

ISSUES IN THE FOUNDATIONS OF MATHEMATICS

Harvey M. Friedman

Gödel Lecture, ASL

Las Vegas, Nevada

<http://www.math.ohio-state.edu/~friedman/>

June 2, 2002

I discuss my efforts concerning 3 crucial issues in the foundations of mathematics that are deeply connected with the great work of Kurt Gödel.

A. To what extent can set theoretic methods be used in an essential way to further the development of normal mathematics?

B. Are there fundamental principles of a general philosophical nature which can be used to give consistency proofs of set theory, including the so called large cardinal axioms?

C. To what extent, and in what sense, is the natural hierarchy of logical strengths represented by familiar systems ranging from exponential function arithmetic to $ZF + j:V \sqsupseteq V$ robust?

Our discussion of A is aimed at mathematicians; B,C at mathematicians & philosophers.

A1. HIGH SCHOOL SEQUENCES AND COLLEGE CONTINUITY.

There exists a longest sequence in 2 letters, x_1, \dots, x_n , such that no block x_i, \dots, x_{2i} is a subsequence of a later block x_j, \dots, x_{2j} . The longest length is $n(2) = 11$.

This was used as a problem for gifted high school students by Paul Sally at U. Chicago. One student proved $n(2) = 11$.

There is a longest sequence x_1, \dots, x_n in 3 letters such that no block x_i, \dots, x_{2i} is a subsequence of a later block x_j, \dots, x_{2j} . Call this longest length $n(3)$.

THEOREM A1.1. $n(1) = 3$, $n(2) = 11$, $n(3) > A_{7198}(158386)$.

Here $A_k(n)$ is the k th level of the Ackermann hierarchy (starting with $A_1 = \text{doubling}$) at n .

THEOREM A1.2. $(\exists k) (n(k) \text{ exists})$ is provable in 3 quantifier induction but not in 2 quantifier induction.

In fact, the growth rate of $n(k)$ lies just beyond the multirecursive functions.

In College Continuity, we use the usual notion of pointwise continuity for functions $f:A \rightarrow B$, where A,B are (countable) sets of real numbers.

The following statement looks like it comes from the era of classical descriptive set theory, but is new:

THEOREM A1.3. Let A,B be countable sets of real numbers. There is a one-one continuous $f:A \rightarrow B$ or a one-one continuous $g:B \rightarrow A$.

This requires a transfinite induction argument of length \aleph_1 in several senses. From the reverse math point of view:

THEOREM A1.4. A1.3 is provably equivalent to ATR_0 over RCA_0 .

This holds even for countable sets of rational numbers.

A2. FINITE TREES.

The first finite combinatorial theorem shown to be unprovable in PA appeared in 1977 by Jeff Paris and Leo Harrington.

By 1977, I had obtained some finite statements independent of even ZFC, but they had nowhere near the simplicity of PH.

At that time, my best contributions concerning independence lie in the Borel world, and are discussed below.

The ideas in PH were expected to be pushed to get the ultimate similarly natural finite statements corresponding to ZFC and beyond.

However, this remained elusive, and the ideas in PH seem insufficient to move forward significantly.

There were some limited advances (e.g., work with McAloon and Simpson), but real progress came from something unrelated to PH the celebrated theorem of J.B. Kruskal:

THEOREM A2.1. (KT). In any infinite sequence of finite trees, one tree is inf preserving embeddable into a later tree.

This was the first satisfying semifinite statement provable in ZFC but not predicatively provable. KT is not provable in ATR and corresponds to bar induction for Σ^1_2 formulas.

The original finite forms of KT involve finite sequences of finite trees, and are also predicatively unprovable:

THEOREM A2.2. (FKT). Let $n \gg k \geq 1$ and T_1, \dots, T_n be finite trees, where each T_i has at most $k+i$ vertices. Then $(\exists i < j) (T_i \text{ is inf preserving embeddable into } T_j)$.

Finite sequences of controlled growth rates provide a natural unifying method for generating finite forms from semifinite forms, such as KT. It is also a natural setting for new investigations connecting combinatorial analysis and proof theory; see recent work of Weiermann.

Despite the naturalness of FKT, 20 years went by before my discovery of finite versions involving only a single sufficiently large finite tree, whose mathematical interest can be clearly identified separately from KT.

