ADVENTURES IN LOGIC FOR UNDERGRADUATES

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

Lecture 5. Foundations of Mathematics

LECTURE 1. LOGICAL CONNECTIVES. Jan. 18, 2011

LECTURE 2. LOGICAL QUANTIFIERS. Jan. 25, 2011

LECTURE 3. TURING MACHINES. Feb. 1, 2011

**LECTURE 4. GÖDEL'S BLESSING AND GÖDEL'S CURSE.
Feb. 8, 2011**

**LECTURE 5. FOUNDATIONS OF MATHEMATICS
Feb. 15, 2011**

SAME TIME - 10:30AM

SAME ROOM - Room 355 Jennings Hall

WARNING: CHALLENGES RANGE FROM EASY, TO MAJOR PARTS OF COURSES

FOUNDATIONS OF MATHEMATICS

In mathematics, we find a huge variety of concepts. We also find “proofs” that we believe are beyond dispute.

But what exactly are the rules of the game? I.e., what are the allowable methods of creating new concepts, and what are the allowable methods of reasoning in proofs?

Some very precise (mathematical!) structures have evolved to address this question. These structures evolved through the efforts and insights of many mathematicians and mathematical philosophers, such as Cauchy, Dedekind, Boole, Cantor, Frege, Russell, Zermelo, Frankel, and others.

The culmination of these efforts has led to the current foundations of mathematics called

the ZFC axiom system.

VARIETY OF MATHEMATICAL CONCEPTS

We find a huge variety of concepts in mathematics. For example: integers, rationals, reals, complexes, addition, subtraction, multiplication, exponentiation, sequence, series, less than, greater than, sets, functions, graphs, relations, member, semigroups, groups, rings, fields, integral domains, vector spaces, topological spaces, continuous functions, differentiable functions, analytic functions, and so forth.

We also have logical notions that allow us to make assertions and do reasoning.

We have already talked about the logical notions in the first two Lectures: the variables $v_1,v_2,...$; the connectives $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$; the quantifiers $\forall,\exists$, and =. These nine items can be reduced, but we gain very little by this, and it is not generally done.

REDUCTION OF MATHEMATICAL CONCEPTS

integers, rationals, reals, complexes, addition, subtraction, multiplication, exponentiation, sequence, series, less than, greater than, sets, functions, graphs, relations, member, semigroups, groups, rings, fields, integral domains, vector spaces, topological spaces, continuous functions, differentiable functions, analytic functions, and so forth.

We keep $v_1, v_2, \ldots, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, =$.

We definitely benefit from sharply reducing the mathematical concepts.

Experience has shown that the most advantageous reduction is to

SETS WITH THE MEMBERSHIP RELATION.

Alternative reductions have been proposed, but none have overthrown this classic standard choice of primitive concepts.

SET THEORETIC FOUNDATIONS OF MATHEMATICS

Everything is a set. The only mathematical relation is membership between sets, written $\in$. I.e., $x \in y$. The logical symbols are $v_1,v_2,\ldots,\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists,=$.

All mathematical concepts are explicitly defined in terms of sets and $v_1,v_2,\ldots,\in,\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists,=$.

All mathematical proofs are conducted within the system ZFC = Zermelo Frankel set theory with the axiom of choice. ZFC looks like this:

1. Axioms and rules of logic for $\in,\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists,=$.
2. Axioms for set theory.

Do mathematicians adhere to ZFC? ABSOLUTELY YES, and ABSOLUTELY NO. We will explain later.

AXIOM OF EXTENSIONALITY

The fundamental EXTENSIONALITY axiom of ZFC says that two sets are equal if and only if they have the same elements.

This is written formally as

$$(\forall z)(z \in x \leftrightarrow z \in y) \rightarrow x = y.$$

This means that in order to define a set, we need only say exactly what its elements are.

This supports set abstraction as a method of defining sets.

There are many other axioms of ZFC, as we shall see.

Set abstraction is introduced on the next page.

SET ABSTRACTION

It is crucial to see how we treat various kinds of mathematical objects as sets, in order to understand the set theoretic foundations of mathematics.

An important set formation construct is set abstraction:

$$\{x: P(x)\}$$

which is read "the set of all x such that P holds of x". I.e., the set consisting of the x such that P(x). I.e., the set whose elements are exactly the x such that P(x).

HOWEVER, there may not be such a set. But

$$\{x \in A: P(x)\}$$

always exists, where A is a set (everything is a set!). This is a very fundamental axiom of set theory called SEPARATION.

WHAT'S WRONG WITH $\{x\colon P(x)\}$? BERTRAND RUSSELL

Let's take a look at $\{x\colon x \notin x\}$. Call this set A.

Is $A \in A$? If so, then A does NOT obey the defining condition for A, namely $x \notin x$. Hence $A \notin A$. But then A DOES obey the defining condition for A. Hence $A \in A$. This is a contradiction.

