

FOUNDATIONS OF MATHEMATICS: PAST, PRESENT, AND FUTURE

by

Harvey M. Friedman

<http://www.math.ohio-state.edu/~friedman/>

May 31, 2000

1. WHAT IS FOUNDATIONS OF MATHEMATICS?

F.o.m. is the exact science of mathematical reasoning, and related aspects of mathematical practice.

This includes a number of issues about which we know nearly nothing in the way of exact science.

For instance, a mathematician instinctively uses an idea of mathematical naturalness when formulating research questions. But we do not have any idea how to characterize this even in very simple contexts.

In f.o.m. we take into account the actual reasoning of actual mathematicians, and the actual development of actual mathematics.

The previous paragraph could be viewed as a gross understatement. Why shouldn't we be literally studying the actual reasoning of actual mathematicians, and the actual development of actual mathematics?

It turns out, time and time again, in order to make serious progress in f.o.m., we need to take actual reasoning and actual development into account at precisely the proper level. If we take these into account too much, then we are faced with information that is just too difficult to create an exact science around - at least at a given state of development of f.o.m. And if we take these into account too little, our findings will not have the relevance to mathematical practice that could be achieved.

This delicate balance between taking mathematical practice into account too much or too little at a given stage in f.o.m. is difficult and crucial.

It also sharply distinguishes f.o.m. from both mathematics and philosophy. In fact, it positions f.o.m. right in between mathematics and philosophy.

In fact, it is the reason why it is of interest to both mathematicians and philosophers, but also why neither mathematicians nor philosophers are fully comfortable with f.o.m.

From the mathematician's point of view, f.o.m. never takes actual mathematics into account enough. Whereas from the philosopher's point of view, f.o.m. takes actual mathematics into account too much, bypassing a number of classical metaphysical issues such as the exact nature of mathematical objects (e.g., what is a number?).

For example, a philosopher might be disappointed to see that f.o.m. has nothing new to say about just what a natural number really is. And a mathematician might be disappointed to see that f.o.m. has nothing new to say about just why complex variables is so useful in number theory.

Yet I expect that f.o.m. will, some day, say something startling about just what a natural number really is, and also say something startling about just why complex variables is so useful in number theory. It's just that now is not the time where we have any idea how to do this.

In fact, this is an example of where interaction between f.o.m. people and mathematicians and philosophers is not only valuable, but crucial. F.o.m. can serve effectively as a middle man (woman) between the two fields. Can you imagine much fruitful discussion between mathematicians and philosophers today about just what a natural number is, or just why complex variables is so useful in number theory? The gap between the two cultures today is just too great to support much of that.

But I maintain that philosophers can fruitfully talk to f.o.m. people about just what a natural number is, and mathematicians can fruitfully talk to f.o.m. people about just why complex variables is so useful in number theory. And such discussions could well lead to serious progress on these issues. It still may not be the right time for big breakthroughs on these topics. But that is difficult to evaluate without such discussions taking place.

For these reasons, f.o.m. needs to be developed on an interdisciplinary basis. If f.o.m. is pursued without the proper combination of mathematical and philosophical

considerations, then it is in danger of becoming sterile, and cannot realize anything like its full potential.

2. F.O.M. AND COMPUTER SCIENCE.

There has been an enormous development of theoretical and applied computer science over the last few decades. How does this relate to f.o.m.?

At the very beginnings of computer science, computer science was hardly distinguishable from f.o.m. In fact, the exact science of algorithms was a key topic in f.o.m. The notion of algorithm was a central concept in mathematics since antiquity, and turning it into an exact science was an important topic in f.o.m.

In fact, it still is, in my view. From the philosopher's point of view, we still don't have a fully convincing "proof" of Church's Thesis. From the computer scientist's point of view, what f.o.m. people think is missing here is closely related to issues haunting computer science such as lack of absolute measures of complexity via preferred models of (especially parallel) computation. Computer science theory is mostly pursued in terms of the asymptotic, with a big fat constant c which is very difficult to make sense of. Yet applied people who want to actually build things are confronted with actual c 's all the time. It's just that the theory of these c 's is lacking.