THEOREM A2.3. Let $r \gg k, n \geq 1$, and T be an n -labeled finite perfect tree of uniform valence k and uniform height r . There is an inf, label, terminal preserving embedding from a truncation of T into a higher truncation of T .

A2.3 is also predicatively unprovable and corresponds roughly to bar induction for Σ^1_2 formulas.

The celebrated graph minor theorem of Robertson and Seymour:

THEOREM A2.4. (GMT) In every infinite sequence of finite graphs, one graph is minor included in a later one.

A2.4 cannot be proved in Σ^1_1 -CA₀, and can be proved in Σ^1_1 -CA + BI. Appropriate finite forms have been given.

A3. BOREL DETERMINACY AND REAL ANALYSIS.

My first unusual independence result was obtained in 1968 and published in 1971: Borel determinacy cannot be proved in

ZC, or even using the cumulative hierarchy up to any suitably specified countable ordinal.

At that time, D.A. Martin had only proved BD from ZFC with large cardinals. In 1974, he proved BD using the cumulative hierarchy on each countable ordinal, completing the circle.

In 1982, I found the following purely analytic form of BD.

THEOREM A3.1. Let $E \subseteq \mathbb{R}^n$ be a Borel set that is symmetric about the origin. Then E contains or is disjoint from the graph of a Borel function from \mathbb{R}^n into \mathbb{R}^n .

Like BD, A3.1 corresponds to the cumulative hierarchy on all countable ordinals.

Recently, I have found a new set of examples from real analysis that exhibit this and other incompleteness phenomena, that appear in work of the functional analysts Debs and Saint Raymond. This is discussed in section A5.

A4. BOREL DIAGONALIZATION.

In 1974, I discovered Borel diagonalization, which led to Borel statements that can be proved with large cardinals but not in ZFC.

The 1974 statements are the denials of Borel versions of "there are uncountably many real numbers". Clearly \exists a Borel diagonalizer $F: \mathbb{R} \rightarrow \mathbb{R}$.

THEOREM A4.1. There is no invariant Borel diagonalizer $F: \mathbb{R} \rightarrow \mathbb{R}$. I.e., no Borel $F: \mathbb{R} \rightarrow \mathbb{R}$ such that $\text{rng}(x) = \text{rng}(y) \implies F(x) = F(y)$, and where each $F(x)$ is off of x .

A4.1 can be proved in Z_3 but not in Z_2 .

From 1974 to the early 1980's I looked for stronger Borel diagonalization statements.

THEOREM A4.2. \exists no invariant Borel diagonalizer for any Borel equivalence relation.

A4.2 corresponds to the cumulative hierarchy on all countable ordinals.

THEOREM A4.3. Let F be an isomorphically invariant Borel function from infinite sequences of finitely generated groups into finitely generated groups. Then all of the values of F at infinite subsequences of some fixed infinite sequence are isomorphically embeddable in some term of that fixed sequence.

A4.3 is one among a complex of my Borel statements from the 80's that can be proved using a measurable cardinal but not using sharps, even if it is relativized to L . (There are sharper results).

A5. BOREL SELECTION.

Recently, we analyzed a complex of Borel statements of Debs/Saint Raymond of U. Paris. They stated them more generally with coanalytic. The incompleteness phenomena are already present with Borel. This is a new chapter in Borel independence results.

Let $S \subseteq A^2$. f is a selection for S on A iff $\text{dom}(f) = A$ and for all $x \in A$, $(x, f(x)) \in S$.

f is a selection for S iff f is a selection for S on $\text{dom}(S)$.

THEOREM A5.1. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ be Borel, and $E \subseteq \mathbb{N}^{\mathbb{N}}$ be Borel. If \square a continuous selection for S on every compact subset of E , then \square a continuous selection for S on E .

THEOREM A5.2. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ be Borel. If \square a constant selection for S on every compact set, then \square a Borel selection for S .

A5.1, A5.2 correspond to the cumulative hierarchy on all countable ordinals.

PROPOSITION A5.3. Let $S \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ be Borel. If \square a Borel selection for S on every compact set, then \square a Borel selection for S .

A5.3 is independent of ZFC, and can be forced.

A6. BOOLEAN RELATION THEORY.

Let $f: A^k \rightarrow B$ and C be a set. Write fC for the set of all values of f at elements of C .

