SEARCH FOR CONSEQUENCES

by
Harvey M. Friedman
Ohio State University
LC '06
Nijmegen, Netherlands
Delivered August 2, 2006
Edited August 9, 2006

NOTE: This is an edited version of my lecture at LC '06. It differs from my earlier lecture at the Gödel Centenary in Vienna, April 29, 2006 most notably in section 5, where "Finite Graph Theory" is replaced by "Order Calculus".

1. GENERAL REMARKS.

I would like to open with the same general remarks that I delivered at the Gödel Centenary meeting in Vienna a few months ago.

Gödel's legacy is still very much in evidence. It must be noted that a careful analysis reveals that his great insights raise more issues than they resolve. The Gödel legacy practically begs for renewal and expansion at a fundamental level.

When I entered the field some forty years ago, I seized on one glaring opportunity for renewal and expansion. The independence results from ZFC and significant fragments lied in a very narrow range, and had systemic features that are glaringly unrepresentative of mathematics and mathematical subjects generally.

This state of affairs suggests obvious informal conjectures to the effect that there are severe systemic limitations to the incompleteness phenomena, culminating in informal conjectures to the effect that, in principle, there is no relevance of set theoretic methods to "genuine" mathematical activity.

Now, there is no question that this central aspect of

Gödel's legacy, incompleteness, will diminish over time if such informal conjectures are not addressed in a substantial way. I have devoted a major part of my efforts over forty years to this endeavor.

I view this effort as part of a perhaps slow but steady evolutionary process. I have every confidence that this process will steadily continue in a striking manner for the foreseeable future.

EXOTIC CONJECTURE

Every interesting mathematical theorem can be recast as one among a natural finite set of statements, all of which can be decided using well studied extensions of ZFC, but not within ZFC itself.

The recasting of mathematical theorems as elements of natural finite sets of statements represents an inevitable general expansion of mathematical activity. This applies to any standard mathematical context. This program has been carried out, to a very limited extent, by BRT - and hopefully soon by Order Calculus. Some details are below.

2. WQO THEORY.

Wqo theory is a branch of combinatorics which has proved to be a fertile source of deep metamathematical pheneomena.

A qo (quasi order) is a reflexive transitive relation $(A,\leq)$. A wqo (well quasi order) is a qo $(A,\leq)$ such that for all $x_1,x_2,\ldots$ from A, $\exists$ $i < j$ such that $x_i \leq x_j$.

Highlights of wqo theory: that certain qo's are wqo's.

J.B. Kruskal treats finite trees as finite posets, and studies the qo

$\exists$ an inf preserving embedding from T_1 into T_2.

THEOREM 2.1. (J.B. Kruskal). The above qo of finite trees as posets is a wqo.

We observed that the connection between wqo's and well orderings can be combined with known proof theory to establish independence results.

The standard formalization of "predicative mathematics" is due to Feferman/Schutte = FS. Poincare, Weyl, and others railed against impredicative mathematics.

THEOREM 2.2. Kruskal's tree theorem cannot be proved in FS.

KT goes considerably beyond FS, and an exact measure of KT is known through published work of Rathjen/Weiermann.

Kruskal actually considered finite trees whose vertices are labeled from a wqo $\leq^*$. The additional requirement on embeddings is that

$$\text{label}(v) \leq^* \text{label}(h(v)).$$

THEOREM 2.3. (J.B. Kruskal). The qo of finite trees as posets, with vertices labeled from any given wqo, is a wqo.

Labeled KT is considerably stronger, proof theoretically, than KT, even with only 2 labels, $0 \leq 1$. I have not seen a metamathematical analysis of labeled KT.

Note that KT is a Π^1_1 sentence and labeled KT is a Π^1_2 in the hyperarithmetic sets.

THEOREM 2.4. Labeled KT does not hold in the hyperarithmetic sets. In fact, RCA_0 + KT implies ATR_0.

It is natural to impose a growth rate in KT in terms of the number of vertices of T_i.

COROLALRY 2.5. (Linearly bounded KT). Let $T_1,T_2,...$ be a linearly bounded sequence of finite trees. $\exists$ $i < j$ such that T_i is inf preserving embeddable into T_j.

