# CONCRETE MATHEMATICAL INCOMPLETENESS

by
Harvey M. Friedman
Distinguished University Professor
Emeritus
Mathematics, Philosophy, Computer Science
Ohio State University

Andrzej Mostowski Centenary
Warsaw, Poland
October 11, 2013

NOTE: THIS 10/19/13 VERSION HAS BEEN UPDATED FROM THE ORIGINAL

# ACKNOWLEDGEMENTS

This research was partially supported by an Ohio State University Presidential Research Grant and by the John Templeton Foundation grant ID #36297. The opinions expressed here are those of the author and do not necessarily reflect the views of the John Templeton Foundation.

**********

We are here to honor Andrzej Mostowski, particularly his role as a key leader of the Polish school. He devoted many publications to various aspects of Incompleteness. I was honored to have a paper in the beautiful volume, "Andrzej Mostowski and Foundational Studies", ed. Ehrenfeucht, Marek, Srebny. I sincerely wish I had the opportunity to interact with him.

Mathematicians view mathematics as a special subject with singularly attractive features. Most intuitively feel that the great power and stability of some "rule book for mathematics" is an important component of their relationship with mathematics. The general feeling is that there is nothing substantial to be gained by revisiting the commonly accepted rule book, and they can continue to do all truly significant mathematics without any foundational concerns.

We approach 100 years of ZFC as the accepted rule book for mathematics. - Nearly all mathematicians are aware of its existence - if not its details - and accept that they are implicitly working within its scope.

Incompleteness is an attack on the power and stability of the rule book. As power and stability are integral parts of the mathematician's relationship with mathematics, Incompleteness is arguably the unique theme in mathematics today that has the real potential of profoundly altering the mathematician's relationship with mathematics at the most fundamental level. This puts Incompleteness in a category all by itself among all mathematical research.

# DEFENSE AGAINST INCOMPLETENESS

Incompleteness, in the modern sense, was initiated by Kurt Gödel through his first and second incompleteness theorems, and his relative consistency of the axiom of choice and the continuum hypothesis - with the follow up development of Paul Cohen on AxC and CH.

The mathematician's basic instinct is to defend against Incompleteness by requiring that any statement that is known to be beyond the scope of the rule book be "real mathematics". The exact nature of the "real mathematics" requirement for Incompleteness has evolved over time according to the evolving nature of Incompleteness.

It was already clear soon after Cohen that mathematicians were at least implicitly putting up a general defense against Incompleteness that was going to hold until there was a radical change in the examples of Incompleteness. An informal notion of "pathological mathematical object" had emerged during the 20th century that has shaped, and continues to shape, the general course of mathematics. Informal discussion has even made it to Wikipedia with the pages "Pathological (mathematics)" and "Well Behaved".

# CONCRETE MATHEMATICAL INCOMPLETENESS
# CMI

In the late 1960s we formulated what we now call Concrete Mathematical Incompleteness (CMI), aimed at developing examples of Incompleteness not involving, directly or indirectly, pathological objects. Here we are 45 years later.

The CMI examples have the important feature that they become provable if we expand the rule book in certain well studied ways (large cardinal hypotheses). Furthermore, there appears to be no alternative way to expand the rule book to remove the CMI. With traditional set theoretic incompleteness, V = L is an alternative way to remove the MI.

We regularly discuss the continually evolving examples of CMI with a range of mathematicians, including top luminaries such as A. Connes, C. Fefferman, H. Furstenburg, T. Gowers, M. Gromov, D. Kazhdan, Y. Manin, B. Mazur, D. Mumford. All of these top luminaries are fully aware of what is at stake, and had interesting reactions.

