THE MATHEMATICAL MEANING OF MATHEMATICAL LOGIC

by
Harvey M. Friedman
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/

April 15, 2000
Rev. April 21, 2000

I am going to discuss the mathematical meaning of
1. the completeness theorem.
2. the incompleteness theorems.
3. recursively enumerable sets of integers.
4. constructivity.
5. the Ackerman hierarchy.
6. Peano arithmetic.
7. predicativity.
8. Zermelo set theory.
9. ZFC and beyond.

Each of these theorems and concepts arose from very specific considerations of great general interest in the foundations of mathematics (f.o.m.). They each serve well defined purposes in f.o.m. Naturally, the preferred way to formulate them for mathe-matical logicians is in terms that are close to their roots in f.o.m.

However, the core mathematician does not come out of the f.o.m. tradition as does the mathematical logician. Instead, he/she comes out of the much older arithmetic/ algebraic/geometric (a.a.g.) tradition. The significance of these theorems and concepts are not readily apparent from the a.a.g. point of view.

In fact, a full formulation of these theorems and concepts requires the introduction of rather elaborate structures which can only be properly appreciated from a distinctly f.o.m. perspective. In fact, the a.a.g. perspective is of little help in gaining facil-ity with these elaborate structures.

So the core mathematician, steeped in a.a.g, is very unlikely to spend the considerable effort required to understand the meaning of such theorems and concepts. In wading through these develop-ments, he/she will not be putting the a.a.g. perspective to effective use, and will not anticipate any corresponding proportionate a.a.g. payoff.

Of course, there is nothing to prevent a core mathematician from becoming familiar with and being perfectly comfort-able with the f.o.m. tradition. But for various reasons, this has become quite rare.

To give a prime example of what I have in mind, most of these theorems and concepts depend on the syntax and semantics of so called first order predicate calculus with equality. This is a rather elaborate structure which, with proper substantial and detailed discussion, sounds like beautiful music to the ears of an f.o.m. oriented listener - but more like painful, long winded noise to many others.

So in this talk, I want to give *relatively* a.a.g. friendly presentations of these fundamental theorems and concepts from f.o.m. I say *relatively* because I do not attempt to go all the way here. One can go much further. But I do go far enough in the direction of a.a.g. friendliness that the mathematical meaning of these presentations should be apparent to this audience. Bear in mind that the project of systematically giving such a.a.g. friendly treatments is, as far I know, quite new, and raises substantial issues - both technical and conceptual - about which I know very little at the present time.

For many of these presenta-tions, in order to be a.a.g. friendly, I do a certain amount of cheating. For instance, these presentations may be substantially less general than usual, even to the point of focusing on only a few illustrative examples.

1. THE COMPLETENESS THEOREM.

The Gödel completeness theorem for first order predicate calculus with equality (1928) has a very simple formulation: every (set of) sentence(s) that is true in all structures has a proof (in fopce). Of course, this simplicity hides the fact that there is an elaborate system of defini-tions underneath that are not a.a.g. friendly.

I start our treatment with equational logic. Let us consider systems of the form $(D,f_1,...,f_n)$, where D is a nonempty set, $n \geq 0$, and each f_i is a multivariate function from D into D. We allow the arity of the various f_i to be various nonnegative integers. The significance of arity 0 is that of a constant.

At the risk of offending most people in the audience, I call such a system $D = (D, f_1, \ldots, f_n)$ an *algebra*. The type of D is $(k_1, \ldots, k_n)$, where k_i is the arity of f_i.

Ex: Groups. These are certain algebras of type (0,2,1). Here f_1 is the identity element, f_2 is the group operation, and f_3 is the additive inverse operation.

We build terms using the variables x_j, $j \geq 1$, and the functions $f_1, \ldots, f_n$. One is normally pedantic, actually using function symbols $F_1, \ldots, F_n$ standing for unknown actual functions $f_1, \ldots, f_n$.

Ex: In the type (0,2,1) of groups, the terms are just the words. In the type (0,0,2,1,2) of rings, the terms are just the polynomials with integer coefficients.

An equation s = t between terms is said to hold universally in an algebra just in case it is true under all assignments of algebra elements to the variables.