So $\{x\colon x \notin x\}$ does not exist. This is due to Bertrand Russell (Russell's Paradox). What about $\{x\colon x = x\}$? Suppose this exists, and write $B = \{x\colon x = x\}$. Note that everything is in B. Now write

$$\{x \in B\colon x \notin x\}$$

which must exist because of the B. But this is just $\{x\colon x \notin x\}$, since B is everything. However, this does not exist. Hence $\{x\colon x = x\}$ does not exist.

SINGLETONS, UNORDERED PAIRS, ORDERED PAIRS, EMPTY SET

Define $\{x,y\} = \{z: z = x \vee z = y\}$. The PAIRING AXIOM says that this exists.

Define $\{x\} = \{x,x\} = \{y: y = x\}$.

$\{x,y\}$ is the unordered pair. What about the ordered pair? Any way of defining this is somewhat artificial. Most standard is

$$<x,y> = \{\{x\},\{x,y\}\}.$$

The only thing we care about is this:

CHALLENGE: $<x,y> = <z,w> \rightarrow x = z \wedge y = w$.

We define $\emptyset = \{x: x \neq x\}$.

RELATIONS AND FUNCTIONS

A relation is a set of ordered pairs. I.e., a set all of whose elements are ordered pairs.

It is convenient to write $R[x,y]$ for

$$R \text{ is a relation } \wedge \langle x,y\rangle \in R.$$

This is read “the relation R holds at x,y”.

A function is a relation f such that

$$(\forall x,y,z)(f[x,y] \wedge f[x,z] \rightarrow y = z).$$

It is convenient to write $f(x)$ for

$$\text{the unique } y \text{ such that } f \text{ is a function and } f[x,y].$$

$f(x)$ is read as “the value of the function f at the argument x”. $f(x)$ may or may not exist - even if f is a function.

SUBSETS, DOMAINS, RANGES, UNIONS, INTERSECTIONS, RELATIVE COMPLEMENTS

We define $x \subseteq y$ iff $(\forall z)(z \in x \to z \in y)$.

We define $\mathrm{dom}(x) = \{y\colon x \text{ is a relation} \wedge (\exists z)(x[y,z])\}$.

We define $\mathrm{rng}(x) = \{y\colon x \text{ is a relation} \wedge (\exists z)(x[z,y])\}$.

We define $f{:}A \to B$ iff f is a function $\wedge$ $\mathrm{dom}(f) = A \wedge \mathrm{rng}(f) \subseteq B$.

We define $x \cup y = \{z\colon z \in x \vee z \in y\}$.

We define $x \cap y = \{z\colon z \in x \wedge z \in y\}$.

We define $x\backslash y = \{z\colon z \in x \wedge z \notin y\}$.

Note that \ is relative complement. We don’t have complement: the complement of $\emptyset$ would be $\{x\colon x = x\}$, which doesn’t exist.

NATURAL NUMBERS - INTUITIVE DEFINITIONS

We have seen that the ordered pair's definition is somewhat artificial, but we only care about its crucial property: $\langle x,y\rangle = \langle z,w\rangle \rightarrow x = z \wedge y = w$.

Likewise, natural numbers in set theory are somewhat artificial. First we give four equivalent intuitive definitions.

$0 = \varnothing$. $1 = \{\varnothing\}$. $2 = \{\varnothing,\{\varnothing\}\}$. $3 = \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$. ...

$0 = \varnothing$. $1 = \{0\}$. $2 = \{0,1\}$. $3 = \{0,1,2\}$. $4 = \{0,1,2,3\}$. ...

$n = \{0,1,...,n-1\}$.

$0 = \varnothing$. $n+1 = n \cup \{n\}$.

However clear these intuitive definitions are, they do not constitute a definition of "being a natural number" in set theory.

NATURAL NUMBERS - CRUCIAL PROPERTY

No matter how we define the natural numbers in set theory, we want a crucial property to hold. We want definitions NAT(x), LESS(x,y), where we can prove that

1. LESS defines a strict linear ordering on the x′s with NAT.
2. This linear ordering has a least element and no greatest element.
3. Every nonempty set, all of whose elements have NAT, has a least element under LESS.

CHALLENGE: Give two definitions NAT(x), LESS(x,y), in set theory, and prove 1-3. Tougher: Stay within finite set theory.

CHALLENGE: Suppose NAT(x), LESS(x,y) are two definitions that have properties 1-3. Suppose NAT′(x), LESS′(x,y) are two others. State and prove an isomorphism theorem for (NAT,LESS) and (NAT′,LESS′).

DEVELOPMENT OF NUMBER SYSTEMS

Once we have definitions NAT, LESS, we can explicitly develop the number systems. Yes, there will still be some artificialities, but they will be limited and manageable.