# TOP LUMINARIES' VIEWS OF FUNDAMENTAL, IMPORTANT MATHEMATICS

**Above all, it is obvious that such top luminaries do not identify, in any way, "fundamental or important mathematics" with "mathematics people have done or are doing now". Our examples are judged by such top luminaries strictly on fundamental mathematical standards of simplicity, naturalness, intrinsic interest, concreteness, and depth. This is fortunate since the integration of CMI with existing concrete mathematical developments will likely occur only at later stages of CMI.**

**On the other hand, very strong mathematicians, even some at the next level below such top luminaries,**

**DO tend to identify "fundamental or important mathematics" with "mathematics people have done or are doing now", and ironically with the mathematics that such top luminaries have done or are doing now!**

# INSTRUCTIVE EXAMPLE OF A DISASTER

As an example of the kind of appalling interaction one can encounter, I was in the office of a Fields Medalist (FM), who arranged a short visit. Note how FM differs from the top luminaries I mentioned earlier.

HF: I want to tell you about some examples about graphs.

FM: Yes...

HF: Do you remember what a graph is?

FM: No.

HF: There is a very simple definition of graph -

FM: I don't know what a graph is... I never want to know what a graph is.

HF: It's just an irreflexive symmetric relation on a set ...

It was too late - FM's eyes had already glazed over, and I sensed that his auditory system had shut down.

# CRITICAL ROLE OF POLISH SPACES IN THE DEVELOPMENT OF CMI

**The outer limits of CMI live in the Borel measurable sets and functions between Polish spaces. Polish spaces are a key strategic unifying concept arising out of the Polish School of Mathematics. Andrzej Mostowski was certainly a key leader of the Polish school.**

**Some historical highlights of CMI are: long finite sequences, continuous comparability of countable sets of reals, Kruskal's and Higman's theorem, Graph Minor Theorem, Borel Diagonalization, Borel determinacy, Borel selection, and Boolean Relation Theory.**

**In light of time constraints, we have chosen to concentrate on the newest developments, which have only crystallized during the preparation of this talk.**

# 1. ORDER EQUIVALENCE, ORDER INVARIANT, ORDER THEORETIC, ROOTS, MAXIMAL ROOTS

**DEFINITION 1.1.** $Q$ is the set of rationals and $N$ is the set of nonnegative integers. $Q_{\leq p} = \{q \in Q: q \leq p\}$.

**DEFINITION 1.2.** $x,y \in Q^k$ are order equivalent iff for all $1 \leq i,j \leq n$, $x_i < x_j \Leftrightarrow y_i < y_j$.

**DEFINITION 1.3.** Let $T \subseteq Q^k$. $S \subseteq T$ is order invariant iff for all order equivalent $x,y \in T$, $x \in S \Leftrightarrow y \in S$.

**DEFINITION 1.4.** $S \subseteq Q^k$ is order theoretic iff $S$ is a Boolean combination of inequalities using only $v_1,...,v_k,<$ and constants from $Q$.

The order invariant (order theoretic) subsets of $Q^k$ are those 0-definable (definable) over $(Q,<)$.

**DEFINITION 1.5.** $S$ is a root of $V \subseteq Q^{2k}$ iff $S^2 \subseteq V$. $S$ is a maximal root of $V \subseteq Q^{2k}$ iff $S$ is a root of $V$ which is not a proper subset of any root of $V$.

# 2. GOOD MAXIMAL ROOTS

**GENERAL SHAPE. Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has a GOOD maximal root $S \subseteq Q_{\leq n}^{k}$.**

**So what is a "good" $S \subseteq Q_{\leq n}^{k}$? We will use invariance under binary relations on $Q^k$ for "good".**

**DEFINITION 2.1. Let $R \subseteq Q^{2k}$. $S \subseteq Q_{\leq n}^{k}$ is R invariant iff for all $x,y \in Q_{\leq n}^{k}$, if $R(x,y)$ then $x \in S \Leftrightarrow y \in S$.**

**TEMPLATE A. Fix order theoretic $R \subseteq Q^{2k}$. Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has an R invariant maximal root $S \subseteq Q_{\leq n}^{k}$. n is fixed, or, alternatively, universally quantified.**

**TEMPLATE B. Fix $(Q,N,+,<)$ definable $R \subseteq Q^{2k}$. Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has an R invariant maximal root $S \subseteq Q_{\leq n}^{k}$. n is fixed, or, alternatively, universally quantified.**

