SHOCKING(?) UNPROVABILITY

by
Harvey M. Friedman
OSU Math Dept
Columbus, Ohio
April 16, 2010

1. WHAT KIND OF SHOCK?
2. GENERAL THESIS.
3. BASES AND KERNELS.
4. LOCAL BASES.
5. LOCAL BASIS CONSTRUCTIONS.
6. POLYNOMIALS AND LOWER YIELDS.
7. INFINITARY LOCAL BASIS CONSTRUCTION THEOREMS.
8. FINITARY LOCAL BASIS CONSTRUCTION THEOREMS.
9. ORDER INVARIANT LOCAL BASIS CONSTRUCTION THEOREMS.
10. UPPER SHIFT LOCAL BASIS THEOREM ON Q^k.

The work reported on here is ultimately aimed at the working mathematician who is not particularly concerned with issues in the foundations of mathematics.

We have maintained a variety of contacts with working mathematicians inside and outside OSU.

We wish to acknowledge the highly valuable feedback I have obtained in recent years from Ovidiu Costin (analysis) and Stephen Milne (combinatorics/number theory) from our Department.

WHAT KIND OF SHOCK?

Mathematical Logic had a glorious period in the 1930s, which was briefly rekindled in the 1960s. Any Shock Value, such as it is, has surrounded unprovability from ZFC.

These unprovability results had some shock value:

1. “ZFC is free of contradiction” is not provable in ZFC. (Goedel 1930s).
2. “Every uncountable set of reals is in one-one correspondence with the set of all real numbers” is not refutable in ZFC (Goedel 1930s).
3. “Every uncountable set of reals is in one-one correspondence with the set of all real numbers” is not provable in ZFC (Cohen, 1960s).

Since then, there have been unprovability results from ZFC more connected with mathematics, but entirely on the set theoretic side of mathematics. Old Shock Value has long since worn off.

It is essential for logic to expand unprovability from ZFC into the finite - and ultimately to familiar, beautiful, and essential finite contexts.

I have been trying to do this for about 100,000 hours over about 40 years. On occasion, I make a report. It is almost always quickly replaced by a major improvement. Today is going to be no exception.

GENERAL THESIS

There appears to be a general concept of an inductive construction of a structure satisfying constraints. The constraints are to be met at any stage. Each relevant object is processed only after all of the relevant objects have been previously processed.

However, we can attempt to radically alter the construction so that objects are processed at a given stage well before relevant objects have been processed. The multiple objects processed at a given stage will include all objects built out of the previously processed objects, regardless of whether we are really ready to know what to do with them with any confidence.

It is not at all clear how we can carry out such a construction meeting the constraints - except for one method.

The method is to first make the ordinary inductive construction, where everything is clear, and then use the resulting completed construction to tell us what to do in the altered construction.

The story continues.

Symmetry properties for the construction are immediately suggested when we, for instance, process all k-tuples from a set of integers.

GENERAL THESIS

Symmetry properties for the construction are immediately suggested, even at the first stage, when we process all k-tuples from a set of integers.

These symmetry properties occur when applying nice functions in mathematics - e.g., piecewise polynomials with nonnegative integer coefficients.

However, some of these strong symmetry properties fail in any structure satisfying the constraints. Therefore, we cannot obtain these strong symmetry properties if we are going to perform the construction indefinitely. We will necessary run into an obstruction.

HOWEVER, the question remains as to whether we can at least continue the construction for a given finite number of stages, with the strong symmetry at the first stage, and satisfying the constraints.

This question is answered in the affirmative - but there is no proof of this fact in ZFC. Large Cardinals are sufficient to give the proofs.

BASES AND KERNELS

Bases for binary relations and Kernels for digraphs are really the same thing. We will talk about both.

N = nonnegative integers. Fix R $\subseteq$ $N^k \times N^k$.

For our purposes, we think of the relation

$$x \; R \; y \text{ and } \max(x) > \max(y)$$

as asserting that "y is a reduction of x".

NOTE: We emphasize that we are NOT requiring that R, or the above reduction relation, be transitive.

Note that we cannot keep reducing forever, because we are lowering the max.

A basis for R is a set A $\subseteq$ N^k such that

i. Every element of N^k is either in A or has a reduction in A.
ii. No element of A has a reduction in A.

If R is transitive, then the obvious basis is the set of all R minimal elements. Things are not so transparent if R is not transitive.

BASES AND KERNELS

THEOREM. Every $R \subseteq N^k \times N^k$ has a unique basis.

We can prove this directly, or derive it from Kernel digraph theory.

A digraph is a pair (V,E), where V is the set of vertices, and E contained in V^2 is the set of edges.

We say that S is a kernel of G = (V,E) if and only if

i. $S \subseteq V$.
ii. There is no edge (x,y), $x,y \in S$.
iii. For all $x \in V \backslash S$, there is an edge (x,y), $y \in S$.

