MAXIMALITY AND INCOMPLETENESS

by
Harvey M. Friedman
Distinguished University Professor
Mathematics, Philosophy, Computer Science
Ohio State University
Brandeis-Harvard-MIT-Northeastern
Joint Mathematics Colloquium
Harvard, March 1, 2012

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

There has evolved, for good reason, a specific set of axioms and rules for mathematics, called ZFC = Zermelo Frankel set theory with the axiom of choice.

This system is massive overkill for the vast bulk of mathematical purposes.

However, when we probe deeper, there are some issues.

But how interesting are these issues from YOUR point of view?

They are getting more interesting.

How interesting? Well, I have about an hour to say.

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction? If NOT, it is (generally regarded to be) worthless.

ISSUE #2. Does anything escape the grasp of ZFC?

ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

WITH REGARD TO ISSUE #1: Kurt Gödel proved the following.

"ZFC IS CONSISTENT" IS NOT PROVABLE IN ZFC - unless ZFC is inconsistent.

It is generally accepted that ZFC is consistent. But what if ZFC turned out to be inconsistent?

Since ZFC is so enormous, we would move to a less enormous fragment of ZFC - like ZC - and make a stand there.

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction?
ISSUE #2. Does anything escape the grasp of ZFC?
ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

So “ZFC is consistent” escapes the grasp of ZFC.

BUT you are a mathematician, not a philosopher, not a logician. You don’t work in foundations of mathematics.

So YOU don’t care about “ZFC is consistent”. YOU care about math.

So is there anything mathematically interesting that escapes the grasp of ZFC?

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction?
ISSUE #2. Does anything escape the grasp of ZFC?
ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

Here is the first example of a mathematical assertion that escapes the grasp of ZFC.

CH (continuum hypothesis). Every infinite set of real numbers is in one-one correspondence with the set of integers or the set of real numbers.

GODEL (1930s). ZFC does not refute CH.

COHEN (1960s). ZFC does not prove CH.

Splashy, but by now, YOU are no longer interested in the continuum hypothesis. Why?

FOUNDATIONS OF MATHEMATICS
IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction?
ISSUE #2. Does anything escape the grasp of ZFC?
ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

CH (continuum hypothesis). Every infinite set of real numbers is in one-one correspondence with the set of integers or the set of real numbers.

Why are you no longer interested in CH?

Because YOUR sets of real numbers are very, or at least, quite reasonable. YOU naturally move on to

REASONABLE CH. Every reasonable infinite set of real numbers is in one-one correspondence with the set of integers or the set of real numbers.

REASONABLE CH can be proved in ZFC! E.g.,

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction?
ISSUE #2. Does anything escape the grasp of ZFC?
ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

REASONABLE CH. Every reasonable infinite set of real numbers is in one-one correspondence with the set of integers or the set of real numbers.

BOREL CH. Every Borel measurable infinite set of real numbers is in Borel one-one correspondence with the set of integers or the set of real numbers.

Borel CH is a classic theorem (Polish school).

Aha!, you say. CH escaped ZFC because of the pathological objects involved!!

Maybe all of this Incompleteness nonsense is essentially fraudulent? If you stuff your mathematics with obnoxious, irrelevant, and unwanted pathological generalities, then you run into trouble.

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction?
ISSUE #2. Does anything escape the grasp of ZFC?
ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

So it appears, maybe, that in order to escape the grasp of ZFC, with something looking anything like regular mathematics, you have to be using alarming amounts of generality - generality that admits (unwanted) pathology.

GENERAL SOLUTION TO FOUNDATIONS(?). Just stay within a reasonable category of mathematical objects, and ask mathematically sensible questions, stay away from logical issues, and the foundational issues are resolved once and for all - by ZFC!

FOUNDATIONS OF MATHEMATICS IN HEADLINE FORM

ISSUE #1. Is ZFC free of contradiction?
ISSUE #2. Does anything escape the grasp of ZFC?
ISSUE #3. Does anything interesting to YOU escape the grasp of ZFC?

In other words, the answer to Issue #3 is NO - because if it is beyond ZFC, then

i. it is not mathematics (maybe its logic); or
ii. it is mathematics, but riddled with pathological objects.