**CONJECTURES A,B. Every instance of Template A (B) is provable or refutable in SRP (a strong extension of ZFC). We know ZFC does not suffice for A, for n = 0 (if ZFC is consistent) - no consistent $SRP_r$ suffices.**

# 3. N TAIL SHIFT INVARIANCE

**DEFINITION 3.1. $H:Q^k \to Q^k$ is a restricted shift operator iff each $H(x)$ is obtained from $x$ by adding 1 to zero or more coordinates of $x$.**

**We start with three very simple restricted shift operators.**

**DEFINITION 3.2. The shift of $x \in Q^k$ adds 1 to all coordinates. The nonnegative shift of $x \in Q^k$ adds 1 to all nonnegative coordinates. The N shift of $x \in Q^k$ adds 1 to all coordinates in N.**

**PROPOSITION 3.1. Every order invariant $V \in Q_{\leq n}^{2k}$ has a (shift, nonnegative shift, N shift) invariant maximal root $S \subseteq Q_{\leq n}^{k}$.**

**THEOREM 3.2. All three forms of Proposition 3.1 are refutable in $RCA_0$.**

**This sets the stage for N tail shift invariance.**

# 3. N TAIL SHIFT INVARIANCE

**DEFINITION 3.3. The N tail of $x \in Q^k$ consists of the $x_i$ such that every $x_j \geq x_i$ is in N. The N tail shift of $x \in Q^k$ adds 1 to the N tail of x.**

**EXAMPLE: The N tail shift of (-1,0,3,7/2,5,5,7) = (-1,0,3,7/2,6,6,8). We put the coordinates in increasing order for readability.**

**INVARIANT MAXIMAL ROOTS (IMR). Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has an N tail shift invariant maximal root $S \subseteq Q_{\leq n}^{k}$.**

**We can strengthen N tail shift invariance - instead of using the (largest) N tail, we can use any N tail.**

**DEFINITION 3.4. An N tail of $x \in Q^k$ consists of the coordinates in the N tail > some given p. An N tail shift of $x \in Q^k$ adds 1 to some N tail of x. $S \subseteq Q_{\leq n}^{k}$ is strongly N tail shift invariant iff for all $x,y \in Q_{\leq n}^{k}$, if y is an N tail shift of x then $x \in S \Leftrightarrow y \in S$.**

**STRONGLY INVARIANT MAXIMAL ROOTS (SIMR). Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has a strongly N tail shift invariant maximal root $S \subseteq Q_{\leq n}^{k}$.**

# 3. N TAIL SHIFT INVARIANCE

**INVARIANT MAXIMAL ROOTS (IMR). Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has an N tail shift invariant maximal root $S \subseteq Q_{\leq n}^{k}$.**

**STRONGLY INVARIANT MAXIMAL ROOTS (SIMR). Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has a strongly N tail shift invariant maximal root $S \subseteq Q_{\leq n}^{k}$.**

**There is an elementary argument for IMR ⇒ SIMR.**

**In fact, we can go further. SIMR is based on the relation "y is an N tail shift of x". Obviously any $S \subseteq Q_{\leq n}^{k}$ invariant under this relation is also invariant under the least equivalence relation containing this relation. We call this least equivalence relation N tail equivalence, and the corresponding invariance notion, N tail invariance.**

**EQUIVALENCE INVARIANT MAXIMAL ROOTS (EIMR). Every order invariant $V \subseteq Q_{\leq n}^{2k}$ has an N tail invariant maximal root $S \subseteq Q_{\leq n}^{k}$.**

**THEOREM 3.3. IMR, SIMR, NTIMR are provably equivalent to Con(SRP) over $WKL_0$. They remain so even if we require that the root be recursive in 0'.**

# 3. N TAIL SHIFT INVARIANCE

**INVARIANT MAXIMAL ROOTS (IMR). Every order invariant V $Q_{\leq n}^{2k}$ has an N tail shift invariant maximal root S $\subseteq$ $Q_{\leq n}^{k}$.**

