INCOMPLETENESS II

by
Harvey M. Friedman
Distinguished University Professor
Mathematics, Philosophy, Computer Science
Ohio State University
Invitation to Mathematics Series
Department of Mathematics
Ohio State University
May 2, 2012
www.math.osu.edu/~friedman.8/

LONG FINITE SEQUENCES FROM A FINITE ALPHABET

Is there a longest finite sequence $x_1,\ldots,x_n$ from $\{1,2\}$ such that a certain pattern is avoided?

PATTERN TO BE AVOIDED. $x_i,\ldots,x_{2i}$ is a subsequence of $x_j,\ldots,x_{2j}$, where $i < j \leq n/2$.

E.g., (2,1,2) is a subsequence of (1,2,2,2,1,1,1,2).

ANSWER: Yes. n = 11. Gifted high school students in Paul Sally's summer program can sometimes prove this.

Is there a longest finite sequence $x_1,\ldots,x_n$ from $\{1,2,3\}$ such that this pattern is avoided?

ANSWER: Yes. I gave a lower bound for n in

Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

$n(3) > A_{7198}(158386)$

where A_p is the p-th Ackermann function from Z^+ to Z^+.

WHAT IS THE ACKERMANN HIERARCHY OF FUNCTIONS?

There are many versions that differ slightly. Most convenient: functions $A_1, A_2, \ldots$ from Z^+ to Z^+ such that
i. $A_1(n) = 2n$.
ii. $A_{i+1}(n) = A_i A_i \ldots A_i(1)$, where there are n A_i's.

We make some derivations.

$A_k(1) = 2$. $A_k(2) = 4$.

$A_2(n) = 2^n$. $A_3(n)$ is an exponential stack of n 2's.

$A_3(3) = A_2A_2A_2(1) = A_2(4) = 16$. $A_3(4) = A_2(A_3(3)) = A_2(16)$ $= 2^{16} = 65{,}536$.

$A_4(3) = A_3A_3A_3(1) = A_3(4) = 2^{16} = 65{,}536$.

$A_4(4) = A_3A_4(3) = A_3(65{,}536)$, which is an exponential stack of 2's of height 65,536.

Ackermann function is $A(n) = A_n(n)$. $A(5)$ = hard to "see".

Recall $n(3) > A_{7198}(158386)$.

LONG FINITE SEQUENCES FROM A FINITE ALPHABET

Is there a longest sequence $x_1,...,x_n$ from $\{1,...,k\}$ avoiding this pattern?

ANSWER: Yes, for any $k \geq 1$. However $n(k)$, as a function of k, grows faster than all multiply recursive functions. The Ackermann function is a 2-recursive function.

This Theorem can be proved using just Induction (Peano Arithmetic).

It can be proved in 3 quantifier induction but not in 2 quantifier induction. This is an example of a Weakly Unprovable Theorem. See

Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

Also: $n(4) > AA...A(1)$, where there are $A_5(5)$ A's.

$A(n) = A_n(n)$.

COUNTABLE SETS OF REALS AND RATIONALS

After you teach pointwise continuity of functions from a set of reals into the reals, you can state the following theorem.

COMPARABILITY THEOREM. If A,B are countable sets of real numbers, then there is a one-one pointwise continuous function from A into B, or a one-one pointwise continuous function from B into A.

This was well known from the early 20th century if A,B are countable and closed.

Despite the elementary statement, my proof uses transfinite induction on all countable ordinals. I proved that this is required. See

Metamathematics of comparability, in: Reverse Mathematics, ed. S. Simpson, Lecture Notes in Logic, vol. 21, ASL, 201-218, 2005.

Transfinite induction on all countable ordinals is required even if for just sets of rationals A,B.

HOW DO WE SAY MATHEMATICALLY THAT TRANSFINITE INDUCTION ON ALL COUNTABLE ORDINALS IS REQUIRED?

There are good proof theoretic ways of saying this, but here is a mathematical way. Experience shows that if we have a Theorem of the form

***)** $(\forall x \in X)(\exists y \in X)(R(x,y))$

where X is a complete separable metric space and R is a Borel relation, and if the proof is "normal", then there is a Borel function $H:X \to X$ **such that**

****)** $(\forall x \in X)(R(x,H(x)))$.

A huge number of Theorems of analysis can be put in form *), where **) holds for some Borel H.