A dag is a directed acyclic graph.

THEOREM. von Neumann. Every finite dag has a unique kernel.

Proof: First enumerate the vertices of the finite dag $v_1,...,v_n$, without repetition, such that every edge points from a vertex to an earlier vertex. Now perform the following inductive construction. Suppose we have determined membership of $v_1,...,v_i \in S$, $i \geq 0$. Put v_{i+1} in S if and only if there is no edge from v_{i+1} to a vertex already in S. If there are two kernels, the first v_i at which they differ provides the required contradiction. QED

BASES AND KERNELS

THEOREM. Every digraph with no infinite path has a unique kernel.

Proof: We can form a transfinite sequence of vertices without repetition where every edge goes from a vertex to an earlier vertex. Then perform the same construction of a kernel by transfinite induction. QED

COROLLARY. Every $R \subseteq N^k \times N^k$ has a unique basis.

Proof: Turn this into digraph theory by defining $G = (N^k,E)$, where (x,y) in E if and only if x R y and max(x) > max(y). Now apply the above Theorem. QED

LOCAL BASES

Let $R \subseteq N^k \times N^k$ and $E \subseteq N$.

A basis for $R|E$ is a set $A \subseteq E^k$ such that

i. Every element of E^k is either in A or has a reduction in A.
ii. No element of A has a reduction in A.

THEOREM 2.1. For all $R \subseteq N^k \times N^k$ and $E \subseteq N$, there is a unique basis for $R|E$.

The various bases for the $R|E$, $E \subseteq N$, are called the local bases of R.

The constructions that we now focus on are constructions of Local Bases.

LOCAL BASIS CONSTRUCTIONS

Fix $R \subseteq N^k \times N^k$. We now introduce a particular kind of natural construction that builds a local basis for R. That is, if the construction is successfully continued for infinitely many steps, it will yield a local basis for R.

We start with nonempty $E \subseteq N$.

We now build $A_1 \subseteq N^k$ as follows. For each $x \in E^k$, put x^* in A_1, where $x^* = x$ or x^* is a reduction of x. Now check to make sure that A_1 is free. If so, then we can continue the construction. If not, then the construction is blocked.

Suppose $A_1,...,A_i$ have been built, $i \geq 1$. We build $A_{i+1} \subseteq N^k$, as follows. For each $x \in (E \cup fld(A_1) \cup ... \cup fld(A_i))^k$, put $x \in A_{i+1}$, or put a reduction of x in A_{i+1}. Check to make sure that $A_1 \cup ... \cup A_{i+1}$ is free.

Suppose this construction can be carried out for infinitely many steps. Let A be the union of the A_i. Then obviously A is a basis for $R|fld(A)$, and $E \subseteq fld(A)$. In particular, A is a local basis for R.

LOCAL BASIS CONSTRUCTIONS

Suppose that we carry out the construction to $A_1,...,A_p$, $p \geq 1$, where we check that A_1 **U** ... **U** A_p is free - and then quit of our own free will. Then we say that the construction has length p.

We use E for the initial set. We can think of the first stage in the construction as a function from E^k into N^k given by the * operation above. I.e., each x* is either x or a reduction of x - in any case, x* is thrown into A_1.

TEMPLATE. Every $R \subseteq N^k \times N^k$ has a local basis construction of any given finite length where the first stage in the construction has nice symmetry properties.

We aim for a complete understanding of all instances of this Template. We know that certain simple symmetry properties arise from applying piecewise polynomials with coefficients from N. This does motivate the simple symmetry properties chosen. Unfortunately, it appears that piecewise polynomials with coefficients from N give us some symmetry properties that make the Template false.

NEWS FLASH!!!

See various refinements and extensions of the work reported here in our abstracts on the FOM email list at http://www.cs.nyu.edu/pipermail/fom/

POLYNOMIALS AND LOWER YIELDS

Even though we are getting the right kind of complete description of the symmetry properties, we still want to have some striking examples of symmetry properties that we can realize in local basis constructions, but only if we go way beyond the ZFC axioms.

Let $f:E^k \to N^k$. The lower yield of E consists of the set of all coordinates of values of f that are less than min(E).

More generally, the lower yield of $E' \subseteq E$ is the set of all coordinates of values of f on E'^k that are less than min(E').

Suppose $f:E^k \to N^k$ is a a nice function and E is thin. We can hope that for lots of $E' \subseteq E$, the lower yields are equal.

THEOREM 4.1. Let $f:E^k \to N^k$ be a piecewise polynomial with coefficients from N, where E consists of all double factorials that are large relative to the coefficients used to present f. The lower yield of any two equinumerous subsets of E, or with at least k elements, are the same.

Note that this is false for f presented as x-1.

INFINITARY LOCAL BASIS CONSTRUCTION THEOREMS

PROPOSITION. Every $R \subseteq N^k \times N^k$ has a length 3 (length k, length p) local basis construction with infinite E, where the lower yield of any two k element subsets of E are the same.