Note that so far we have NOT committed to the existence of infinite sets. In particular, we have not used {x: NAT(x)}.

I.e., we have stayed within what we call FINITE SET THEORY. This is a very good place to be, even though ZFC has an Axiom of Infinity.

We can continue the set theoretic foundations within finite set theory, for the ordered semiring of natural numbers, the ordered ring of integers, and the ordered field of rationals.

When we arrive at the ordered field of reals, we will need the Axiom of Infinity. This is because a general real number is going to have to be an infinite set.

ADDITION ON NATURAL NUMBERS

This requires Cartesian products and binary functions. We define $A \times B = \{<x,y>: x \in A \wedge y \in B\}$.

Let 0 be the least x with NAT(x), and x' be the immediate successor of x, both with respect to LESS. We use $<$ for LESS.

CHALLENGE: Let NAT(x). There is a unique function f with domain $\{y: y < x\} \times \{y: y < x\}$ such that

$$f(<y,0>) = y,\ f(<y,z'>) = f(<y,z>)'$$

provided $0,y,z' < x$.

CHALLENGE: These unique functions agree on their common domains.

We then define $x + y = z$ iff for some such f, $f(<x,y>) = z$.

CHALLENGE: $+,<$ puts an ordered commutative semigroup structure on the natural numbers.

MULTIPLICATION ON NATURAL NUMBERS

CHALLENGE: Let $\mathrm{NAT}(x)$. There is a unique function g with domain $\{y: y < x\} \times \{y: y < x\}$ such that

$$g(<y,0>) = y,\ g(<y,z'>) = g(<y,z>) + y$$

provided $0,y,z' < x$.

CHALLENGE: These unique functions agree on their common domains.

We then define $x \bullet y = z$ iff for some such g, $g(<x,y>) = z$.

CHALLENGE: $+,\bullet,<$ puts a commutative ordered semiring structure on the x with $\mathrm{NAT}(x)$.

SUBTRACTION ON NATURAL NUMBERS
ORDERED RING OF INTEGERS

CHALLENGE: If $x \leq y$ then there is a unique z such that $x+z = y$.

For $x \leq y$, we write $y-x$ for this unique z.

Define the integers to be the natural numbers together with the $\langle 0,x \rangle$, where NAT(x). The $\langle 0,x \rangle$ serve as the negative integers.

CHALLENGE: Define $<,\leq,+,-,\bullet$ appropriately for the integers. Prove that $<,+,-,\bullet$ puts a commutative ordered ring structure on the integers.

For integers x,y, define $x|y$ iff $(\exists z)(x \bullet z = y)$. Write $y \div x$ for this unique z (assuming $x \neq 0$).

CHALLENGE: Let x,y be integers, $y \neq 0$. There is a greatest z such that $z|x \wedge z|y$. This is written gcd(x,y).

ORDERED FIELD OF RATIONALS

To build the rationals, first develop the pre rationals, which are the <x,y>, x,y integers, y > 0.

Define <x,y> + <z,w> = <x•w + y•z,y•w>. <x,y>•<z,w> = <x•z,y•w>. Define <x,y> ≡ <z,w> iff x•w = y•z.

CHALLENGE. ≡ is an equivalence relation on the pre rationals, compatible with +,•.

The rationals are the pre rationals <x,y>, where gcd(x,y) = 1.

CHALLENGE: Every pre rational is ≡ to a unique rational. It is <x÷gcd(x,y),y÷gcd(x,y)>. It is called the reduction.

The sum (product) of rationals is obtained by taking + (•) as pre rationals, and then taking the reduction.

CHALLENGE: +,• puts a commutative field structure on the rationals, using <x,y> < <z,w> iff x•w < y•z.

ORDERED FIELD OF REALS

So far, we have stayed within finite set theory. But now we have to enter the realm of INFINITE SET THEORY.

We take the approach of Dedekind (Dedekind cuts of rationals). This has advantages and disadvantages over other approaches.

We let Q be the set of all rationals. The left cuts in Q are the nonempty A ⊆ Q such that
i. if x < y and y ∈ A, then x ∈ A.
ii. A is not all of Q.

The real numbers are defined to be the left cuts in Q.

Define A + B = {x+y: x ∈ A ∧ y ∈ B}. Define A < B iff A is properly included in B. The definition of A • B is trickier.

CHALLENGE: Define • appropriately. Show that <,+,• puts an ordered field structure on the reals.

ORDERED FIELD OF REAL NUMBERS
COMPLETENESS

We say that x is an upper bound of a set of real numbers if and only if x is at least at large as every element of the set.

CHALLENGE: Prove that every nonempty set of real numbers with an upper bound, has a least upper bound.