The Comparability Theorem can be put in form *), via infinite sequences of reals (R^∞**). Yet there is no Borel H with **).**

$f(x_1,...,x_k) \leq f(x_2,...,x_{k+1})$

THEOREM A. For all $k,r \geq 1$ and $f:N^k \to N^r$, there exist distinct $x_1,...,x_{k+1}$ such that $f(x_1,...,x_k) \leq f(x_2,...,x_{k+1})$ coordinatewise.

THEOREM B. For all $k \geq 1$ and $f:N^k \to N$, there exist distinct $x_1,...,x_{k+2}$ such that $f(x_1,...,x_k) \leq f(x_2,...,x_{k+1}) \leq f(x_3,...,x_{k+2})$.

THEOREM C. For all $k \geq 1$ and $f:N^k \to N$, there exist distinct $x_1,...,x_{k+1}$ such that $f(x_2,...,x_{k+1}) - f(x_1,...,x_k) \in 2N$.

For f given by an algorithm, A,B,C are statements in the language of Peano Arithmetic (PA).

We have shown that A,B,C cannot be proved in PA for (even very efficiently) computable functions f. For any fixed k, the can be proved in PA for computable f.

If we require that $\max(f(x)) \leq \max(x)$, then we obtain the existence of a uniform upper bound on the $x_1,...,x_{k+1}$. This yields a finite statement that is not provable in Peano Arithmetic.

HOMEOMORPHIC EMBEDDINGS BETWEEN FINITE TREES

We use finite rooted trees. Each forms a topological space, with a notion of homeomorphic embedding between them. For our purposes, this is almost the same as an inf preserving one-one map from vertices into vertices.

J.B. KRUSKAL. In any infinite sequence of finite trees, one is homeomorphically embeddable in a later one.

Kruskal's proof and all subsequent proofs use uncountable sets. in particular, an infinite sequence of finite trees is constructed with reference to all such.

We proved that this is necessary. In fact, necessary even for very computable infinite sequences. See

Internal finite tree embeddings, in: Lecture Notes in Logic, volume 15, 62-93, 2002, ASL.

There are stronger results related to the Graph Minor Theorem of Robertson and Seymour. See

(with N. Robertson and P. Seymour), The Metamathematics of the Graph Minor Theorem, AMS Contemporary Mathematics Series, vol. 65, 1987, 229-261.

CANTOR'S THEOREM
BOREL DIAGONALIZATION

CANTOR. The reals are uncountable.
CANTOR. Every infinite sequence of reals omits a real.

The Hilbert cube $\Re^\infty$ has the product topology. It is a Polish space (complete separable metric space).

THEOREM. There is a Borel measurable $F:\Re^\infty \to \Re$ such that for all $x \in \Re^\infty$, $F(x)$ is not a coordinate of x.

The standard proof produces an F where if x,y have the same range, then F(x),F(y) may be different.

QUESTION: Is there a Borel diagonalizer $F:\Re^\infty \to \Re$ such that $rng(x) = rng(y) \to F(x) = F(y)$?

BOREL DIAGONALIZATION THEOREM. No.

This is proved using a Baire category argument on $\underline{\Re}^\infty$, where $\underline{\Re}$ is the discrete topology on $\Re$.

The Borel Diagonalization Theorem cannot be proved in SEPARABLE mathematics.

BOREL SETS IN THE PLANE AND ONE DIMENSIONAL BOREL FUNCTIONS

In any topological space, the Borel sets form the least σ algebra of sets containing the open sets. For uncountable Polish spaces (complete separable metric spaces), this leads to a hierarchy of Borel sets of length ω_1. However, most delicate issues arise at the finite levels, or even at the third level.

THEOREM. (Using a result of D.A. Martin from Infinitely Long Game Theory). Every Borel set in $\Re^2$, symmetric about the line $y = x$, contains or is disjoint from the graph of a Borel function from $\Re$ into $\Re$.