Here is the sharpest statement of this kind.

PROPOSITION. Every $R \subseteq N^k \times N^k$ has a length 3 (length k, length p) local basis construction with infinite E, where the lower yield of any two equinumerous subsets of E, or subsets of E with at least k elements, are the same.

These are unprovable in ZFC, but can be proved with certain large cardinal hypotheses.

FINITARY LOCAL BASIS CONSTRUCTION THEOREMS

Here are the semifinite versions. They are also provable with certain large cardinals, but not in ZFC.

PROPOSITION. Every $R \subseteq N^k \times N^k$ has a length 3 (length k, length p) local basis construction, where the lower yield of any two k element subsets of the k+1 element E are the same.

PROPOSITION. Every $R \subseteq N^k \times N^k$ has a length 3 (length k, length p) local basis construction, where the lower yield of any two equinumerous subsets of the k element E are the same.

There are two paths to an explicitly Π01 forms of these Propositions. One is to replace N with a large initial segment of N, which we do now. The other path is followed later, using the order invariance of R.

FINITARY LOCAL BASIS CONSTRUCTION THEOREMS

In the context of R contained in $\{0,...,t\}^k \times \{0,...,t\}^k$ we assume that all local basis constructions live in $\{0,...,t\}$ or $\{0,...,t\}^k$.

PROPOSITION. For all t >> k, every R $\subseteq$ $\{0,...,t\}^k \times \{0,...,t\}^k$ has a length 3 (length k, length p) local basis construction, where the lower yield of any two k element subsets of the k+1 element E are the same. It is sufficient for t to be greater than the length 8k exponential stack of 2's (8kp if we use p).

PROPOSITION. For all t >> k, every R $\subseteq$ $\{0,...,t\}^k \times \{0,...,t\}^k$ has a length 3 (length k, length p) local basis construction, where the lower yield of any two equinumerous subsets of the k element E are the same. It is sufficient for t to be greater than the length 8k exponential stack of 2's (8kp if we use p).

Obviously these Propositions are explicitly Π^0_1.

They are provable using certain large cardinals but not in ZFC.

ORDER INVARIANT LOCAL BASIS CONSTRUCTION THEOREMS

In the context of R contained in $\{0,...,t\}^k \times \{0,...,t\}^k$ we assume that all local basis constructions live in {0,...,t} or {0,...,t}^k.

PROPOSITION. For all t >> k, every R $\subseteq$ $\{0,...,t\}^k \times \{0,...,t\}^k$ has a length 3 (length k, length p) local basis construction, where the lower yield of any two k element subsets of the k+1 element E are the same. It is sufficient for t to be greater than the length 8k exponential stack of 2's (8kp if we use p).

PROPOSITION. For all t >> k, every R contained in $\{0,...,t\}^k \times \{0,...,t\}^k$ has a length 3 (length k, length p) local basis construction, where the lower yield of any two equinumerous subsets of the k element E are the same. It is sufficient for t to be greater than the length 8k exponential stack of 2's (8kp if we use p).

Obviously these Propositions are explicitly Π01.

They are provable using certain large cardinals but not in ZFC.

ORDER INVARIANT LOCAL BASIS CONSTRUCTION THEOREMS

PROPOSITION. For all r > (8k)!!, every order invariant $R \subseteq N^k \times N^k$ has a length 3 (length k) local basis construction, starting with $\{r,r^2,...,r^{k+1}\}$, where $\{r,r^2,...,r^k\}$ and $\{r^2,r^3,...,r^{k+1}\}$ have the same lower yield.

Obviously, these Propositions are explicitly Π01.

This Proposition is provable from certain large cardinals, but not in ZFC.

LOCAL UPPER SHIFT KERNEL THEOREM ON Q^k

If we are willing to consider statements that assert the existence of a countably infinite set, then major new possibilities for necessary uses of large cardinals arise.

We extend order equivalence to Q^k in the obvious way.

Let G be a digraph on Q^k. We say x is isolated in G if and only if x is in Q^k, and there are no edges (x,y), (y,x).

We say that G is order invariant if and only if its edge set is order invariant, viewed as a subset of $Q^{2k} = Q^k \times Q^k$.

We say that G is regressive if and only if for all edges (x,y) in G, max(x) > max(y).

The kernels of G have been defined in section 1.

The upper shift of $q \in Q$ is q+1 if q is nonnegative; q otherwise. The upper shift extends to Q^k coordinatewise. The upper shift of a subset of Q^k is the set of upper shifts of its elements.

PROPOSITION. Every regressive order invariant digraph on Q^k in which x is isolated, has a local kernel containing its upper shift and x.

LOCAL UPPER SHIFT KERNEL THEOREM ON Q^k

We are also looking forward to a major structure theory for local kernels of order invariant digraphs on Q^k, where necessary uses of large cardinals abound.