Ex: Groups are the algebras of type (0,2,1) which obey the usual group axioms universaly. Rings are the algebras of type (0,0,2,1,2) which obey the usual ring axioms universally.

What does it mean to say that a given equation ϕ follows from a given set of equations S?

There are two ways to look at this: algebraically and formally.

Under the algebraic approach, this means that ϕ holds universally in every algebra where S holds universally (i.e., every element of S holds universally).

Under the formal approach, this means that one can derive the equation ϕ from the set of equations S. But what is a derivation of ϕ from S?

Just what it means in high school algebra when one first learns to play around with equations.

It means that there is a finite sequence of equations ending with ϕ, where each equation either follows from previous equations by the transitivity and symmetry of equality, or is

obtained from an earlier equation by replacing variables with terms in such a way that the equality of all of the terms replacing the same variable have been previously proved.

THEOREM 1. □ follows from S algebraically iff □ follows from S formally.

COROLLARY 2. □ follows from S algebraically iff □ follows from some finite subset of S algebraically.

Of course, many algebraic contexts are not strictly equational; e.g., fields.

This suggests looking at situ-ations that are almost, but not quite equational. E.g., □ and/or some elements of S are negations of equations. Or implications between equations. Or implications between conjunctions of equations. Or disjunctions of equations.

Most generally, both □ and all elements of S are of the form

*) a conjunction of equations implies a disjunction of equations.

The degenerate cases are handled in an obvious manner.

REMARK: finite sets of statements of the form *) have the same effect as arbitrary combinations involving negation, disjunction, conjunction, and implication.

Once we go all the way up to *), we have passed from equational logic to what is called free variable logic.

It would be interesting to see a systematic treatment of notions of derivation when free variable logic is approached incrementally from equational logic.

In free variable logic, it is clear what we mean by □ follows from S algebraically. So what does "□ follows from S formally" mean here?

For this general context, the most a.a.g. friendly way to go is to avoid derivations and use another algebraic notion.

We say that Φ follows from T locally algebraically iff for every algebra D and assignment α to the variables, if all elements of T are true under α then Φ is true under α. The so called substitution instances of a free variable statement are obtained by replacing identical variables with identical terms.

THEOREM 3. (Herbrand's theorem). Let S be a set of free variable statements and Φ be a free variable statement. Then Φ follows from S algebraically iff Φ follows from a finite set of substitution instances of elements of S locally algebraically.

We can think of this finite set of substitution instances as a "Herbrand proof" of Φ from S, and count the number of occurrences of function symbols as a measure of its size.

COROLLARY 4. (Tarski compactness). Let S be a set of free variable statements and Φ be a free variable statement. Then Φ follows from S algebraically iff Φ follows from a finite subset of S algebraically.

Let S be a set of free vari-able statements. There is an important process of expanding S through the introduction of new symbols that goes back to Hilbert with his ε-calculus. It amounts to a relatively a.a.g. friendly treatment of quantifier logic.

Let $\Phi(x_1,...,x_{n+1})$ be any free variable statement that uses only function symbols appearing in S.

We then introduce a new function symbol F which is n-ary, and add the free variable statement

$$\Phi(x_1,...,x_{n+1}) \rightarrow \Phi(x_1,...,x_n,F(x_1,...,x_n))$$

to S.

We can repeat this process indefinitely, eventually taking care of all free variable statements in this way involving any of the function symbols that eventually get introduced. Any two ways of doing this are essentially equivalent. We write the result as S*.

THEOREM 5. Let S be a set of free variable statements. Any algebra in which S holds universally can be made into an

algebra in which S* holds universally without changing the domain and functions of the original algebra.

COROLLARY 6. Let S be a set of free variable statements and Φ be a free variable statement using only function symbols appearing in S. Then Φ follows from S* algebraically iff Φ follows from S algebraically.

We can compare the least size of a Herbrand proof of Φ from S* and from S. There is a necessary and sufficient iterated exponential blowup in passing from S* to S.

This corresponds to the situa-tion with cut elimination in mathematical logic.

2. THE INCOMPLETENESS THEOREMS.

Gödel's first incompleteness theorem asserts that in any consistent recursively axiomatized formal system whose axioms contain a certain minimal amount of arithmetic, there exist sentences that are neither provable nor refutable. (This is actually a sharpening of Gödel's original theorem due to Rosser). This can be made more friendly by

1) looking only at systems with finitely many axioms;
2) making the "minimal amount of arithmetic" very friendly.