But my main point here isn't that f.o.m. is the same as f.o.c.s. (foundations of computer science). It isn't, although there can be considerable overlap.

Instead I want to say that f.o.m. is but one of many foundations fields. There is a general concept of what I call foundational studies that cuts across just about every discipline pursued at the University.

I don't have the time to develop this idea here of foundational studies. But let me just say that f.o.m. is by far the most well developed area in foundational studies.

And note just how long it took for f.o.m. to really get off the ground. This can be credited to the great philosopher Frege with his invention of predicate calculus. Of course, there are other ways of looking at history here, but in any

case it is clear that f.o.m. is really had to wait for the late 19th early 20th century. And this, despite the fact that mathematics has been seriously pursued for perhaps 2500 years.

So the serious development of areas of foundational studies can be expected to be a difficult and sophisticated process.

That is why I think that it is so crucial to learn carefully from the development of f.o.m.

In fact, of all of the areas of foundational studies, it appears that f.o.c.s. is the one that is most closely connected to f.o.m. This makes perfect sense for a number of reasons. Firstly, the mathematical nature of computer science itself. Secondly, because of the special role of discrete mathematics both in computer science and in f.o.m. And thirdly, because of the fact that at the very beginnings, f.o.m. and f.o.c.s. could hardly be distinguished.

3. CRUCIAL DEVELOPMENTS IN THE FOUNDATIONS OF MATHEMATICS.

There is now an exact science of "universally applicable reasoning" through the development of first order predicate calculus with equality.

There is the strong feeling among philosophers and f.o.m. people that fopce carves out a fundamentally important form of reasoning. However, this has yet to be demonstrated in any fully convincing way. In particular, what is so special about first order instead of either higher order or fragments of higher order such as "infinitely many"?

Maybe the right way of looking at fopce is as the unique minimum logic just sufficient to support formalization everywhere. One needs to pin down a clear sense in which "smaller" logics are insufficient to support formalization. E.g., it is a familiar "fact" that propositional logic is too small. Formalization, if it can be done at all, would have unacceptable features of various kinds, including length blowup. Also, one has to get clear the sense in which fopce itself does support formalization everywhere.

There is an aspect of fopce that is usually ignored in modern treatments, which take the domains of models to be sets. The original interpretation of fopce can be taken to have the

domain consist of absolutely everything. Under this approach, a new kind of completeness theorem is needed since, e.g., it is entirely implausible that the axioms for linear ordering have a model. I.e., that the universe of absolutely everything can be linearly ordered.

This leads to various axioms of indiscernibility and new completeness theorems for fopce which properly incorporates the usual completeness theorem. I sometimes give talks about this in Philosophy Departments under the quasi serious name "A complete theory of everything." There is much more to do here.

We now move from universal formalization to the formalization of mathematics in particular. By 1925 the usual formalization of mathematics via the system ZFC (Zermelo Frankel set theory with the axiom of choice) had jelled and has remained the commonly accepted gold standard. It is based on fopce for just a binary relation (for set membership), the special binary relation for equality, and with additional axioms representing fundamental principles about sets.

Here is an example of where over the years one properly takes more and more into account of the actual practice of mathematics.

The original formulation of ZFC is completely useless for actual formalization of mathematics in that it doesn't even support abbreviation power. So one subsequent development is the addition of abbreviation power.

However, as computer systems became more powerful and sophisticated, the idea of creating completely correct proofs with man/machine interaction became feasible. The most developed of such projects goes under the name of Mizar.

Actually, the goals in this "automated theorem proving" community - part of the computer science community - are somewhat different than what I am emphasizing here.

Here I would like to emphasize the project of reworking the usual formalization of mathematics via ZFC into a system that supports formalization of mathematics at the practical level. One wants to be able to read and write in a friendly way so that the formal proofs are very close in structure and length to what the mathematician has in mind. This should be good

enough to support a serious study of the actual structure of actual mathematical proofs. Right now, that is pretty much at the relatively crude stage of simply figuring out what axioms are needed to prove what theorems. This is already a big step beyond the early days of formalization of mathematics, and today generally goes under the name of "reverse mathematics" - an area I set up in the late 60's and early 70's.