COROLLARY 2.6. (Computational KT). Let $T_1,T_2,...$ be a sequence of finite trees in a given complexity class. There exists $i < j$ such that T_i is inf preserving embeddable into T_j.

Note Corollary 2.6 is Π^0_2.

THEOREM 2.7. Corollary 2.5 cannot be proved in FS. This holds even for linear bounds with nonconstant coefficient 1.

THEOREM 2.8. Corollary 2.6 cannot be proved in FS, even for linear time, logarithmic space.

By an obvious application of weak Konig's lemma, Corollary 2.5 has very strong uniformities.

THEOREM 2.9. (Uniform linear-ly bounded KT). Let $T_1,T_2,...$ be a linearly bounded sequence of finite trees. There exists $i < j \leq n$ such that T_i is inf preserving embeddable into T_j, where n depends only on the given linear bound, and not on the trees $T_1,T_2,...$.

With this kind of strong uniformity, we can obviously strip the statement of infinite sequences of trees.

For nonconstant coefficient 1, we have:

THEOREM 2.10. (finite KT). Let n >> k. For all finite trees $T_1,...,T_n$ with each $|T_i| \leq i+k$, there exists $i < j$ such that T_i is inf preserving embeddable into T_j.

Since Theorem 2.10 → Theorem 2.9 → Corollary 2.5 (nonconstant coefficient 1), we see that Theorem 2.10 is not provable in FS.

Other Π^0_2 forms of KT involving only the internal structure of a single finite tree can be found in the Feferfest volume.

I proved analogous results for EKT = extended Kruskal theorem, which involves a finite label set and a gap embedding condition. Only here the strength jumps up to that of Π^1_1-CA_0.

I said that the gap condition was natural (i.e., EKT was natural). Many people were unconvinced.

Soon later, EKT became a tool in the proof of the famous graph minor theorem of Robertson/Seymour.

THEOREM 2.11. Let $G_1,G_2,...$ be finite graphs. There exists $i < j$ such that G_i is minor included in G_j.

I then asked Robertson/ Seymour to prove a form of EKT that I knew implied full EKT, just from GMT. They complied, and we wrote a triple paper.

The upshot is that GMT is not provable in Π^1_1-CA_0. Just where GMT is provable is unclear, and recent discussions with Robertson have not stabilized. I disavow remarks in the triple paper about where GMT can be proved.

An extremely interesting consequence of GMT is the subcubic graph theorem. A subcubic graph is a graph where every vertex has valence ≤ 3. (Loops and multiple edges are allowed).

THEOREM 2.12. Let $G_1,G_2,\ldots$ be subcubic graphs. There exists $i < j$ such that G_i is embeddable into G_j as topological spaces (with vertices going to vertices).

Robertson/Seymour also claims to be able to use the subcubic graph theorem for linkage to EKT. Therefore the subcubic graph theorem (even in the plane) is not provable in Π^1_1-CA_0.

We have discovered lengths of proof phenomena in wqo theory. We use Σ^0_1 sentences.

*) Let $T_1,\ldots,T_n$ be a sufficiently long sequence of trees with vertices labeled from $\{1,2,3\}$, where each $|T_i| \leq i$. There exists $i < j$ such that T_i is inf and label preserving embeddable into T_j.

**) Let $T_1,\ldots,T_n$ be a sufficiently long sequence of subcubic graphs, where each $|T_i| \leq i+13$. There exists $i < j$ such that G_i is homeomorphically embeddable into G_j.

THEOREM 2.13. Every proof of *) in FS uses at least $2^{[1000]}$ symbols. Every proof of **) in Π^1_1-CA_0 uses at least $2^{[1000]}$ symbols.

Andreas Weiermann and his colleagues have been vigorously pursuing striking “threshold” or “phase transition” phenomena surrounding finite KT (Theorem 2.10 above) and many other combinatorial statements. In finite KT, for fixed k, i+k is a linear function. I.e., the functions f(i) = i+k form a class of functions used for finite KT. For a given class of functions, appropriately presented, we can ask about the metamathematical status of finite KT based on these functions. The results tell us that if the class of functions represent a growth rate below (above) a certain threshold growth rate, then finite KT (or the combinatorial statement being treated) is provable (unprovable) in a relevant formal system.