However, formal systems still remain. So we wish to go further and capture the mathematical essence without using formal systems.

To maximize friendliness, we incorporate work of Matiyase-vich/Robinson/Davis/Putnam on Hilbert's 10th problem.

THEOREM 7. Let S be a finite set of statements in free variable logic, including the ring axioms, that hold universally in some algebra. There is a ring inequation that holds universally in the ring of integers but does not follow from S algebraically.

Gödel's second incompleteness theorem is more delicate than his first incompleteness theorem.

It asserts that for any consistent recursively axiomatized formal system whose axioms contain a certain minimal amount of arithmetic, that system cannot prove its own consistency.

(This is actually a sharpening of Gödel's ori-ginal theorem due to several people).

Again, this can be made more friendly as before by

1) looking only at systems with finitely many axioms;
2) making the "minimal amount of arithmetic" very friendly.

However, formal systems still remain, as well as issues concerning appropriate formalizations of consistency. So we go further and capture the mathematical essence without using formal systems.

For this purpose, we introduce the concept of an interpretation. This concept, formalized by Tarski, is normally presented in terms of the first order predicate calculus with equality.

Here we only use interpretations between sets of free variable statements. An inter-pretation of S_1 into S_2 consists of definitions of the functions of S_1 by free variable statements using the functions of S_2 with the property that the translation of each statement in S_1 through these definitions follows from S_2 algebraically.

THEOREM 8. Let S be a finite set of free variable state-ments which hold universally in some infinite algebra. There exists a free variable statement $\Box$ such that $S \cup \{\Box\}$ holds universally in some infinite algebra but is not interpretable into S*.

Theorem 8 follows from the second incompleteness theorem. On the other hand, I don't see how to derive the second incompleteness theorem from Theorem 8.

3. RECURSIVELY ENUMERABLE SETS OF INTEGERS.

Recursively enumerable (r.e.) sets of integers occur throughout math logic. The most common definition is:

There is an algorithm such that S is the set of all integers n for which the algorithm eventually finishes computation when applied to n.

This very simple definition of course depends on having a model of computation. And there is a great deal of robustness

in that any reasonable model of general computation - without regard to resource bounds - will yield the same family of sets of integers.

However, no one at the moment knows a really friendly way of defining what a "reasonable model of general computation" is. So for the purposes of a.a.g. friendliness, we avoid models of computation. We present a known characterization which comes from the solution to Hilbert's 10th problem by Matiyasevich/Robinson/Davis/Putnam 1970.

To begin with, r.e. sets of nonnegative integers are normally considered rather than of integers. $S \subseteq Z$ is r.e. iff $S \subseteq N$ and $-S \subseteq N$ are r.e. The following is a byproduct of Matiyasevich/ Robinson/Davis/Putnam.

THEOREM 9. $S \subseteq N$ is r.e. iff S is the nonnegative part of the range of a polynomial of several integer variables with integer coefficients.

From Matiyasevich 1992 con-cerning nine variable Diophantine representations, one can easily read off the following:

THEOREM 10. $S \subseteq N$ is r.e. iff S is the nonnegative part of the range of a polynomial of 13 integer variables with integer coefficients. 13 can be replaced by higher number.

It is known that 13 cannot be replaced by 2, but can it be replaced by 3? This is open.

There is virtually no understanding of the nonnegative (integral) parts of ranges of polynomials of several rational variables with rational coefficients. It is well known that they are r.e.

4. CONSTRUCTIVITY.

In mathematical logic, con-structivity is treated in terms of certain formal sys-tems based on intuitionistic first order predicate calculus which go back to Heyting. This is definitely not a.a.g. friendly.

In many general contexts, the existence of a constructive proof of a theorem implies a sharper form of that theorem.

That sharper form may be false or open. Great interest may be attached to the sharper form, independently of any interest in the general foundational concept of constructivity.

As a first example, consider the following well known fact:

*) For all polynomials P:Z $\to$ Z of nonzero degree, there are finitely many zeros of P.

