ARE THE USUAL AXIOMS SUFFICIENT?

by
Harvey M. Friedman
Distinguished University Professor
Mathematics, Philosophy, Computer Science
Ohio State University
Pat Suppes' 90th Birthday
Stanford, March 10, 2012

I am deeply honored to be speaking at Pat's 90th birthday celebration.

Pat was Chairman of the Philosophy Department when I was hired as Assistant Professor of Philosophy right after my Ph.D. in Mathematics from MIT, way back in September, 1967.

Pat Suppes is arguably the greatest polymath on the planet today.

I am going to talk a bit about recent advances in a longstanding project of mine in the foundations of mathematics.

Foundations of mathematics is just one of countless areas in which Pat has made substantial contributions.

After writing two well received textbooks in 1957 and 1960, Pat's main interest in foundations of mathematics went into the direction of the foundations of mathematics as used in the sciences. There is a focus on the foundations of finitism, geometry, and infinitesimal reasoning.

PAPERS BY PAT IN THE FOUNDATIONS OF MATHEMATICS

(1957) *Introduction to Logic*.

(1960) *Axiomatic set theory*.

With N. Moler. (1968) Quantifier-free axioms for constructive plane geometry. (1988)

(1988) Philosophical implications of Tarski's work.

With R. Chuaqui. (1990) An equational deductive system for the differential and integral calculus.

With R. Chuaqui. (1993) A finitarily consistent free-variable positive fragment of infinitesimal analysis.

With R. Chuaqui. (1995) Free-variable axiomatic foundations of infinitesimal analysis: A fragment with finitary consistency proof.

With R. Sommer. (1996) Finite models of elementary recursive nonstandard analysis.

With R. Sommer. (1997) Dispensing with the continuum.

Of course, there are many more contributions to other aspects of logic, by Pat.

THE USUAL AXIOMS FOR MATHEMATICS

I doubt if many of you can recite the commonly accepted axioms for mathematics. But this is not a problem for what I want to say.

The usual setup is ZFC = Zermelo Frankel set theory with the Axiom of Choice.

The variables range over sets, with the single primitive relation of membership (written $\in$). Equality is also usually taken as primitive.

ZFC consists of intelligible axioms about sets, together with the usual axioms and rules of first order predicate calculus with equality.

ZFC is gigantic overkill for the support of mathematical proof. ZFC is so successful as a general foundation for mathematics, that mathematicians today generally have little idea what it is - but are at least aware of its existence.

THE CLASSICAL LIMITATIONS OF ZFC

Yet ZFC does have certain limitations.

An obvious issue concerning ZFC - or, for that matter, any proposed system for supporting mathematical proofs - is whether it supports a contradiction.

Prima facie, any system that supports a contradiction is worthless as a foundation for mathematics.

So we want to be certain that ZFC is consistent (free of contradiction).

Form work of Kurt Gödel, we have the following classical limitation of ZFC:

either ZFC does not prove that ZFC is consistent, or ZFC is not consistent.

The generally accepted view is that the former holds; not the latter.

Furthermore, Gödel's work shows that this situation cannot be repaired by modifying ZFC.

THE CLASSICAL LIMITATIONS OF ZFC

We have learned to accept this first limitation of ZFC:

ZFC does not prove that ZFC is free of contradiction.

However, this does not reveal any limitation of ZFC for any "normal mathematical purpose".

There is a crucial problem in abstract set theoretic mathematics called the continuum hypothesis (CH):

every infinite set of real numbers is in one-one correspondence with the integers or the real numbers.

Gödel (1930s) and Cohen (1960s) established the following limitation of ZFC:

ZFC can neither prove nor refute CH.

The Gödel/Cohen development sparked a substantial development whereby various further limitations of ZFC for abstract set theoretic mathematics were established.

NEW LIMITATIONS OF ZFC

What do we mean by “abstract set theoretic mathematics?”

The key feature of abstract set theoretic mathematics is that extremely general uncountable sets are involved.