**STRONGLY INVARIANT MAXIMAL ROOTS (SIMR). Every order invariant V $\subseteq$ $Q_{\leq n}^{2k}$ has a strongly N tail shift invariant maximal root S $\subseteq$ $Q_{\leq n}^{k}$.**

**EQUIVALENCE INVARIANT MAXIMAL ROOTS (EIMR). Every order invariant V $\subseteq$ $Q_{\leq n}^{2k}$ has an N tail invariant maximal root S $\subseteq$ $Q_{\leq n}^{k}$.**

**THEOREM 3.4. x,y $\in$ $Q^k$ are N tail equivalent iff x,y are order equivalent, and the parts of x,y off of their respective N tails are identical.**

**By merely invoking Gödel's completeness theorem, we see that IMR, SIMR, EIMR are provably equivalent to $\Pi^0_1$ sentences over $WKL_0$.**

# 4. N/ORDER INVARIANTLY RESTRICTED SHIFT OPERATORS

**DEFINITION 4.1. A restricted shift operator $H:Q^k \to Q^k$ is order invariantly restricted iff for order equivalent $x,y \in Q^k$, $H(x)-x = H(y)-y$.**

**The order invariantly restricted shift operators cannot be used for IMR.**

**THEOREM 4.1. ($RCA_0$). Let $H:Q^k \to Q^k$ be an order invariantly restricted shift operator. Suppose every order invariant $V \subseteq Q_{\leq n}{}^{2k}$ has an H invariant maximal root $S \subseteq Q_{\leq n}{}^k$. Then H is the identity.**

**DEFINITION 4.2. $x,y \in Q^k$ are N/order equivalent iff for all $1 \leq i,j \leq k$, $(x_i < x_j \Leftrightarrow y_i < y_j) \wedge (x_i \in N \Leftrightarrow y_i \in N)$.**

**DEFINITION 4.3. A restricted shift operator $H:Q^k \to Q^k$ is N/order invariantly restricted iff for all N/order equivalent $x,y \in Q^k$, $H(x)-x = H(y)-y$.**

**Note that the N tail shift is N/order invariantly restricted.**

# 4. N/ORDER INVARIANTLY RESTRICTED SHIFT OPERATORS

**THEOREM 4.2. Let $H:Q^k \rightarrow Q^k$ be an N/order invariantly restricted shift operator. The statement "every order invariant $V \subseteq Q_{\leq n}^{2k}$ has an H invariant maximal root $S \subseteq Q_{\leq n}^{k}$" is provable or refutable in SRP. n is fixed, or, alternatively, universally quantified. Furthermore, no consistent $SRP_r$ suffices (for all H,n, or, alternatively, for all H).**

**BOTTOM LINE: Expansion of the Rule Book from ZFC to SRP settles IMR, SIMR, EIMR, and all appropriate instances of the statement in quotes using N/order invariantly restricted shift operators. The existing Rule Book does not suffice.**

# 5. INDUCTIVELY MAXIMAL ROOTS

**Inductive maximality is a variant of maximality that leads to additional incompleteness phenomena. We can work with Q instead of $Q_{\leq n}$, avoiding ambient spaces.**

**DEFINITION 5.1. For $S \subseteq Q^k$, S# is the least $A^k$ containing S and the origin.**

**DEFINITION 5.2. Let $V \subseteq Q^{2k}$. An inductively maximal root of V is a root S of V such that for all $x \in S\#\backslash S$, $S_{<x} \cup \{x\}$ is not a root of V.**

**DEFINITION 5.3. The nonnegative shift of $S \subseteq Q^k$ adds 1 to all nonnegative coordinates of elements of S.**

**INVARIANT INDUCTIVELY MAXIMAL ROOTS (IIMR). Every order invariant subset of $Q^{2k}$ has an inductively maximal root that contains its upper shift.**