Even the Borel measurable - which appears to be safe, could be cut back, if it turned out to be dangerous - since even the Borel measurable is way way way more than what YOU care about.

NOT SO FAST...

SOME ADVANCED UNDERGRAD MATH

EVERY SET OF ORDERED PAIRS CONTAINS A MAXIMAL SQUARE.

Let's make sure there is no misunderstanding.

Let R be a set of ordered pairs from anywhere. Among the $A \times A \subseteq R$, there is a maximal one under inclusion.

Now this is a very general statement, and because of its great generality, the proof requires the axiom of choice. In fact the statement is outright equivalent to the axiom of choice.

Since I am joining YOU in hating pathology, I only care about this statement if the set of ordered pairs is countable.

SOME ADVANCED UNDERGRAD MATH

EVERY *COUNTABLE* SET OF ORDERED PAIRS CONTAINS A MAXIMAL SQUARE.

In order to stir up the undergraduate in YOU, here is what you do. Let R be a subset of K × K, where K = $\{x_1,x_2,...\}$.

We define a tower of finite sets A_i, $i \geq 1$, as follows. Suppose A_i has been defined so that $A_i \subseteq \{x_1,...,x_i\}$ and $A_i \times A_i \subseteq R$.

Set $A_{i+1} = A_i \cup \{x_{i+1}\}$ if $A_{i+1} \times A_{i+1} \subseteq R$; A_i otherwise.

Then A × A is a maximal square in S, where A is the union of the A's.

SOME ADVANCED UNDERGRAD MATH

EVERY *COUNTABLE* SET OF ORDERED PAIRS CONTAINS A MAXIMAL SQUARE.

We are going to put invariance conditions on the given set of ordered pairs, and an invariance condition on the maximal square.

In order to use invariance conditions, we need to have some structure. Let Q be the set of all rationals.

EVERY SUBSET OF Q^{2k} CONTAINS A MAXIMAL SQUARE.

So far, this is trivially the same statement.

But the Q^k have enough structure to support interesting notions of invariance.

We also use $Q[0,n]^k$, where $Q[0,n] = Q \cap [0,n]$.

INVARIANCE IN RATIONAL VECTORS

EVERY SUBSET OF Q^{2k} CONTAINS A MAXIMAL SQUARE.

Here is where we are headed.

EVERY INVARIANT SUBSET OF Q^{2k} CONTAINS AN INVARIANT' MAXIMAL SQUARE.

We will be using two specific invariance conditions on subsets of Q^{2k} for the above statement.

We also work with

EVERY INVARIANT SUBSET OF $Q[0,n]^{2k}$ CONTAINS AN INVARIANT' MAXIMAL SQUARE.

EVERY INVARIANT SUBSET OF $Q[0,16]^{32}$ CONTAINS AN INVARIANT' MAXIMAL SQUARE.

INVARIANCE IN RATIONAL VECTORS

EVERY SUBSET OF Q^{2k} CONTAINS A MAXIMAL SQUARE.

EVERY INVARIANT SUBSET OF Q^{2k} CONTAINS AN INVARIANT' MAXIMAL SQUARE.

EVERY INVARIANT SUBSET OF $Q[0,n]^{2k}$ CONTAINS AN INVARIANT' MAXIMAL SQUARE.

EVERY INVARIANT SUBSET OF $Q[0,16]^{32}$ CONTAINS AN INVARIANT' MAXIMAL SQUARE.

We can prove the latter three statements using strong Axioms of Infinity that go well beyond ZFC.

In the case of the latter two statements, we know that ZFC does not suffice. This is open for the second statement.

GENERAL SETUP FOR INVARIANCE

Let K be an ambient space anywhere. (We will be using the various Q^k, $Q[0,n]^k$ as ambient spaces).

Let E be an equivalence relation anywhere. Let T be a function anywhere.

$S \subseteq K$ is E invariant. For all E equivalent $x,y \in K$, $x \in S \Rightarrow y \in S$.

$S \subseteq K$ is T invariant. For all $x,T(x) \in K$, $x \in S \Rightarrow T(x) \in S$.

$S \subseteq K$ is completely T invariant. For all $x,T(x) \in K$, $x \in S \Leftrightarrow T(x) \in S$.

