before the graph minor theorem was proved, we proved an extension of Kruskal's theorem called EKT.

We proved EKT using a finitely iterated minimal bad sequence argument. We showed that these iterations are unavoidable.

We asked Robertson/Seymour to explicitly derive our EKT from their GMT. Robertson/ Seymour succeeded in doing this. Therefore the GMT is at least as exotic as the EKT.

Let $r \geq 1$ and T_1 and T_2 be finite r-labeled trees with labeling functions l_1 and l_2. We say that h is a gap embedding from T_1 to T_2 iff

i) h is a one-one map from the vertices of T_1 to the vertices of T_2;
ii) for all vertices $h(a) < c < h(b)$ of T_2, $l_2(c) \geq l_2(h(b))$.

THEOREM 7.2. Extended Kruskal's Theorem. Let $r \geq 1$ and $T_1,T_2,...$ be an infinite sequence of finite r-labeled trees. There exist $i < j$ and an inf and label preserving gap embedding from T_i into T_j.

We gave finite forms for Theorem 7.2 in terms of sequences of trees. We also gave a version for a single tall finite tree, analogously as we did for Kruskal's theorem. These have the expected exotic properties.

Let |G| be the sum of the number of vertices and the number of edges in the finite graph G.

THEOREM 7.3. Let $k \geq 1$ and $G_1,...,G_n$ be a sufficiently long finite sequence of finite graphs, where each $|G_i| \square k+i$. There exist $i < j$ such that G_i is minor included in G_j.

The EKT, GMT, and their finite forms are much more exotic than KT and its finite forms.

8. Continuous comparison of countable sets of reals.

It is now time to present a hierarchy of formal systems that are normally used to measure the level of intrinsic exoticness.

Recall that in the second lecture, the logical issues were the level of induction needed, and growth rates involving the Ackermann hierarchy of functions. There it was sufficient to use fragments of PA and PA(F) as yardsticks.

These tools are also entirely suitable for our discussion of the block subsequence theorem, which we saw blows up numerically with only 3 letters.

However, when it comes to KT, EKT, and GMT, as well as their finite forms, we are way beyond systems like PA and PA(F).

We will place all theorems in lectures 2,3 in terms of some standard systems with quantifiers over natural numbers and sets of natural numbers.

We begin with a particularly strong such system, Z_2. Here is the syntax of Z_2.

i) variables over natural numbers (lower case);
ii) variables over sets of natural numbers (upper case);
iii) 0,S,+,•,= (in the natural numbers only);
iv) □ (between natural numbers and sets).

Number terms are built up from number variables and 0,S,+,•, in the obvious way.

The atomic formulas of Z_2 are s = t, and t □ A, where s,t are number terms and A is a set variable. Formulas are built up from atomic formulas by □,□, ,□ ,□ and □n,□A,□n,□A.

The axioms of Z_2 are as follows.

1. □S(x) = 0, S(x) = S(y) □ x = y.
2. x+0 = x, x+S(y) = S(x+y).
3. x•0 = 0, x•S(y) = (x•y)+x.
4. (0 □ A □ (□n)(n □ A □ S(n) □ A)) □ (□n)(n □ A).
5. (□A)(□n)(n □ A □ □), where □ is any formula in the language in which A does not appear.

The theorems of lectures 2,3 are easily proved in weak fragments of Z_2, and so Z_2 is gross overkill for our present purposes. But just wait until the fourth lecture, where Z_2 is grossly inadequate!

What we use here is carefully chosen fragments of Z_2. Five such fragments have emerged most frequently as benchmarks for the logical analysis of a great number of theorems.

These are our formal systems RCA_0, WKL_0, ACA_0, ATR_0, $□^1{}_1$-CA_0. They are all weak fragments of full Z_2. These are from weakest to strongest.

The "naughts" have historical significance indicating the explicit way induction is formulated.

1. RCA_0. The set comprehension axiom is called "recursive comprehension". Details later.

2. WKL_0. This is RCA_0 together with "every infinite finitely branching tree has an infinite path".

3. ACA_0. Same as Z_2 except in the comprehension axiom, no set quantifiers are allowed in φ.

4. ATR_0. This is ACA_0 together with "arithmetic transfinite recursion". This means that transfinite recursion, with arithmetic recipes, can be performed along any well ordering of numbers.

5. Π^1_1-CA_0. Same as Z_2 except in the comprehension axiom, at most one set quantifier is allowed in φ.