**THEOREM 5.1. IIMR is provably equivalent to Con(SRP) over $WKL_0$.**

**By invoking Gödel's completeness theorem, we see that IIMR is provably equivalent to a $\Pi^0_1$ sentence over $WKL_0$.**

# 5. INDUCTIVELY MAXIMAL ROOTS

**TEMPLATE C. Let $H:Q^k \to Q^k$ be definable over $(Q,N,+,<)$. Every order invariant subset of $Q^{2k}$ has an inductively maximal root that contains its H value.**

**CONJECTURE. Every instance of Template C is provable or refutable in SRP. ZFC does not suffice (if consistent). We know that no consistent $SRP_r$ suffices (for all H).**

**Inductively maximal roots are much easier to work with than maximal roots, and this Conjecture is within reach.**

# 6. INDUCTIVELY MAXIMAL $\geq$-ROOTS

**DEFINITION 6.1.** For $S \subseteq Q^k$, $S^{\geq} = \{x \in S: x_1 \geq \ldots \geq x_k\}$. $S$ is a $\geq$-root of $V \subseteq Q^{2k}$ iff $S^{\geq} \times S \cup S \times S^{\geq} \subseteq V$. $S$ is an inductively maximal $\geq$-root of $V \subseteq Q^{2k}$ iff for all $x \in S\#^{\geq} \backslash S$, $S_{<x} \cup \{x\}$ is not a $\geq$-root of $V \subseteq Q^{2k}$.

**DEFINITION 6.2.** $S_x = \{y: (x,y) \in S\}$. $S$ sharply contains $E$ iff $E \subseteq S$ and every $E_x \subseteq Q$ is some $S_y$.

**INDUCTIVELY MAXIMAL $\geq$-ROOTS (IIMR($\geq$)).** Every order invariant subset of $Q^{2k+4}$ has an inductively maximal $\geq$-root that sharply contains the shift of its nonnegative part.

**THEOREM 6.1.** IIMR($\geq$) is provably equivalent to Con(HUGE) over $WKL_0$.

Here the huge cardinal hierarchy can be taken to be $j:V(\lambda) \to V(\mu)$, where $\lambda = jj...j(\kappa)$, $\kappa$ = critical point.

By invoking Gödel's completeness theorem, we see that IIMR($\geq$) is provably equivalent to a $\Pi^0_1$ sentence over $WKL_0$.

# 7. COMPUTER INVESTIGATIONS

There are obvious infinite length nondeterministic computer algorithms for constructing various kinds of invariant maximal roots. I have thought about inductively maximal roots, with, simultaneously, two invariances. One is N tail invariance. The other is nonnegative shift invariance. The latter has an obvious strengthening where we shift $\geq t$, $t \in N$.

As witnesses are generated in the nondeterministic algorithm, new tuples are created out of the rationals generated. This corresponds with the use of S#.

By the tree lemma, being able to navigate such an algorithm for any given finite number of steps is equivalent to being above to navigate the algorithm for an infinite number of steps, and equivalent to Con(SRP). This is explicitly $\Pi^0_1$.

We can try to **actually** navigate for a small number of steps. If we design the nondeterministic algorithm and parameters properly, we will have the following.

# 7. COMPUTER INVESTIGATIONS

1. A large exhaustive search can be conducted for such a practical length certificate. Here challenging order invariant $V \subseteq Q^{2k}$, k small, are constructed through a combination of heuristics, randomness, and theory.

2. We know from Con(SRP) that the exhaustive search must be successful.

3. We expect experiments to show that almost all navigation decisions lead to dead ends. I.e., there are very few short certificates.

4. With the help of experiments such as 3, it appears that the large cardinals are intensively engaged. No mathematician has even the slightest idea as to how to begin navigating the nondeterministic algorithm.

5. We expect such exhaustive searches to be successful. This can be viewed as a practical confirmation of Con(SRP) - or at least Con(ZFC). If not, we obtain inconsistencies in large cardinals.

6. The work is expected to appropriately extend to apply to the huge cardinal hierarchy, and perhaps beyond.