Because E is symmetric, the $\Rightarrow$ in the first notion can be automatically strengthened to $\Leftrightarrow$.

SPECIFIC RELATIONS AND FUNCTIONS ON Q*

Q* is the set of all finite sequences of rationals.

ORDER EQUIVALENCE ON Q*

lth(x) = lth(y). For all $1 \leq i,j \leq$ lth(x), $x_i < x_j \Leftrightarrow y_i < y_j$.

Ex: (9,-1/2,8), (3,1,5/2) are order equivalent.

LIFTING FUNCTION $Z^+\uparrow$ FROM Q* INTO Q*

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

Ex: $Z^+\uparrow(-1,0,1,3/2,3,5) = (-1,0,1,3/2,4,6)$.

SPECIFIC RELATIONS AND FUNCTIONS ON Q*

ORDER EQUIVALENCE ON Q*

Ex: (9,-1/2,8), (3,1,5/2) are order equivalent.

LIFTING FUNCTION $Z^+\uparrow$ FROM Q* INTO Q*

Ex: $Z^+\uparrow$(-1,0,1,3/2,3,5) = (-1,0,1,3/2,4,6).

UPPER INTEGRAL EQUIVALENCE ON Q*

x,y are upper integral equivalent if and only if

x,y are order equivalent, and

for all i, if $x_i \neq y_i$ then every $x_j \geq x_i$ lies in Z^+, and every $y_j \geq y_i$ lies in Z^+.

Ex: (-1,0,1,3/2,3,5), (-1,0,1,3/2,2,87) are upper integral equivalent.

SPECIFIC RELATIONS AND FUNCTIONS ON Q*

ORDER EQUIVALENCE ON Q*

Ex: (9,-1/2,8), (3,1,5/2) are order equivalent.

LIFTING FUNCTION $Z^+\uparrow$ FROM Q* INTO Q*

Ex: $Z^+\uparrow$(-1,0,1,3/2,3,5) = (-1,0,1,3/2,4,6).

UPPER INTEGRAL EQUIVALENCE ON Q*

Ex: (-1,0,1,3/2,3,5), (-1,0,1,3/2,2,87) are upper integral equivalent.

We will use

ORDER INVARIANT $S \subseteq Q^k$ ($S \subseteq Q[0,n]^k$)

COMPLETELY $Z^+\uparrow$ INVARIANT $S \subseteq Q^k$ ($S \subseteq Q[0,n]^k$)

UPPER INTEGRAL INVARIANT $S \subseteq Q^k$ ($S \subseteq Q[0,n]^k$)

THE STATEMENTS

EVERY SUBSET OF Q^{2k} CONTAINS A MAXIMAL SQUARE.

EVERY ORDER INVARIANT SUBSET OF Q^{2k} CONTAINS A COMPLETELY $Z^{+}\uparrow$ INVARIANT MAXIMAL SQUARE.

EVERY ORDER INVARIANT SUBSET OF Q^{2k} CONTAINS AN UPPER INTEGRAL INVARIANT MAXIMAL SQUARE.

EVERY ORDER INVARIANT SUBSET OF $Q[0,16]^{32}$ CONTAINS A COMPLETELY $Z^{+}\uparrow$ INVARIANT MAXIMAL SQUARE.

EVERY ORDER INVARIANT SUBSET OF $Q[0,16]^{32}$ CONTAINS AN UPPER INTEGRAL INVARIANT MAXIMAL SQUARE.

I use much more than ZFC to prove 2-5. This is required for 4,5. For 2,3, not yet clear if required.

Upper Integral Invariance is the strongest invariance notion that can be used, that satisfies some basic conditions.

DETACHED CHOICE

Let's go back to the beginning, and use a function instead of a square.

EVERY SET OF ORDERED PAIRS CONTAINS A MAXIMAL SQUARE.

EVERY REFLEXIVE SYMMETRIC RELATION HAS A **DETACHED CHOICE FUNCTION.**

Let R be a relation (set of ordered pairs). A detached choice function F for R obeys

i. For all $x \in dom(R)$, $R(x,F(x))$.
ii. For all distinct $x,y \in rng(F)$, $\neg R(x,y)$.