The most primitive examples of BRT are:

THEOREM A6.1. For all $f:N^k \rightarrow N$ there exists infinite $A \subseteq N$ such that $fA \neq N$.

THEOREM A6.2. \exists strictly dominating $f:N^k \rightarrow N$, \exists infinite $A \subseteq N$ such that $fA = N \setminus A$.

A6.1 is provable in ACA but not in ACA_0 . A6.2 is provable in RCA_0 .

Observe that these assert "for all multivariate maps of a certain kind there is a set of a certain kind such that a Boolean relation holds between the set and its image under the map".

In (equational) BRT, we look at statements of the form "for all k multivariate maps of a certain kind, there exists n sets of a certain kind such that a particular Boolean equation holds between the sets and their images under the maps".

THEOREM A6.3. Consider BRT with 2 multivariate maps from N into N of expansive linear growth and 3 infinite subsets of N . Among the 2^{512} such statements (up to formal Boolean equivalence), some are provable using large cardinals but not in ZFC.

CONJECTURE. Every one of the 2^{512} can be proved or refuted using large cardinals (even Mahlo cardinals of finite order).

This conjecture seems out of reach. For about two years, I searched for an appropriate subclass of the 2^{512} for which I could establish this conjecture. In March, 2002, I found something truly unexpected.

A7. THE UNEXPECTED.

PROPOSITION A7.1. For all multivariate functions from N into N of expansive linear growth, there exist infinite $A, B, C \subseteq N$ such that

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

Here \cup indicates disjoint union. Thus \cup is the same as \cup together with the assertion that the terms in the union are disjoint.

There are $3^4 = 81$ such inclusions, and $81^2 = 6561$ ordered pairs.

Here is the truly unexpected.

THEOREM A7.2. A7.1 is provable using Mahlo cardinals of finite order but not in ZFC. **But with all other pairs of inclusions (up to symmetry), we have decidability within RCA_0 .**

B1. IS SET THEORY CONSISTENT?

To the true believer in set theory (with large cardinals), formal set theory (with large cardinals) is consistent since the axioms are true; by induction, the theorems are true. No justification is necessary.

There have been a number of attempts to informally justify (at least the consistency of) the axioms of ZFC, and also to informally justify (at least the consistency of) the axioms of ZFC with large cardinals.

My approach to this problem is to search for some clear unifying principles that stand independently of set theory and even mathematics, and then show that set theory (with large cardinals) is interpretable using these principles. The simplicity of such principles and their distance from set theory and mathematics are to be maximized.

The principles are generally given by philosophical stories, which will undoubtedly need careful modification and polish over a considerable period of time.

I regard the results discussed below as highly suggestive, but **definitely not decisive**.

I conjecture that this approach can be carried out based on a variety of common sense notions from everyday life. In fact, pushing virtually any common sense notion too far leads to contradictions, and we conjecture that there is a common way to resolve such contradictions which provides formalisms that are mutually interpretable with set theory (with large cardinals).

B2. THE EXPANDING MIND/1.

I assume a mind M that will grow more powerful, indefinitely. We let $M = M[1], M[2], M[3], \dots$, be an infinite sequence of minds, representing "critical" stages in the unending expansion of M .

One measure of the power of a mind is the unary/binary relations on N that it can define. We do not specify precisely how the minds make such definitions. Ordinary arithmetic and logical operations are available to any mind.

Also each mind can imagine the infinite sequence of successively more powerful minds under discussion, which can be used to define unary and binary relations on N . However, no mind can have access to individual unary/binary relations defined by a more developed mind. Otherwise, the two minds would define the same unary/binary relations on N .

The previous paragraph yields an appropriate comprehension axiom scheme for unary/binary relations on N defined by $M[i]$, involving the sequence $M[1], M[2], \dots$.

One mind fully dominates another if \square a binary relation on N defined by the former whose cross sections are the unary relations on N defined by the latter. I use that each $M[i+1]$ fully dominates $M[i]$.

I also use that the present/future looks the same to all $M[i]$. I.e., $M[i], M[i+1], \dots$ and $M[i+1], M[i+2], \dots$ satisfy the same appropriate formulas with parameters from N , or even parameters from the unary/binary relations on N defined by $M[i]$.