RCA_0 is the weakest. Call a formula existential numerical if and only if it begins with zero or more existential number quantifiers followed by only bounded numerical quantifiers (i.e., $(\forall n < m\bullet r)$, where < is defined in the usual way). Here are the axioms of RCA_0. There are many equivalent versions.

1. Numerical axioms 1-3 of Z_2.

2. $(\varphi[n/0] \wedge (\forall n)(\varphi \rightarrow \varphi[n/S(n)])) \rightarrow \varphi$, where φ is existential numerical.

3. $(\forall n)(\varphi \leftrightarrow \neg\psi) \rightarrow (\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ,ψ are existential numerical and do not mention A.

In reverse mathematics, we analyze mathematical theorems in the following way. First we formalize a proof in one of the five systems RCA_0, WKL_0, ACA_0, ATR_0, Π^1_1-CA_0, the weaker the better.

E.g., the theorem is proved in ACA_0. Then show that the theorem is equivalent to ACA_0 over RCA_0 by proving ACA_0 using RCA_0 together with the theorem.

Failing that, use a host of other logically natural systems to generate a match, but always use RCA_0 as the "base theory".

And failing that, set up a new formal system for an exact match.

I could easily spend 4 lectures on the story of reverse mathematics. Instead see: Steve Simpson, Subsystems of Second Order Arithmetic, Springer, 1999.

Here is a status table for the theorems of lectures 2,3, including Ramsey's theorem.

PROVABLE IN RCA$_0$

The finite Ramsey theorem.

Minimization in norm of integral polynomials.

Lex descent for fixed dimension. Strengthening with $□_c$ for fixed fixed dimension. Finite forms for fixed dimension.

Hilbert basis theorem for fixed dimension. Various consequences involving algebraic sets for fixed dimension. Finite forms for fixed dimension.

PROVABLE IN ACA$_0$

The infinite Ramsey theorem for fixed dimension. An exotic finite form for fixed dimension.

Lex descent. Strengthening with $□_c$. Finite forms.

Hilbert basis theorem. Various consequences involving algebraic sets. Finite forms.

The block subsequence theorem. Finite sequences from any {1,...,k} are wqo. Higman's theorem.

PROVABLE IN ATR$_0$

The infinite Ramsey theorem. An exotic finite form (Paris and Harrington).

For any two sets of rationals, one can be continuously embeddable into the other. Same with reals.

PROVABLE IN $□^1_1$-CA$_0$

Kruskal's theorem (even with labels and orientation). Finite forms.

Extended Kruskal's theorem for any fixed set of finite labels. Finite forms for any fixed set of finite labels.

The existence of minimal infinite bad sequences.

NOTE: The extended Kruskal theorem and the graph minor theorem are a bit beyond even $\square^1_1$-CA$_0$.

To illustrate the reversal idea, we give the following relevant examples.

THEOREM 8.1. Any of the following are provably equivalent to "$\square^{\square}$ is well ordered" over RCA$_0$. Lex descent. Strengthening with $\square_c$. Hilbert basis theorem. Various consequences involving algebraic sets.

THEOREM 8.2. Any of the following are provably equivalent to "every level of the Ackermann hierarchy exists" over RCA$_0$. Finite forms of lex descent. Finite forms of strengthening with $\square_c$. Finite forms of Hilbert basis theorem. Finite forms of various consequences involving algebraic sets.

THEOREM 8.3. The block subsequence theorem is equivalent to "every multiply recursive function exists" over RCA$_0$.

THEOREM 8.4. Higman's theorem is equivalent to ACA$_0$ over RCA$_0$.

THEOREM 8.5. "For any two sets of rationals, one can be continuously embeddable into the other" is equivalent to ATR$_0$ over RCA$_0$. The same is true if we replace "rationals" with "reals".

THEOREM 8.6. Kruskal's theorem is equivalent to a specific large proof theoretic ordinal "is well ordered" over RCA$_0$. Same with extended Kruskal's theorem and the graph minor theorem for bounded tree width.

THEOREM 8.7. The existence of minimal infinite bad sequences is equivalent to $\square^1_1$-CA$_0$ over RCA$_0$.

LECTURE 4
BOREL DIAGONALIZATION, BOREL SELECTION, BOOLEAN RELATION THEORY

Harvey M. Friedman
The Ohio State University
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/

September 20, 2002

In this final lecture, the gap between the statement of the theorems and what must be involved in the proofs is particularly apparent.

In the first half, we work in the context of Borel measurable sets and functions on the reals or other complete separable metric spaces (Polish spaces). We will generally stay within ZFC.