A constructive proof of *) would imply the also well known sharper fact:

**) There is an algorithm such that for all polynomials P:Z $\to$ Z of nonzero degree, the algorithm applied to P produ-ces an upper bound on the magnitudes of all zeros of P.

This can be seen to be a special case of the following general principle.

Suppose that there exists a constructive proof of a statement of the form

$(\forall n \in Z)(\exists m \in Z)(R(n,m))$.

Then there exists an algorithm Φ such that

$(\forall n \in Z)(R(n,\Phi(n)))$.

Now consider the obvious statement

#) For all multivariate polynomials P from Z into Z, $\exists$ a value of P whose magnitude is as small as possible.

If #) has a constructive proof then the following sharper statement must hold:

##) There is an algorithm such that for all multivariate polynomials P from Z into Z, the algorithm applied to P produces a value of P whose magnitude is as small as possible.

But using Matiyasevich/Robinson/Davis/Putnam, one can refute ##). Hence #) has no constructive proof.

There are important examples in number theory where the constructivity is not known. E.g., in Roth's theorem about

rational approximations to irrational algebraic numbers, and Falting's solution to Mordell's conjecture.

5. THE ACKERMAN HIERARCHY.

This is a basic hierarchy of functions from Z^+ into Z^+ with extraordinary rates of growth. Yet these rates of growth occur naturally in a number of basic mathematical contexts including the Bolzano Weierstraas theorem and walks in lattice points.

Let $f:Z^+ \to Z^+$ be strictly increasing. We define $f\#:Z^+ \to Z^+$ by $f\#(n) = ff...f(1)$, where there are n f's.

We define the Ackerman hierarchy as follows. Take $f_1:Z^+ \to Z^+$ to be doubling. Take $f_{k+1}:Z^+ \to Z^+$ to be $(f_k)\#$.

Note that f_2 is base 2 exponentiation, and f_3 is base 2 superexponentiation.

BW THEOREM. Let x[1],x[2],... be an infinite sequence from the closed unit interval [0,1]. There exists $k_1 < k_2 < ...$ such that the subsequence $x[k_1],x[k_2],...$ converges.

BW WITH ESTIMATE. Let x[1], x[2],... be an infinite sequence from the closed unit interval [0,1]. There exists $k_1 < k_2 < ...$ such that $|x[k_{i+1}]-x[k_i]| < 1/k_{i-1}^2$, $i \geq 2$.

THEOREM 11. Let $r >> n \geq 1$ and $x[1],...,x[r] \in [0,1]$. There exists $k_1 < ... < k_n$ such that $|x[k_{i+1}]-x[k_i]| < 1/k_{i-1}^2$, $2 \leq i \leq n$.

In the r >> n above, how large must r be relative to n? If n = 11 then $r > f_3(64)$ = an exponential stack of 64 2's. $f_{n-8}(64) < r(n) < f_{n+c}(n+c)$, for some universal c, $n \geq 10$. In fact, it is outrageous earlier than n = 11. We are looking to see just when.

Let $k \geq 1$. A walk in N^k is a finite or infinite sequence $x_1,x_2,... \in N^k$ such that the Euclidean distance between successive terms is exactly 1.

A self avoiding walk in N^k is a walk in N^k in which no term repeats.

Let $x,y \in N^k$. We say that x points outward to y iff for all $1 \leq i \leq k$, $x_i \geq y_i$.

THEOREM 12. Let $x \in N^k$. In every sufficiently long finite self avoiding walk in N^k starting at x, some term points outward to a later term which is at least twice the Euclidean distance from the origin.

Now let W(x) be the least n such that:

in every self avoiding walk in N^k of length n starting at x, some term points outward to a later term which is at least twice the Euclidean distance from the origin

THEOREM 13. $W(2,2,2) \geq 2^{192,938,011}$. $W(1,1,1,1) \geq E^*(102,938,011)$. $\exists c,d > 0$ such that $\forall k,n \geq 1$, $A(k,n+c) \leq W(n,...,n) \leq A(k,n+d)$, where there are k n's.

6. BLOCK SUBSEQUENCES.

For each $k \geq 1$, let n(k) be the length of the longest finite sequence $x_1,...,x_n$ such that no consecutive block

$x_i,...,x_{2i}$

is a subsequence of any other consecutive block

$x_j,...,x_{2j}$.