I can interpret ZFC + #'s in this philosophical story, and the philosophical story can be interpreted in ZFC + measurable cardinal. There are sharper results.

B3. THE EXPANDING MIND/2.

Here we obtain substantial strength with only two minds, M and the more powerful M^* . M has its domain of objects $d(M)$, and M^* has its domain of objects $d(M^*)$, where every object of M is an object of M^* but not vice versa. Thus $d(M^*)$ is richer than $d(M)$.

One measure of the strength of a mind is the unary/binary relations on its domain that the mind M can define. Those relations are given by mental constructions of M that output the truth value of the relation at arguments from $d(M)$. The same relation may be given by different mental constructions, as relations are extensional and constructions are intensional.

I assume that every mental construction of M is a mental construction of M^* . Its range of applicability under M is $d(M)$ and its range of applicability under M^* is $d(M^*)$.

I use a very strong form of comprehension for the unary/binary relations defined by M . M can use not only M^* but any individual unary/binary relations defined by M^* , for the purposes of defining unary/ binary relations.

I assume that M^* fully dominates M in the sense that there is a binary relation defined by M^* whose cross sections are the unary relations defined by M .

I also assume that M and M^* agree on the truth values of all appropriate statements with parameters from the objects of M and the mental constructions of M .

The interpretation power of this philosophical story lies between a proper class of Woodin cardinals and an elementary embedding from a rank $+1$ into a higher rank $+1$.

WARNING: There are basic incompatibilities between version 1 and version 2.

This story can be extended in an appropriate way to an infinite sequence of minds M, M^*, M^{**}, \dots . This leads to a philosophical story of interpretation power between n -huge cardinals and a rank into itself.

The axiom of choice is not a natural part of these stories, so we sometimes rely on work of Woodin on the interpretation of the axiom of choice in large cardinals.

C1. THE MATHEMATICAL LOGICAL UNIVERSE.

There appears to be a natural hierarchy of formal systems considered in mathematical logic.

They range from, say, EFA (exponential function arithmetic) through the largest of the large cardinal axioms.

There are plenty of interesting/natural incompatibilities (e.g., ZC versus ZF), but there does not seem to be any really interesting/natural incompatibilities in terms of interpretation power.

This suggests an underlying hidden structure of striking robustness. But how do we get at this since it is easy to construct lots of theories, no one of which is interpretable in any other, even using single axioms?

My approach to this problem is to consider only the SIMPLE first order axiomatic theories in first order predicate calculus with equality. Here theories are required to be presented as finitely many axioms together with finitely many axiom schemes.

The intention is that no matter what notion of "simple" is used, there are only finitely many simple theories (up to change of letters).

C2. SIMPLICITY CONJECTURES.

To make some formal conjectures, we choose a specific reasonable looking **experimental** context.

We consider theories T in first order predicate calculus with one binary relation and equality, given by finitely many formulas and formula schemes. The complexity is taken to be the total number of atomic formulas. For instance, consider the theory

$$(\forall z)(\forall w)(w \leq z \leftrightarrow ((z \leq x \rightarrow z = y) \leftrightarrow \varphi[z])).$$

$\varphi[z]$ indicates that φ is any formula without z free. This theory is mutually interpretable with PA, and its complexity is 4.

Note that there are only finitely many theories of any given complexity, up to change of letters.

CONJECTURE 1. Every consistent theory of complexity ≤ 4 is interpretable in ZFC. Any two which interpret EFA are interpretation comparable.

CONJECTURE 2. For small n , any two theories of complexity $\leq n$ interpreting EFA are interpretation comparable, the highest one among the consistent ones being mutually interpretable with a standard formal system of set theory. A variety of levels of the mathematical logical universe can be identified in this way.

Here is a more focused form of Conjecture 2:

CONJECTURE 3. There exists n such that every consistent theory of complexity $\leq n$ is interpretable in ZFC + \aleph_1 supercompact cardinal, and ZFC + \aleph_1 measurable cardinal is interpretable in some consistent theory of complexity $\leq n$. Among these that interpret EFA, we have interpretation comparability.

C3. SIMPLICITY IN SET THEORY.

I discuss set theory with the usual primitives $\in, =$, with the following notion of simplicity for **sentences**: the number of quantifiers.

Schematic letters are not needed here since we are in the set theory context.