In the second half, we work in discrete mathematics, with functions on and sets of natural numbers. After some preliminary results, we will require something beyond the accepted axioms for mathematics.

9. Borel Diagonalization.

Consider Cantor’s theorem.

THEOREM 9.1. In any infinite sequence of real numbers, some real number is not a coordinate of the sequence.

One defines a sequence of nondegenerate closed intervals with rational endpoints, shrinking to a point that lies off of the sequence. By standard descriptive set theoretic technology:

THEOREM 9.2. There is a Borel measurable function F:¬ □ ¬ such that for all x □ ¬•, F(x) is not a coordinate of x.

F(x) may depend only on the (set of) coordinates of x.

THEOREM 9.3. There is no Borel measurable function F:¬• □ ¬ obeying rng(x) = rng(y) □ F(x) = F(y), such that for all x □ ¬•, F(x) is not a coordinate of x.

Or put positively,

THEOREM 9.4. Let F:¬• □ ¬ be Borel measurable, where for all x,y in ¬•, rng(x) = rng(y) □ F(x) = F(y). There exists x □ ¬• such that F(x) is a coordinate of x.

We sketch a proof of a sharp form of Theorem 9.4. There is something exotic about it.

Let ¬* be the reals with the ***discrete topology***. Is the discrete topology is one of those worthless meaningless things from the new new new new math? We shall see.

Granted, ¬* is silly, but ¬*$^{\bullet}$ is not. The basic open sets in ¬*$^{\bullet}$ are the V_x = {f □ ¬*$^{\bullet}$: f extends x}, where x □ FS(¬) = set of all finite sequences from ¬. Obviously every open (Borel) subset of ¬$^{\bullet}$ is an open (Borel) subset of ¬*$^{\bullet}$ but not vice versa.

In any topological space, a set is called meager iff it is contained in a countable union of nowhere dense sets; comeager iff its complement is meager; Borel iff it is in the least □ algebra containing all open sets.

LEMMA 9.5. In any topological space, every Borel set differs from an open set by a meager set.

Baire category for ¬$^{\bullet}$:

LEMMA 9.6. ¬$^{\bullet}$ is not meager. In fact, no V_x is meager.

0,1 laws for ¬$^{\bullet}$:

LEMMA 9.7. Let A □ ¬$^{\bullet}$ be Borel and permutation invariant. Then A is meager or comeager.

We say that F: ¬$^{\bullet}$ □ ¬ is Borel iff the inverse image of every open subset of ¬ is a Borel subset of ¬$^{\bullet}$.

LEMMA 9.8. Every permutation invariant Borel f:¬$^{\bullet}$ □ ¬ is constant on a comeager set.

THEOREM 9.9. Every permutation invariant Borel f:¬$^{\bullet}$ □ ¬ maps some argument to a coordinate of itself.

Obviously the use of the discrete topology to prove a statement living in standard separable spaces is highly unusual. Recall the standard well known 0,1 law:

Every permutation invariant Borel function f:¬$^{\bullet}$ □ ¬
is constant on a comeager set of full measure.

But this does not allow us to derive Theorem 9.9 because

For all c, {x □¬$^{\bullet}$: c is a coordinate of x}
is meager and null.

There are metamathematical results to the effect that Theorem 9.9 is a separable theorem that has no separable proof. One formulation that is not wholly satisfactory is that Theorem 9.9 cannot be proved in countable set theory. But Theorem 9.9 cannot even be directly stated in countable set theory since it mentions ¬.

Two ways of clarifying this: One is to indicate how countable set theory can formulate separable statements like Theorem 9.9, by treating Borel functions as recipes for producing values at arguments, thereby avoiding the use of any uncountable sets.

A second way is less standard but perhaps better. This is to use class theory with countable sets. The complete separable metric spaces are classes rather than sets. Borel sets and Borel functions are treated as classes.

Under both approaches, one sees how separable mathematics is easily formalized, and we can prove that Theorem 9.9 is not provable in the corresponding formal systems. The class theory with countable sets includes the set theory with countable sets.

The usual axioms of ZFC:

1. Extensionality.
2. Pairing.
3. Union.
4. Separation.
5. Infinity.
6. Foundation.
7. Choice.
8. Power set.
9. Replacement.

Countable set theory is obtained by removing power set, written ZFC\P. Can't prove the existence of uncountable sets.

The class theoretic approach is based on NBG = von Neumann, Bernays, Godel, which is the standard class theory associated with ZFC. For our purpose, use NBG\P + AxC.