We proved that it is necessary and sufficient to use uncountably many iterations of the power set operation. For finite level Borel sets in $\Re^2$, it is necessary and sufficient to use infinitely many iterations of the power set operation. See

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

BOOLEAN RELATION THEORY

Boolean Relation Theory concerns Boolean relations between sets and their images under functions. This leads to Unprovable Theorems. There is a book draft on my website - Boolean Relation Theory and Incompleteness.

The two starting points of BRT are the ZFC theorems

THIN SET THEOREM. For all $f:N^k \to N$, there exists infinite $A \subseteq N$ such that $f[A^k] \neq N$.

COMPLEMENTATION THEOREM. For all strictly dominating $f:N^k \to N$, there is a unique $A \subseteq N$ such that $A \cup. f[A^k] = N$.

Strictly dominating means $f(x_1,...,x_k) > x_1,...,x_k$. Also $\cup.$ is disjoint union.

We restate as a Fixed Point Theorem:

COMPLEMENTATION THEOREM. For all strictly dominating $f:N^k \to N$, there is a unique $A \subseteq N$ such that $A = N\setminus f[A^k]$.

There are some mildly exotic features of proofs, more so with the Thin Set Theorem.

BOOLEAN RELATION THEORY

Let ELG be the set of all $f:N^k \to N$, $k \geq 1$, where there exist $c,d > 1$ such that

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

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

TEMPLATE. For all $f,g \in$ ELG, there exists infinite $A,B,C \subseteq N$ such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fQ \subseteq R \cup. gS.$$

where the letters X,Y,V,W,P,Q,R,S are among the letters A,B,C. fE is $f[E^k]$, where $\mathrm{dom}(f) = N^k$, and $\cup.$ means "disjoint union".

There are $3^8 = 6561$ instances of the Template. All but 12 are provable/refutable in a very weak fragment of ZFC. The 12 are provable using strongly Mahlo cardinals of finite order, but not in ZFC.

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

GRAPHS AND MAXIMAL CLIQUES

A graph on V is a pair G = (V,E), where E is an irreflexive symmetric relation on V.

V is the set of vertices of G, and E is the adjacency relation.

A clique in G is a subset of V such that any two distinct elements of V are adjacent.

A maximal clique in G is a clique in G which is not a proper subset of any clique in G.

EVERY GRAPH HAS A MAXIMAL CLIQUE.

This is proved by Zorn's Lemma, and is known to be equivalent to the axiom of choice over ZF.

If the graph is countable, then there is a nice explicit construction of a maximal clique by what is called a greedy algorithm.

INVARIANCE

Invariance is a principal theme in mathematics. We use the following general formulation.

Let R be any relation (set of ordered pairs). We define the R invariant subsets S of an ambient space K.

We say that $S \subseteq K$ is R invariant if and only if for all $x,y \in K$ with $R(x,y)$, we have $x \in S \Rightarrow y \in S$.

We say that $S \subseteq K$ is completely R invariant if and only if for all $x,y \in K$ with $R(x,y)$, we have $x \in S \Leftrightarrow y \in S$.

Two important cases: R is a function, R is an equivalence relation. Functions R are treated as relations.

RATIONAL VECTORS AND ORDER INVARIANT GRAPHS

Q is the set of all rationals. Q* is the set of all nonempty finite sequences of rationals. Q[0,n] is the set of all rationals in [0,n].

All of our graphs are going to be on $Q[0,n]^k$.

We use order equivalence on Q*. $x,y \in Q^*$ are order equivalent if and only if $lth(x) = lth(y)$ and for all $1 \le i,j \le lth(x)$, $x_i < x_j \Leftrightarrow y_i < y_j$.

A graph on $Q[0,n]^k$ is said to be order invariant if and only if its adjacency relation $E \subseteq Q[0,n]^{2k}$ is invariant with respect to order equivalence on Q*.

We now look at

EVERY GRAPH ON $Q[0,n]^k$ HAS A MAXIMAL CLIQUE.

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS AN "INVARIANT" MAXIMAL CLIQUE.

FULL SHIFT, UPPER HALF SHIFT

The Full Shift $FS:Q^* \to Q^*$ is defined by $FS(x) = x+1$. I.e., add 1 to all coordinates.