3. BOREL SELECTION.

Let S $\subseteq \mathfrak{R}^2$ and E $\subseteq \mathfrak{R}$. A selection for A on E is a function f:E $\rightarrow \mathfrak{R}$ whose graph is contained in S.

A selection for S is a selection for S on $\mathfrak{R}$.

We say that S is symmetric if and only if S(x,y) $\leftrightarrow$ S(y,x).

THEOREM 3.1. Let S $\subseteq \mathfrak{R}^2$ be a symmetric Borel set. Then S or $\mathfrak{R}^2$\S has a Borel selection.

My proof of Theorem 3.1 relied heavily on Borel determinacy, due to D.A. Martin.

THEOREM 3.2. Theorem 3.1 is provable in ZFC, but not without the axiom scheme of replacement.

There is another kind of Borel selection theorem that is implicit in work of Debs and Saint Raymond of Paris VII. They take the general form: if there is a nice selection for S on compact subsets of E, then there is a nice selection for S on E.

THEOREM 3.3. Let S $\subseteq \mathfrak{R}^2$ be Borel and E $\subseteq \mathfrak{R}$ 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.

THEOREM 3.4. Let S $\subseteq \mathfrak{R}^2$ be Borel and E $\subseteq \mathfrak{R}$ 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.

THEROEM 3.5. Theorem 3.3 is provable in ZFC but not without the axiom scheme of replacement. Theorem 3.4 is neither provable nor refutable in ZFC.

We can say more.

THEOREM 3.6. The existence of the cumulative hierarchy up through every countable ordinal is sufficient to prove

Theorems 3.1 and 3.3. However, the existence of the cumulative hierarchy up through any suitably defined countable ordinal is not sufficient to prove Theorem 3.1 or 3.3.

DOM: The $f:N \to N$ constructible in any given $x \subseteq N$ are eventually dominated by some $g:N \to N$.

THEOREM 3.7. ZFC + Theorem 3.4 implies DOM (H. Friedman). ZFC + DOM implies Theorem 3.4 (Debs/Saint Raymond).

4. BOOLEAN RELATION THEORY.

We begin with two examples of statements in BRT of special importance for the theory.

THIN SET THEOREM. Let $k \geq 1$ and $f:N^k \to N$. There exists an infinite set $A \subseteq N$ such that $f[A^k] \neq N$.

COMPLEMENTATION THEOREM. Let $k \geq 1$ and $f:N^k \to N$. Suppose that for all $x \in N^k$, $f(x) > \max(x)$. There exists an infinite set $A \subseteq N$ such that $f[A^k] = N\backslash A$.

These two theorems are official statements in BRT. In the complementation theorem, A is unique.

We now write them in BRT form.

THIN SET THEOREM. For all $f \in MF$ there exists $A \in INF$ such that $fA \neq N$.

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N\backslash A$.

The thin set theorem lives in IBRT in A,fA. There are only $2^{2\hat{}2} = 16$ statements in IBRT in A,fA. These are easily handled.

The complementation theorem lives in EBRT in A,fA. There are only $2^{2\hat{}2} = 16$ statements in IBRT in A,fA. These are easily handled.

For EBRT/IBRT in A,B,C,fA,fB,fC,gA,gB,gC, we have $2^{2\hat{}9} = 2^{512}$ statements. This is entirely unmanageable. It would take several major new ideas to make this manageable.

DISCOVERY. There is a statement in EBRT in A,B,C,fA,fB, fC,gA,gB,gC that is independent of ZFC. It can be proved in MAH+ but not in MAH. In fact, it cannot be proved in MAH + V = L.

Here MAH+ = ZFC + "for all n there exists a strongly n-Mahlo cardinal". MAH = ZFC + $\{$there exists a strongly n-Mahlo cardinal$\}_n$.

The particular example is far nicer than any "typical" statement in EBRT in A,B,C,fA,fB,fC,gA,gB,gC. However, it is not nice enough to be regarded as suitably natural.

Showing that all such statements can be decided in MAH+ seems to be too hard.

What to do? Look for a natural fragment of full EBRT in A,B,C,fA,fB,fC,gA,gB,gC that includes the example, where I can decide all statements in the fragment within MAH+.