In the continuum hypothesis (CH), arbitrary infinite sets of real numbers are involved.

Examination of mathematics reveals that the “reasonable” uncountable sets are Borel measurable subsets of complete separable metric spaces. Even this is far more than what is encountered for normal purposes.

What happens if we are to give a more reasonably concrete formulation of CH?

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

Borel CH is a well known theorem of ZFC from the Polish school. The independence from ZFC is removed in this way.

NEW LIMITATIONS OF ZFC

The New Limitations of ZFC are now much more concrete than Borel measurable sets and functions on the reals.

The New Limitations involve only rather concrete discrete and even finite mathematics.

CAUTION: It is doubtful if any discrete/finite mathematical problems that have already arisen are neither provable nor refutable from ZFC.

But we claim that the new examples are simple and natural and strategic enough to

1. conform to existing standards for normal mathematical investigations of a concrete nature.

2. provide interesting and valued concrete mathematical information.

I am working with leading core mathematicians concerning strategy for integrating the examples further into current concrete mathematical culture.

INVARIANCE IN SETS OF RATIONAL VECTORS

I present a recent example of a simple concrete statement neither provable nor refutable in ZFC.

In fact, the statement are provable using certain far reaching and well studied extensions of the ZFC axioms - but not in ZFC alone.

Let Q be the set of rationals. We begin with the following well known statement.

EVERY SET OF ORDERED PAIRS CONTAINS A MAXIMAL SQUARE.

Here a maximal square is a subset $A \times A$ which is not properly contained in any subset $B \times B$.

In the countable case, this is proved by a straightforward greedy construction.

We are moving towards

EVERY INVARIANT SET OF ORDERED PAIRS CONTAINS AN INVARIANT' MAXIMAL SQUARE.

INVARIANCE IN SETS OF RATIONAL VECTORS

We need to have some structure for invariance. Let Q be the set of all rationals, and Z^+ be the set of all postitive integers.

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

We say that $x,y \in Q^k$ are order equivalent if and only if for all i,j, $x_i < x_j \Leftrightarrow y_i < y_j$.

Ex: (3,-1/2,2) and (2,1,3/2) are order equivalent.

Let $x \in Q^k$. $Z^+\uparrow(x)$ results from adding 1 to all coordinates greater than all coordinates outside Z^+.

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

$S \subseteq Q^k$ is order invariant iff for all order equivalent $x,y \in Q^k$, $x \in S \Rightarrow y \in S$.

$S \subseteq Q^k$ is completely $Z^+\uparrow$ invariant iff for all $x \in Q^k$, $x \in S \Leftrightarrow Z^+\uparrow(x) \in S$.

INVARIANCE IN SETS OF RATIONAL VECTORS

We have proved the following:

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

but only by using far more than ZFC. We don't know if ZFC suffices.

However, we can use $Q[0,16]^{32}$ instead of Q^{2k}, where we restrict to [0,16]. $Z^+\uparrow$ is applied only to $Q[0,16)^{32}$.

We have proved

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

using far more than ZFC, and we know that ZFC does not suffice.

INVARIANCE IN SETS OF RATIONAL VECTORS

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

This statement is very concrete in the following senses.

First of all, it is an easy exercise to construct a finite set of sentences in predicate calculus such that the statement is outright equivalent to their satisfiability. By Gödel’s completeness theorem, the statement is therefore equivalent to the formal consistency of a finite set of sentences in predicate calculus.

Secondly, there is a nondeterministic algorithm, straightforwardly associated with the statement, such that the statement holds if and only if this algorithm can be run for infinitely many steps without reaching an obstruction.

It can also be shown that the statement holds if and only if this algorithm can be run for any given finite number of steps, without reaching an obstruction.

FURTHER EXAMPLES

There are some further examples of statements neither provable nor refutable from ZFC which are a little more involved, and live entirely in initial segments of the natural numbers. These are explicitly finite.

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.