I came across the following statement in class theory:

Every proper transitive class has a four element chain.

I.e., there are four elements of the class that form a chain under proper inclusion.

This is independent of MKC, and equivalent to "On is a subtle cardinal" over VBC.

Here is the purely set theoretic formulation:

The transitive sets with no four element chains form a set.

This is equivalent to ZFC + a subtle cardinal.

In fact, the rank and cardinality of this extremely elementary set is the first subtle cardinal.

The set theoretic version has 7 quantifiers, but there is a modification that has 6 quantifiers and is equivalent to "there are arbitrarily large subtle cardinals" over ZFC. This is the simplest known independence result from ZFC in terms of the # of quantifiers in primitive notation.

There is a paper by Daniel Gogol from the late 70's claiming that all 3 quantifier sentences are decided in ZFC, with admittedly lots of details missing.

I can supply the details, and a very small fragment of ZFC suffices.

I conjecture that all 4 quantifier sentences are provable or refutable in ZFC, and all 6 quantifier sentences are provable or refutable in ZFC + "there are arbitrarily large subtle cardinals".

I conjecture that, in the presence of ZFC, we have interpretation comparability among the 9 quantifier sentences, and the highest among the consistent ones is mutually interpretable with a set theory representing one of the highest levels of the large cardinal hierarchy.

I conjecture that a more detailed stratification of the mathematical logical universe arises when one considers not only the count on the quantifiers but also the number of atomic formulas. Our 6,7 quantifier examples have a particularly small number of atomic formulas.

Under any of these reasonable complexity measures, at some point, utter chaos sets in via unabashed Gödel coding, but when and in what sense? In the low teens?

I conjecture that all incremental roads from the immediately obvious to the inconsistent pass through the large cardinal hierarchy and then through logical chaos.

REFERENCES

HIGH SCHOOL SEQUENCES

HMF, Long finite sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

COLLEGE CONTINUITY

HMF, Metamathematics of comparability, to appear in Reverse Mathematics, ed. Simpson, <http://www.math.ohio-state.edu/~friedman/>

FINITE TREES

S.G. Simpson, Nonprovability of certain combinatorial properties of finite trees, in: Harvey Friedman's Research on the Foundations of Mathematics, ed. Harrington, Morley, Scedrov, Simpson, 1985, 87-117.

HMF, N. Robertson, P. Seymour, The Metamathematics of the Graph Minor Theorem, Logic and Combinatorics, ed. S. Simpson, AMS Contemporary Mathematics Series, vol. 65, 1987, 229-261.

HMF, Internal finite tree embeddings, in: Reflections on the Foundations of Mathematics: Essays in honor of Solomon Feferman, ed. Wilfried Sieg, Richard Sommer, Carolyn Talcott, Association for Symbolic Logic, pp. 62-93, 2002. (Was supposed to be in libraries by now, but is late).
<http://www.math.ohio-state.edu/~friedman/>

BOREL DETERMINACY

HMF, Higher Set Theory and Mathematical Practice, Annals of Math. Logic, Vol. 2, No. 3, (1971), pp. 325-357.

BOREL DIAGONALIZATION

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

Lee Stanley, Borel diagonalization and abstract set theory: recent results of Harvey Friedman, in: Harvey Friedman's Research on the Foundations of Mathematics, ed. Harrington, Morley, Scedrov, Simpson, 1985, 11-86.

BOREL SELECTION

HMF, Selection for Borel relations,
<http://www.mathpreprints.com/math/Preprint/show/>, Proceedings of Logic Colloquium '01, to appear. <http://www.math.ohio-state.edu/~friedman/>

BOOLEAN RELATION THEORY

HMF, Boolean relation theory notes
7 October 2001 <http://www.math.ohio-state.edu/~friedman/>

HMF, Lecture notes on baby Boolean relation theory, 3 October 2001 <http://www.math.ohio-state.edu/~friedman/>

THE UNEXPECTED

HMF, FOM email list, 126:Correction, 3/9/02, 2:10AM

<http://www.math.psu.edu/simpson/fom/postings/0203/msg00019.html>

SIMPLICITY IN SET THEORY

HMF, Primitive Independence Results, 25 October 2001, to appear in JML. <http://www.math.ohio-state.edu/~friedman/>