If we add the axiom "S(N) exists" to either of these systems, we can prove Theorem 9.9.

Our original method for proving such Borel theorems uses the forcing technique of Paul J. Cohen, which was invented to show the independence of the continuum hypothesis from the axioms of choice over ZFC.

Sometimes one can straightforwardly eliminate all razzle dazzle in favor of simple Baire category arguments, such as for Theorem 9.9. However, most often the elimination is awkward and unrewarding.

There are a number of further Borel diagonalization results at this level of logical power.

THEOREM 9.10. Let f:¬• ▯ ¬• be a Borel function such that rng(x) = rng(y) ▯ rng(f(x)) = rng(f(y)). There exists x such that rng(f(x)) ▯ rng(x).

For x,y ▯ ¬•, define x ~ y iff y is a permutation of x.

THEOREM 9.11. Let f: ¬• ▯ ¬• be such that x ~ y ▯ f(x) ~ f(y). There exists x ▯ ¬• such that F(x) is a subsequence of x.

Let 2^N be the usual Cantor space. Let s:2^N ▯ 2^N be given by s(x)(n) = x(n+1). f:K ▯ K is called shift invariant iff f(x) = f(sx).

THEOREM 9.12. Let f:K ▯ K be a shift invariant Borel function. There exists x ▯ K such that f(x) = $x^{(2)}$.

Here $x^{(2)} = (x_1,x_4,x_9,x_{16},\ldots)$.

Let T be the circle group. f:T ▯ T is double invariant if and only if T(2x) = T(x).

THEOREM 9.13. There is a Borel f:T ▯ T which agrees with every double invariant g:T ▯ T somewhere.

There are some additional Borel statements of this same level of logical power.

Let GRP(N) be the groups with domain N.

THEOREM 9.14. Let f:GRP(N) ▯ GRP(N) be an isomorphically invariant Borel function. There exists G such that f(G) is embeddable in G.

We now move to a much higher level: Let E □ ¬□¬ be a Borel equivalence relation. E induces an equivalence relation on ¬$^{\bullet}$, coordinatewise.

THEOREM 9.15. Let E be a Borel equivalence relation on R and f:¬$^{\bullet}$ □ ¬ be Borel, where x E y □ f(x) E f(y). There exists x □ ¬$^{\bullet}$ such that f(x) is E-equivalent to a coordinate of x.

Let GRA(N) be the graphs with vertex set N (undirected, no multiple edges). Subgraphs are obtained by deleting edges and vertices. Induced subgraphs are obtained by deleting vertices only. GRA(N) forms a Cantor space.

THEOREM 9.16. Let f:GRA(N) □ GRA(N) be an isomorphically invariant Borel function. There exists G such that every connected component of f(G) is isomorphic to a connected component of G.

THEOREM 9.17. Let f:GRP(N)$^{\bullet}$ □ GRP(N) be an isomorphically invariant Borel function. There exists x such that f(x) is isomorphic to a coordinate of x.

Theorems 9.15 - 9.17 are provable in ZFC\P plus "the power set operation can be iterated along any countable ordinal". This is legal; i.e., it is a subsystem of ZFC.

However, ZFC\P plus "the power set operation can be iterated along □", where □ is any suitably specified countable ordinal, is not sufficient for any of Theorems 9.15 – 9.17.

10. Borel selection/ antiselection in symmetric Borel sets.

We will be at the level of ZFC\P + "the power set operation can be iterated along any countable ordinal".

The history starts with work on infinite games. Two players I,II successively play natural numbers, for infinitely many years.

At the end of the game, I has played x □ N^N and II has played y □ N^N.

Before they start playing, W □ N^N□N^N is given. After they finish playing, the win is assigned to I or II according to whether (x,y) □ W.

There is a clear notion of winning strategy. This is a recipe for producing plays according to the earlier plays of your opponent, so that no matter how your opponent plays, you will win the game after infinitely many plays.

A series of results appeared saying that if W is a low level Borel set then one of the two players has a winning strategy for the game associated with W. The proofs got a bit more exotic as one crawled up a little ways in the Borel hierarchy.

In the mid 1960's, D.A. Martin proved the existence of winning strategies for all Borel W using axioms far beyond those available in ZFC. This is called Borel determinacy (BD).

In 1968, we showed that there is no proof of BD in ZFC\P + "the power set operation can be iterated along □", where □ is any suitably specified countable ordinal.