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS A COMPLETELY FS INVARIANT MAXIMAL CLIQUE.

Unfortunately, this is false for $k \geq 1$, $n \geq 2$. We can restrict FS so this is true:

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS A COMPLETELY $FS|(\min \geq 1)$ INVARIANT MAXIMAL CLIQUE.

For $x \in Q^*$, the upper half consists of the coordinates greater than at least half of the coordinates.

The Upper Half Shift $UHS:Q^* \to Q^*$ is defined by $UHS(x)$ = the result of adding 1 to the upper half.

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS A COMPLETELY UHS INVARIANT MAXIMAL CLIQUE.

This is also false for $k \geq 1$, $n \geq 2$.

How do we fix this?

UPPER HALF SHIFT

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS A COMPLETELY UHS INVARIANT MAXIMAL CLIQUE.

This is false. To fix it, we restrict UHS to the vectors where UHS shifts only positive integers.

In general, $T:Q^* \to Q^*$ restricted to the vectors where T moves only positive integers, is called T#.

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS A COMPLETELY UHS# INVARIANT MAXIMAL CLIQUE.

This can be proved, but only by going well beyond the usual axioms of ZFC.

A THIRD SHIFT, $Z^+\uparrow$

Define $Z^+\uparrow : Q^* \to Q^*$ as follows.

$Z^+\uparrow(x)$ is the result of adding 1 to all coordinates of x that are greater than all coordinates of x outside Z^+.

EVERY ORDER INVARIANT GRAPH ON $Q[0,n]^k$ HAS A COMPLETELY $Z^+\uparrow$ INVARIANT MAXIMAL CLIQUE.

This can be proved, but only by going well beyond the usual axioms of ZFC.

WHAT ARE THE LARGE CARDINALS USED FOR BOOLEAN RELATION THEORY?
strongly inaccessible cardinals are not enough!

An (von Neumann) ordinal is the set of its predecessors, and a (von Neumann) cardinal is an ordinal not equinumerous with any predecessor.

κ is a strong limit cardinal iff for all $\alpha < \kappa$,

$\mathrm{card}(\wp(\alpha)) < \kappa$.

κ is a regular cardinal iff κ is not the sup of a subset of κ of cardinality $< \kappa$.

κ is an inaccessible cardinal iff κ is a regular strong limit cardinal $> \omega$.

ZFC does not suffice to prove the existence of a strongly inaccessible cardinal.

Grothendieck Topoi (strong kind).

WHAT ARE THE LARGE CARDINALS USED FOR BOOLEAN RELATION THEORY?
strongly k-Mahlo cardinals

κ is a strongly 0-Mahlo cardinal iff κ is a strongly inaccessible cardinal.

κ is a strongly n+1-Mahlo cardinal iff κ is a strongly n-Mahlo cardinal such that every closed and unbounded subset of κ has an element that is a strongly n-Mahlo cardinal.

The 12 exotic cases in Boolean Relation Theory are provable in

$SMAH^+$ = ZFC + "for all k there exists a strongly k-Mahlo cardinal",

but (assuming SMAH is consistent) not in

SMAH = ZFC + {there exists a strongly k-Mahlo cardinal}.

In fact, they are provably equivalent, in a weak fragment of ZFC, to the 1-consistency of SMAH.

WHAT ARE THE LARGE CARDINALS USED FOR THE INVARIANT MAXIMALITY THEOREMS? k-SRP ordinals

Let λ be a limit ordinal. We say that $E \subseteq \lambda$ is stationary if and only if E meets every closed and unbounded subset of λ.

We say that a limit ordinal λ has the k-SRP if and only if every 2 coloring of its k element subsets is monochromatic on a stationary subset of λ.

The Invariant Maximality Theorems are provable in

SRP^{+} = ZFC + "for all k there exists a k-SRP ordinal",

but (assuming SRP is consistent) not in

SRP = ZFC + $\{$there exists a k-SRP ordinal$\}_k$.

In fact, they are provable equivalent, in a weak fragment of ZFC, to the consistency of SRP.