Also look for a bonus: a striking feature of the classification that is itself independent of ZFC.

Then we have a single natural statement independent of ZFC.

In order to carry this off, we use somewhat different functions.

We use ELG = expansive linear growth.

These are functions $f:N^k \to N$ such that there exist constants $c,d > 1$ such that

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

holds for all but finitely many $x \in N^k$.

TEMPLATE. For all $f,g \in$ ELG there exist $A,B,C \in$ INF such that

$$X \,\dot{\cup}\, fY \subseteq V \,\dot{\cup}\, gW$$
$$P \,\dot{\cup}\, fR \subseteq S \,\dot{\cup}\, gT.$$

Here X,Y,V,W,P,R,S,T are among the three letters A,B,C.

Note that there are 6561 such statements. We have shown that all of these statements are provable or refutable in RCA_0, with exactly 12 exceptions.

These 12 exceptions are really exactly one exception up to the obvious symmetry: permuting A,B,C, and switching the two clauses.

The single exception is the **exotic case**

PROPOSITION A. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

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

This statement is provably equivalent to the 1-consistency of MAH, over ACA'.

If we replace "infinite" by "arbitrarily large finite" then we can carry out this second classification entirely within RCA_0.

Inspection shows that all of the nonexotic cases come out with the same truth value in the two classifications, and that is of course provable in RCA_0.

Furthermore, the exotic case comes out true in the second classification.

THEOREM 4.1. The following is provable in MAH+ but not in MAH (or even MAH + V = L). An instance of the Template holds if and only if in that instance, "infinite" is replaced by "arbitrarily large finite".

From the Introduction, recall

EXOTIC CONJECTURE

Every interesting mathematical theorem can be recast as one among a natural finite set of statements, all of which can be decided using well studied extensions of ZFC, but not within ZFC itself.

Theorem 4.1 as it stands is not exactly a case of this Exotic Conjecture, as the Exotic Case (Proposition A) is not a mathematical theorem. It can also be criticized as being too ad hoc to be interesting.

However, consider the considerably more natural statements:

THEOREM I. For all $f,g \in ELG$ there exist $A,B \in INF$ such that

$$A \cup. fA \subseteq B \cup. gB.$$

THEOREM II. For all $f,g \in ELG$ there exist $A,B,C \in INF$ such that

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

These are both Theorems of RCA_0.

We could start from any one or both of these mathematical theorems and then embed them into our class of 6561 statements in order to provide an instance of this Exotic Conjecture.

We freely admit that this is not a very satisfactory instance of this Exotic Conjecture, and is certainly poor evidence for it. Nevertheless we believe in this Exotic Conjecture.

5. ORDER CALCULUS.

There is a well known theorem in graph theory, with many essentially equivalent formulations. It is really our complementation theorem in a graph theory setting.

THEOREM 5.1. In any finite dag G there exists $A \subseteq V(G)$ such that $GA = A'$. Furthermore, A is unique.

Here GA is the set of all heads of edges in G whose tail lies in A, and $A' = V(G)\backslash A$.

According to Steve Hedetniemi hedet@cs.clemson.edu,

"A is what is called a solution in digraph theory, and if you reverse all arcs, you get the well-known *kernel*. In our book Fundamentals of Domination in Graphs, by T.W. Haynes, S.T. Hedetniemi and P.J. Slater, Marcel Dekker, 1998, we have a 1,224 entry bibliography in the back. This bibliography must contain about 100 papers on kernels in graphs."

We will instead use ordinary relation notation, and take this in a purely order theoretic direction.

Let $R \subseteq [1,n]^k \times [1,n]^k$. We think of R as the digraph G whose vertex set is $[1,n]^k$, and whose edges are the elements of R.

For $A \subseteq [1,n]^k$, we write $RA = \{y: (\exists x \in A)(R(x,y))\}$. Note that RA is the same as the GA used above.

We say that R is strictly dominating iff $R(x,y) \rightarrow \max(x) < \max(y)$.

Note that if R is strictly dominating then the corresponding digraph G is obviously a dag.