THEOREM 14. For all $k \geq 1$, n(k) exists.

BRAIN DEAD: n(1) = 3.

GIFTED HIGH SCHOOL: n(2) = 11.

What about n(3)?? n(3) approx. 60? n(3) approx. 100? n(3) approx. 200? n(3) approx. 300?

Bad estimates. E.g., n(3) > 2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2^2.

In fact, n(3) > an exponential stack of 2's of length the above number.

A better lower bound: n(3) > the 7198-th level of the Ackerman hierarchy at 158,386.

What about n(4)?? Let A(n) be the n-th level of the Ackerman hierarchy at n.

THEOREM 15. n(4) > AA...A(1), where there are A(187196) A's.

Now that is a big number.

7. PEANO ARITHMETIC.

Peano arithmetic (PA) is a very fundamental system for f.o.m. It is the formal system that Gödel used to cast his incompleteness theorems.

Here we give an example of what PA cannot handle. The first appropriate example of a genuinely combinatorial nature is Paris/Harrington 1977. Here is a more state of the art example. Below we use | | for the sup norm.

THEROEM 16. Let $n >> k \geq 1$ and $F:[0,n]^k \to [0,n]^k$ obey $|f(x)| \leq |x|$. There exist $x_1 < ... < x_{k+1}$ such that $F(x_1,...,x_k) \leq F(x_2,...,x_{k+1})$ coordinatewise. This cannot be proved in PA.

8. PREDICATIVITY.

Predicativity is the view that it is illegitimate to form a set of integers obeying a property that involves all sets of integers. One is allowed to form sets of integers only through definitions that involve sets of integers that have been previously formed. This view was attrac-tive to Poincare and Weyl and others.

A modification of this view:

impredicativity is useful for normal mathematics only for the purpose of proving the existence of infinite sets of integers of a problematic character.

In this form, the view is demonstrably false, as witnessed by, say, J.B. Kruskal's tree theorem 1960:

KRUSKAL'S THEOREM. Let $T_1,T_2,...$ be finite trees. There exists $i < j$ such that T_i is continuously embeddable into T_j as topological spaces.

(Continuous embeddability of finite trees is a purely combinatorial notion, involving only the vertices and the edge relation.)

Kruskal's proof is blatantly impredicative. Results from mathematical logic show that under the usual formalizations of predicativity, there is no predicative proof of Kruskal's Theorem.

Here is a modified view:

impredicativity cannot be used for proving normal mathematical theorems that involve only finite objects.

Here is a refutation of this.

THEOREM 17. Let T be a sufficiently tall rooted finite tree of bounded valence (splitting). There is an inf preserving embedding of some truncation of T into a taller truncation of T which sends the highest vertices of the former into the highest vertices of the latter.

Results from math logic again show that there is no predicative proof of this finite version of Kruskal's Theorem.

9. ZERMELO SET THEORY.

Zermelo set theory with the axiom of choice, ZC, is a very powerful fragment of the usual axioms and rules of mathematics (ZFC), and is far more than what is needed to formalize nearly all of existing normal mathematics. ZC consists of the axioms of exten-sionality, pairing, union, separation (comprehension), infinity, power set, and choice.

We now give an example of a uniformization theorem from normal real analysis that cannot be proved in ZC. It can, however, be proved in ZFC, using the Replacement axiom.

THEOREM 18. (using D.A. Martin). Let E be a Borel measurable subset of the ordinary unit square which is symmetric about the diagonal. Then E contains or is disjoint from the graph of a Borel measurable function from the unit interval into itself.

10. ZFC AND BEYOND.

Are there examples of discrete or even finite normal mathematics which cannot be carried out within the usual axioms and rules of mathematics as formalized by ZFC?

This question naturally arises since even ZC is overkill for nearly all normal mathematical contexts.

There is ongoing work suggesting that not only are there such examples, but that there is a new thematic subject which cuts across nearly all mathematical contexts, readily digestible at the undergraduate mathematics level, but which can be properly carried out with and only with the use of certain previously proposed new axioms for mathematics going under the name of “large cardinal axioms.”

However, it would be premature for me to report on this work with any specificity at this important gathering, and so I will end this lecture at this time. Thank you very much.