Let R be reflexive and symmetric on A. Take a maximal S such that no two distinct elements of S are R related. For $x \in S$, define $F(x) = x$. For $x \in A\backslash S$, define $F(x) \in A$ so that $R(x,F(x))$ and $F(x)$ in A.

Note that F is a detached choice function for R.

DETACHED CHOICE STATEMENTS

EVERY REFLEXIVE SYMMETRIC RELATION ON Q^k HAS A DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON Q^k HAS A COMPLETELY $Z^+\uparrow$ INVARIANT DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON Q^k HAS AN UPPER INTEGRAL INVARIANT DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $Q[0,16]^{16}$ HAS A COMPLETELY $Z^+\uparrow$ INVARIANT DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $Q[0,16]^{16}$ HAS AN UPPER INTEGRAL INVARIANT DETACHED CHOICE FUNCTION.

A function is ... Invariant iff its graph is.

2-5 proved using much more than ZFC. Required for 4-5.

DETACHED CHOICE STATEMENTS

EVERY REFLEXIVE SYMMETRIC RELATION ON Q^k HAS A DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON Q^k HAS A COMPLETELY $Z^+\uparrow$ INVARIANT DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON Q^k HAS AN UPPER INTEGRAL INVARIANT DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $Q[0,16]^{16}$ HAS A COMPLETELY $Z^+\uparrow$ INVARIANT DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $Q[0,16]^{16}$ HAS AN UPPER INTEGRAL INVARIANT DETACHED CHOICE FUNCTION.

Can we move this show into the positive integers?

Maybe even to $\{1,...,16t\}^{16}$, where t,2t,...,16t are distinguished?

What would the lifting look like here? What would upper integral invariance look like here?

DETACHED CHOICE IN $\{1,...,16t\}^{16}$

We will treat t,2t,...,16t as distinguished.

We use the lifting function $tZ^+\uparrow : Z^{+*} \rightarrow Z^{+*}$ given by:

$tZ^+\uparrow(x)$ is the result of adding t to all coordinates greater than all coordinates outside tZ^+.

THESE BELOW ARE WRONG!

LET t >> 1. EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS A COMPLETELY $tZ^+\uparrow$ INVARIANT DETACHED CHOICE FUNCTION.

Let t >> 1. EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS AN UPPER tZ^+ INVARIANT DETACHED CHOICE FUNCTION.

We must weaken "detached"!!

DETACHED CHOICE IN $\{1,...,16t\}^{16}$

THESE BELOW ARE WRONG!

LET t >> 1. EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS A COMPLETELY $tZ^+\uparrow$ INVARIANT DETACHED CHOICE FUNCTION.

Let t >> 1. EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS AN UPPER tZ^+ INVARIANT DETACHED CHOICE FUNCTION.

We must weaken "detached"!!

RECALL: F is detached iff no two distinct values of F are related.

F is r-detached iff no two distinct values of F are related, provided each is written with at most r applications of coordinate functions of F, and t,2t,..., 16t.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS A COMPLETELY $tZ^+\uparrow$ INVARIANT log(t)/1000-DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS AN UPPER tZ^+ INVARIANT log(t)/1000-DETACHED CHOICE FUNCTION.

DETACHED CHOICE IN $\{1,...,16t\}^{16}$

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS A COMPLETELY $tZ^+\uparrow$ INVARIANT log(t)/1000-DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16t\}^{16}$ HAS AN UPPER tZ^+ INVARIANT log(t)/1000-DETACHED CHOICE FUNCTION.

We can prove these by going well beyond ZFC - and not otherwise.

In fact, these two statements are each provably equivalent to the consistency of certain large cardinal hypotheses.

DETACHED CHOICE IN $\{1,...,16t\}^{16}$

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16(100!!!!!!!)\}^{16}$ HAS A COMPLETELY $100!!!!Z^+\uparrow$ INVARIANT 100!!!!-DETACHED CHOICE FUNCTION.

EVERY ORDER INVARIANT REFLEXIVE SYMMETRIC RELATION ON $\{1,...,16(100!!!!!!!)\}^{16}$ HAS AN UPPER $100!!!!Z^+$ INVARIANT 100!!!!-DETACHED CHOICE FUNCTION.