In 1974, Martin finally gave a legal proof of BD; i.e., in ZFC, and in fact using just ZFC\P + "the power set operation can be iterated along any countable ordinal". According to Martin, knowledge that this logical power is necessary was crucial.

In the 1980's we brought BD into the realm of classical analysis as follows. Let E □ ¬x¬ and A □ ¬. A selection for E on A is a function f:A □ ¬ such that for all x □ A, (x,f(x)) □ E. We say that E is symmetric if and only if (x,y) □ E □ (y,x) □ E.

THEOREM 10.1. Let E □ ¬□¬ be a symmetric Borel set. Then E or ¬\E has a Borel selection on ¬.

We showed that Theorem 10.1 has the same status as BD. I.e., we need arbitrarily long countable well ordered iterations of the power set operation. As in BD, the number of iterations needed corresponds directly to the level in the Borel hierarchy of the given Borel set (and not on the level of the Borel selection obtained).

11. Borel selection in Borel sets.

Logical issues in Borel statements remained dormant from the mid 80’s to this century. We came into contact with G.

Debs of Paris VII and his series of joint papers with Saint Raymond concerning selection theorems (they use different terminology).

They mostly worked in more general settings than Borel functions, and used strong set theoretic methods beyond ZFC. We asked Debs what happens when their stuff is pared down to Borel functions. The reply was that high powered set theoretic methods appear to still be needed. In particular, they would still need to use BD for some statements, and principles outside ZFC for others.

We know high powered set methods are necessary here.

Many of their theorems take the form of local/global principles of selection.

THEOREM 11.1. Let S □ ¬□¬ be Borel and E □ R 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.

The proof uses BD, and so it suffices to use iterations of the power set operation along any countable ordinal. We have shown that iterations along any suitably specified countable ordinal does not suffice.

PROPOSITION 11.2. Let S □ R x R and E □ R be Borel. If there is a Borel selection of S on every compact subset of E, then there is a Borel selection for S on E.

Debs/Saint Raymond prove Proposition 11.2 by using the following technical axiom that goes beyond ZFC:

COUNT. There are at most countably many sets of integers Gödel constructible in any given set of integers.

COUNT has been studied by set theorists already in the 1960’s. It is immediate from Gödel that COUNT is not provable in ZFC.

COUNT is somewhat tame because of the following relative consistency result due to Levy and Solovay:

THEOREM 11.3. ZFC + COUNT is consistent iff ZFC + “there is a strongly inaccessible cardinal” is consistent.

Some algebraic geometers are familiar with the assumption "there is a strongly inaccessible cardinal" as the set theoretic formulation of "there is a Grothendieck universe".

We showed that Proposition 11.2 is not provable in ZFC.

Our results concerning Theorem 11.1 and Proposition 11.2 are an elaboration on our original techniques from 1968 showing the logical power of BD. They involve various manipulations of non well founded models of fragments of ZFC.

DIGRESSION ON BOREL STATEMENTS OF GREAT LOGICAL STENGTH.

Let FG(N) be the space of all finitely generated groups whose domain is N. This is a Borel subspace of the Baire space B(N) of binary functions from N into N.

The following is provable using all finite number of iterations of the power set operation starting at N, but not any finite number.

THEOREM 11.4. Let $F:FG(N)^{\bullet} \to FG(N)$ be an isomorphically invariant Borel function. There exists $x \in FG(N)^{\bullet}$ such that f(x) is embeddable in a coordinate of x.

Now consider the following.

THEOREM 11.5. Let $F:FG(N)^{\bullet} \to FG(N)$ be an isomorphically invariant Borel function. There exists $x \in FG(N)^{\bullet}$ such that for all infinite subsequences y of x, f(y) is embeddable in a coordinate of y.

This is proved only by using axioms that go far beyond Grothendieck universes, or arbitrarily large such, etc. Furthermore, we do not have tameness in the sense that one cannot derive the consistency of ZFC + Theorem 11.5 from, say, ZFC + "there are arbitrarily large Grothendieck universes". END OF DIGRESSION.

12. 6561 cases of Boolean relation theory.

We have discovered a general class of mathematical problems that make good sense in a great variety of contexts, but carry 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

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

We find it very convenient to suppress the arity of f and use the notation fA.

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

There is a ridiculously large number of such pairs that are natural signatures of myriad areas and subareas of mathematics.

In baby BRT we consider only one function and one set. We seek to understand all statements of the following form in a fixed BRT setting (V,K):

For all $f \in V$ there exists $A \in K$ such that a given Boolean relation holds between A,fA.