THEOREM 5.2. For all $n,k \geq 1$ and strictly dominating $R \subseteq [1,n]^k \times [1,n]^k$, there exists $A \subseteq [1,n]^k$ such that $RA = A'$. Furthermore, A is unique.

We say that $B \subseteq [1,n]^k$ is order invariant iff for all order equivalent $x,y \in [1,n]^k$, $x \in B$ iff $y \in B$.

We state the weakened order invariant form of Theorem 5.2.

THEOREM 5.3. For all $n,k \geq 1$ and strictly dominating order invariant $R \subseteq [1,n]^k \times [1,n]^k$, there exists $A \subseteq [1,n]^k$ such that $RA = A'$. Furthermore, A is unique.

We now make our fundamental informal move.

INFORMAL. For all $n,k \geq 1$ and strictly dominating order invariant $R \subseteq [1,n]^k \times [1,n]^k$, there exists $A \subseteq [1,n]^k$ such that RA and A' are related.

Let $B,C \subseteq [1,n]^k$ and α,β be finite sequences from $[1,n]$. We say that B,C are lower triple equivalent from α to β iff

$$(\forall x,y,z \in B \cup C)(\exists u,v,w \in B \cap C)$$
$$((x,y,z,\alpha),(u,v,w,\beta) \text{ are order equivalent and}$$
$$\min(x,y,z,\alpha,\beta) \geq \min(u,v,w,\alpha,\beta)).$$

PROPOSTION A. For all n >> k and strictly dominating order invariant $R \subseteq [1,4n]^k \times [1,4n]^k$, there exists $A \subseteq [1,3n]^k$ such that RA,A' are lower triple equivalent from n,2n to 2n,3n, and from 2n,3n to n,2n.

PROPOSTION B. For all n >> k and strictly dominating order invariant $R \subseteq [1,5n]^k \times [1,5n]^k$, there exists $A \subseteq [1,3n]^k$ such that RA,A' are lower triple equivalent from n,2n,3n to 2n,3n,4n, and from 2n,3n,4n to n,2n,3n.

PROPOSITION C. For all n >> k,p and strictly dominating order invariant $R \subseteq [1,pn]^k \times [1,pn]^k$, there exists $A \subseteq [1,pn]^k$ such that RA,A' are lower triple equivalent from n,2n,...,pn-2n to 2n,3n,...,pn-n, and from 2n,3n,...,pn-n to n,2n,...,pn-2n.

THEOREM 5.4. The following is provable in EFA. Proposition A implies Con(ZFC + "there exists a totally indescribable cardinal") and is implied by Con(ZFC + "there exists a subtle cardinal"). Proposition B implies Con(ZFC + “there exists a subtle cardinal”) and is implied by Con(ZFC +”there exists a 2 subtle cardinal”). Proposition C is equivalent to Con(SUB).

Here SUB = ZFC + $\{\text{there exists an n subtle cardinal}\}_n$.

Note that Propositions A-C are only explicitly Π^0_3. They can be put into an equivalent explicitly Π^0_1 form by eliminating n in favor of an expression in k,m (and k,m,p) as follows.

PROPOSITION A'. For all $n \geq (8k)!$ and strictly dominating order invariant $R \subseteq [1,4n]^k \times [1,4n]^k$, $\exists A \subseteq [1,3n]^k$ such that RA,A' are lower triple equivalent from n,2n to 2n,3n, and from 2n,3n to n,2n.

PROPOSITION B'. For all $n \geq (8k)!$ and strictly dominating order invariant $R \subseteq [1,5n]^k \times [1,5n]^k$, $\exists A \subseteq [1,4n]^k$ such that RA,A' are lower triple equivalent from n,2n,3n to 2n,3n,4n, and from 2n,3n,4n to n,2n,3n.

PROPOSITION C'. For all $n \geq (8kp)!$ and strictly dominating order invariant $R \subseteq [1,pn]^k \times [1,pn]^k$, $\exists A \subseteq [1,pn]^k$ such that RA,A' are lower triple equivalent from n,2n,...,pn-2n to 2n,3n,...,pn-n, and from 2n,3n,...,pn-n to n,2n,...,pn-2n.

We now come to plans for Templating these Propositions. Recall the successful Templating of Proposition A by the 6561 statement Template above in section 4.