I have been involved in a small part of this project of formalizing mathematics at the practical level. And that is the friendly communication of mathematical information. Here one concentrates only on semantic issues, and works out, for instance, a theory of abbreviations which carefully reflects just how mathematicians do their abbreviations. That is already complex, particularly when one gets to issues surrounding change of notation, overloading of symbols, etcetera. But notice also that such issues rear their heads in the design of programming languages. Again, one sees considerable overlap between f.o.m. and various issues in computer science, both theoretical and applied.

We now come to the incompleteness theorems of Gödel.

The first incompleteness theorem asserts that in any reasonable formal system adequate for the formalization of the arithmetic of integers, there remain sentences which cannot be proved or refuted.

The original formulation of this theorem was focused on PA = Peano Arithmetic, an important special case. It applies equally well to the much more powerful system ZFC.

We can apply what the audience probably now views as a recurrent theme in the development of f.o.m. Namely, we can reexamine past spectacular advances in f.o.m. and rethink them in terms of pushing them into a higher level of relevance to mathematical practice.

So how do we want to rethink the first incompleteness theorem in the direction of higher relevance?

Of course, Gödel himself did just this when he went into the direction of the second incompleteness theorem. We will come to that next, but right now I want to go into a different direction.

We can ask: how complicated does a sentence in the language of ZFC or PA have to be to be neither provable nor refutable in, respectively, ZFC or PA?

Put it another way, is it the case that any "simple" sentence of ZFC or PA, respectively, has a proof or refutation in ZFC or PA, respectively?

This turns out to be a very challenging problem under various approaches in various directions. The crudest measure of simplicity is length in primitive notation. Here there are no impressive results at the moment.

I have been recently involved with the closely related project of Diophantine equations in PA. Here the idea is to come up with as large an integer n as one can so that every Diophantine equation with at most n symbols (appropriately measured) either has a solution or can be proved in PA to have no solution. One can even demand also that the proof be short and that the solutions also be reasonably small. The current state of the art - using serious number theory of Baker and Siegel - is about 13. A nice interaction between mathematics and f.o.m.

We now turn to the second incompleteness theorem. This states that for any reasonable formal system, one cannot prove the consistency of that formal system within itself.

Again applying the rethinking method, we can ask what happens if we just want to prove "practical" consistency. I.e., that there is no inconsistency using at most n symbols, where n is pretty large. Here n might represent the number of electrons on the earth, or whatever.

My finite 2nd incompleteness theorem says that it takes asymptotically at least square root of n symbols to prove this. And also that, asymptotically, n^2 symbols suffices.

However, the lower bound result is asymptotic, and hardly means anything with actual formalizations of actual mathematics. Thus this rethinking of the second incompleteness theorem needs to be rethought.

The situation where one system S is trying to prove a form of the consistency of a second stronger system T is even more interesting.

Recall that Hilbert wanted to prove the consistency of all of mathematics within a fragment of arithmetic; e.g., prove the consistency of ZFC within PA. This is impossible by the second incompleteness theorem (unless PA is inconsistent).

Here the lower bound is the same as before. I.e., to prove in S that any inconsistency in T has at least n symbols requires asymptotically n^2 symbols. But the upper bound is only asymptotically 2^n . Yet one suspects that the lower bound is also asymptotically exponential.

However, an asymptotically exponential result would essentially solve $P = NP$ in the negative. Thus this rethinking of the second incompleteness theorem via the finite second incompleteness theorem immediately leads to the famous problems in theoretical computer science - another striking connection between mathematics, philosophy, and computer science.

I now want to speak about some issues regarding the usual axioms for mathematics.

1. Where do the axioms of mathematics come from?
2. The need for a unifying viewpoint that generates these axioms as well as certain extensions of them known as large cardinals.
3. The two universe approach, which is very suggestive.
4. The move for increased relevance of the incompleteness of axiomatic set theory.
5. Previous talk: does mathematics need new axioms? Boolean relation theory, and its promise.