"Boolean relation" comes in flavors; e.g.; in equational BRT, we mean Boolean equations. In inequational BRT, we mean Boolean inequations.

Here are some examples. Let MF(N) be the set of all functions whose domain is some N^k and whose range is a subset of N. Let SD(N) be the set of all $f \in MF(N)$ such that for all $x \in dom(f)$, $f(x) > |x|$, where | | is the sup norm. Let INF(N) be the set of all infinite subsets of N.

1. For all $f \in MF(N)$ there exists infinite $A \subseteq N$ such that $fA \neq N$. (Complementation theorem).

2. For all $f \in SD(N)$ there exists infinite $A \subseteq N$ such that $fA = N\backslash A$. (Thin set theorem).

3. Let V be the set of all linear operators on Hilbert spaces and K is the set of all nontrivial subspaces. For all $f \in V$, there exists $A \in K$ such that $fA \subseteq A$.

1 encapsulates the essence of recursion. 2 lies at the heart of the original Ramsey theorem. 3 is open (the invariant subspace problem).

THEOREM 12.1. For all f □ SD(N) there exists infinite A □ N such that fA = N\A. There is a unique A □ N such that fA = N\A.

To see existence, suppose we have determine membership of 0,1,…,r-1 in A.

Put r in A iff r □ fA so far. QED

1 and 3 lie in equational BRT. We can put 2 in equational BRT as follows:

2′. For all f □ SD(N) there exists infinite A,B □ N such that fA = B and A □ B = ∅.

We have determined the truth value of all statements in equational and inequational BRT for (MF(N),INF(N)) and (SD(N),INF(N)), with 1 function and 1 set. There are 16 statements to analyze in each of these four cases.

In adult BRT we consider k functions and n sets. Fix a BRT setting (V,K).

We seek to understand all statements of the following form:

For all $f_1,…,f_k$ □ V there exists $A_1,…,A_n$ □ K such that a given Boolean relation holds between these sets and their images under the functions.

Let f □ MF(N)., We say that f is of expansive linear growth iff there exist c,d > 1 such that for all but finitely many x □ dom(F),

$$c|x| \; □ \; f(x) \; □ \; d|x|.$$

We use X □. Y for X □ Y together with the commitment that X,Y are disjoint.

E.g.,]

$$X \; □. \; Y \; □ \; Z \; □. \; W$$

means

$$X \square\ Y \square\ Z \square\ W \square$$
$$X \square\ Y = \varnothing \square\ Z \square\ W = \varnothing.$$

Write ELG(N) for the set of all f □ MF(N) of expansive linear growth. We work in the BRT setting (ELG(N),INF(N)).

PROPOSITION 12.2. For all f,g □ ELG(N) there exists A,B,C □ INF(N) such that

$$A \square.\ fA \square\ C \square.\ gB$$
$$A \square.\ fB \square\ C \square.\ gC.$$

We have given a proof of Proposition 12.2 using certain large cardinal that go well beyond the usual axioms of ZFC. We have also shown that ZFC alone does not suffice. In fact, a little less potent large cardinals than are used in the proof do not suffice.

The large cardinals involved are called the Mahlo cardinals of finite order. These cardinals are far beyond Grothendieck universes and standard elaborations of them.

It is clear that Proposition 12.2 has a particularly simple structure compared to a typical statement in BRT. In fact, the two clauses there have the form

$$X \square.\ fY \square\ Z \square.\ gW$$
$$S \square.\ fT \square\ U \square.\ gV$$

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 BRT of cardinality $3^8 = 6561$.

We have been able to show that all of these 6561 statements are provable or refutable using the same large cardinal axioms that we use to prove Proposition 12.2 Obviously, we need the large cardinal axioms since 12.2 is among the 6561.

In fact, Proposition 12.2 is the only one of the 6561 up to symmetry that involves any logical difficulties.

Furthermore, the logical difficulties associated with Proposition 12.2 appear even in concrete forms of these 6561 cases where the functions and sets are drawn from nice countable classes of very effective functions and sets.

We think BRT is mathematically sufficiently interesting that mathematicians will develop it for its own sake, despite the necessary rethinking of the foundations for mathematics that this entails.

BRT itself is a special case of what we call “intellectual parameterization”.

We conjecture that “intellectual parameterization” will lead to a thematic expansion of mathematics where the necessary use of large cardinal axioms going well beyond the currently usual axioms for mathematics (ZFC) will become standard.