We haven't yet worked on any of these Templating plans. Nevertheless, we think that it is informative to present them.

To begin with, we can use an arbitrary list of pairs of tuples of multiples of n.

TEMPLATE I. For all n >> k,p and strictly dominating order invariant $R \subseteq [1,pn]^k \times [1,pn]^k$, there exists $A \subseteq [1,p]^k$ such that RA,A' are lower triple equivalent from α_1 to β_1, from α_2 to β_2, ..., from α_q to β_q. Here p,q are specific positive integers, and the α's and β's are finite tuples from {n,2n,...,pn}.

We at least know that Template I holds if and only if for all i, αi and βi have the same order type, and the entry pn occurs in the same positions. What remains to be seen is just what the logical strength is of each statement.

We can also use various Boolean combinations of A and RA.

TEMPLATE II. For all n >> k,p and strictly dominating order invariant $R \subseteq [1,pn]^k \times [1,pn]^k$, there exists $A \subseteq [1,pn]^k$ such that $B_1(A,RA),B_1'(A,RA)$ are lower triple equivalent from α1 to β1, $B_1(A,RA),B_1'(A,RA)$ are lower triple equivalent from α2 to β2, ..., $B_q(A,RA),B_q'(A,RA)$ are lower triple equivalent from α_q to β_q,. Here p,q are specific positive integers, the α's and β's are finite tuples from {n,2n,...,pn}, and the $B_1(A,RA),B_2(A,RA)'$ are specific Boolean combinations of A,RA.

This should be fully analyzable. Considerably more ambitious would be to allow the following wider class of compound Boolean expressions in A,R. These are defined inductively by

i. A is an expression.
ii. Boolean combinations of expressions are expressions.
iii. R(X) is an expression if X is an expression.

Thus we arrive at

TEMPLATE III. For all n >> k,p and strictly dominating order invariant $R \subseteq [1,pn]^k \times [1,pn]^k$, there exists $A \subseteq [1,pn]^k$ such that $B_1(A,RA),B_1'(A,RA)$ are lower triple equivalent from α_1 to β_1, $B_1(A,RA),B_1'(A,RA)$ are lower triple equivalent from α_2 to β_2, ..., $B_q(A,RA),B_q'(A,RA)$ are lower triple equivalent from α_q to β_q,. Here p,q are specific positive integers, the α's and β's are finite tuples from {n,2n,...,pn}, and the $B_1(A,RA),B_2(A,RA)'$ are specific compound Boolean combinations of A,RA.

Much more ambitious Templates arise by asking for more than one set A. We can ask for sets $A_1,...,A_t$ such that some set of lower triple equivalences holds between various pairs of Boolean combinations of $A_1,...,A_t$, $R(A_1),...,R(A_t)$ on various sets of multiples of n. We can even use compound Boolean combinations of $A_1,...,A_k$,R.

We can even go much much further by considering more than one strictly dominating order invariant R.

A whole new dimension of difficulty arises when we wish to template the definition of

B,C are lower triple equivalent from α to β.

Recall that this takes the $\forall\exists$ form

$$(\forall x,y,z \in B \cup C)(\exists u,v,w \in B \cap C)$$
$$((x,y,z,\alpha),(u,v,w,\beta) \text{ are order equivalent and}$$
$$\min(x,y,z,\alpha,\beta) \geq \min(u,v,w,\alpha,\beta)).$$

We can replace $B \cup C$, and $B \cap C$, by various Boolean combinations of B,C. We can replace $\geq$ by >,<,=, and use various patterns of the letters x,y,z,u,v,w,α,β and allow multiple clauses inside the quantifier free part. We can also allow multiple $\forall\exists$ sentences of this form, taken conjunctively. We can, of course, use two sets of variables, each of finite cardinalities other than 3 each, and also more Greek variables.

Furthermore, we can combine the previous paragraph with the earlier Templating ideas.

As above, these Templates are, technically speaking, Π^0_3 Templates. However, we can appropriately replace n >> k,t with $n \geq (8kt)!$ and obtain Π^0_1 Templates. I.e., each instance is a Π^0_1 sentence. (Here t represents the size of the conclusion statement).