PRESUMABLY -

These can be proved in ZFC, but only by using more than 100!! symbols.

WHAT IS BEING USED BEYOND ZFC?

Just beyond ZFC is a strongly inaccessible cardinal, which corresponds to Grothendieck universes (big kind).

κ is a strong limit cardinal if and only if for all $\kappa' < \kappa$, $2^{\kappa'} < \kappa$.

κ is a strongly inaccessible cardinal if and only if

i. κ is a strong limit cardinal.
ii. κ is not the supremum of a set of cardinals $< \kappa$ of cardinality $< \kappa$.
iii. κ is uncountable.

WHAT IS BEING USED BEYOND ZFC?

The ones used (and needed) here are a lot bigger than the first strongly inaccessible cardinal.

We think of each cardinal as an ordinal. Each ordinal is the set of all smaller ordinals.

Let κ be an infinite cardinal. We say that $A \subseteq \kappa$ is closed if and only if the sup of any nonempty bounded subset of A without a maximum element, is an element of A.

We say that $A \subseteq \kappa$ is stationary if and only if A meets every closed unbounded subset of κ.

We say that κ has the k-SRP if and only if for any partition of the unordered k-tuples from κ into two pieces, there is a stationary subset of k whose unordered k-tuples all lie in one piece.

We use

for all $1 \leq k < \infty$, some cardinal has the k-SRP.

HOW ARE THESE STATEMENTS PROVED?

We will give a rough sketch of

EVERY ORDER INVARIANT SUBSET OF $Q[0,n]^{2k}$ CONTAINS AN UPPER INTEGRAL INVARIANT MAXIMAL SQUARE.

Let κ be a suitable large cardinal. Let R be an invariant subset of $Q[0,n]^{2k}$.

There is a canonical lifting of R to the k-tuples from any linear ordering. We use $<^* = \kappa \times Q[0,1)$ ordered lexicographically.

We lift R to R^* on $(\kappa \times Q[0,1))^{2k}$.

We now want to build a maximal square $S \times S \subseteq R^*$.

We construct S by transfinite induction along $(\kappa \times Q[0,1))^{2k}$. The problem is that $(\kappa \times Q[0,1))^{2k}$ is not well ordered.

So we modify the ordering, temporarily, by using an enumeration of $Q[0,1)$.

HOW ARE THESE STATEMENTS PROVED?

EVERY ORDER INVARIANT SUBSET OF $Q[0,n]^{2k}$ CONTAINS AN UPPER INTEGRAL INVARIANT MAXIMAL SQUARE.

Let k be a suitable large cardinal, and R be as given. We lift R to R* on $(\kappa \times Q[0,1))^{2k}$.

We construct S by transfinite induction along $(\kappa \times Q[0,1))^{2k}$. Temporarily, we use an enumeration of Q[0,1).

We need to focus on a crucial closed and well ordered subset of $\kappa \times Q[0,1)$. This is $\kappa \times \{0\}$.

Using combinatorics of κ, we obtain an infinite sequence

$\lambda_1 < \lambda_2 < \ldots < \kappa$, where $(\lambda_1,0) <^* (\lambda_2,0) <^* \ldots$ can be moved around a lot in the maximal square S × S.

Focus on $([(0,0),(\lambda_n,0)],<^*,S,(0,0),(\lambda_1,0),\ldots,(\lambda_n,0))$. This is much too large, but behaves exactly how we want $(Q[0,n],<,S',0,\ldots,n)$ to behave, where S′ results from transferring S into Q[0,n].

The transfer is accomplished by a straightforward sequential construction. VERIFY: S′ × S′ is maximal in R just like S × S is maximal in R*.

HOW DO WE PROVE THAT THESE STATEMENTS ARE NOT PROVABLE IN ZFC?

We assume hypothetically that the statement P is true.

We then go through a complicated process that constructs a model of ZFC.

Thus we have a proof, well within ZFC, that

$$P \Rightarrow \text{Con(ZFC)}.$$

Now suppose that P is provable in ZFC. Then ZFC proves Con(ZFC). By Gödel’s Second Incompleteness Theorem, ZFC is inconsistent.

Thus we have established that P is not provable in ZFC, under the (required) assumption that ZFC is consistent.