FIELD OF COMPLEX NUMBERS

The complex numbers are the $\langle x,y \rangle$, where x,y are real numbers. We define $\langle x,y \rangle + \langle z,w \rangle = \langle x+z,y+w \rangle$, $\langle x,y \rangle \bullet \langle z,w \rangle = \langle x \bullet z - y \bullet w, x \bullet w + y \bullet z \rangle$.

CHALLENGE: Prove that $+,\bullet$ puts a field structure on the complex numbers.

THE FINITE SET THEORETIC UNIVERSE

We now give a description of the finite set theoretic universe using ordinary mathematics. This is quite a rich hierarchy.

Define POW(x) = $\{y: y \subseteq x\}$. This is the power set construction.

Define V(0) = $\emptyset$. V(n+1) = POW(V(n)). V(ω) = $\cup_n$ V(n).

We know from ordinary mathematics that the power set of a finite set is finite, and therefore by induction, each V(n) is finite.

We say that x is transitive iff every element of every element of x is an element of x.

CHALLENGE: Each V(n) is transitive. V(ω) is transitive. Each V(n) $\in$ V(n+1). Each V(n) $\in$ V(ω). No V(n) $\in$ V(n). V(ω) $\notin$ V(ω). Each V(n) is a proper subset of V(n+1). V(ω) is infinite. Every x $\in$ V(ω) is finite.

(V(ω),$\in$) forms a structure. We shall see that it obeys ALL of the axioms of ZFC except one: the Axiom of Infinity.

EXTENSIONALITY, PAIRING HOLD IN $(V(\omega),\in)$

Define $V(0) = \emptyset$. $V(n+1) = POW(V(n))$. $V(\omega) = \cup_n V(n)$.

EXTENSIONALITY: Any two sets with the same elements are equal.

Let $x,y \in V(\omega)$ have the same elements according to $(V(\omega),\in)$. Since $V(\omega)$ is transitive, x,y really have the same elements. Hence $x = y$.

PAIRING: The set consisting of x,y exists.

Let $x,y \in V(\omega)$. Of course $\{x,y\}$ exists. But we need to show that $\{x,y\}$ not only lies in $V(\omega)$, but is, in the opinion of $V(\omega)$, the set consisting of x,y.

Let $x \in V(n)$, $y \in V(m)$. Wlog, $n \leq m$. By $V(n) \subseteq V(m)$, we have, $x,y \in V(m)$. Now $\{x,y\} \subseteq V(m)$. Hence $\{x,y\} \in V(m+1)$. So $\{x,y\} \in V(\omega)$. It is clear that $\{x,y\}$ is the set consisting of x,y in the opinion of $V(\omega)$.

UNION, SEPARATION HOLD IN $(V(\omega),\in)$

Define $V(0) = \varnothing$. $V(n+1) = POW(V(n))$. $V(\omega) = \cup_n V(n)$.
Extensionality, Pairing hold in $(V(\omega),\in)$.

UNION: The set consisting of all elements of elements of x, exists.

Let $x \in V(\omega)$. Let $x \in V(n)$. By transitivity of $V(n)$, the elements of elements of x lie in $V(n)$. Hence the set A of all elements of elements of x is a subset of $V(n)$. Hence $A \in V(n+1)$. Hence $A \in V(\omega)$. In the opinion of $V(\omega)$, A is the set consisting of all elements of elements of x.

SEPARATION: $\{x \in A\text{: } P(x) \text{ holds}\}$ exists.

Let $A \in V(\omega)$. Let $A \in V(n)$. Let $B = \{x \in A\text{: } P(x) \text{ holds in } (V(\omega),\in)\}$. Then $B \subseteq A \subseteq V(n)$. Hence $B \in V(n+1)$. So $B \in V(\omega)$. In the opinion of $V(\omega)$, B is $\{x \in A\text{: } P(x) \text{ holds}\}$.

POWER SET HOLDS IN $(V(\omega),\in)$
RANKS OF ELEMENTS OF $V(\omega)$

Define $V(0) = \emptyset$. $V(n+1) = POW(V(n))$. $V(\omega) = \cup_n V(n)$.
Extensionality, Pairing, Union, Separation hold in $(V(\omega),\in)$.

POWER SET: The set of all subsets of x exists.

Let $x \in V(\omega)$. Let $x \in V(n)$. Then $x \subseteq V(n)$. So every subset of x lies in $V(n+1)$. These are the same as the "subsets of x in the opinion of $V(\omega)$". Hence the set B of all "subsets of x in the opinion of $V(\omega)$" is a subset of $V(n+1)$. Hence $B \in V(n+2)$, $B \in V(\omega)$. Clearly B is the set all subsets of x in the opinion of $V(\omega)$.

Define the rank of $y \in V(\omega)$ as the least n such that $y \in V(n)$.

CHALLENGE: If $x \in y \in V(\omega)$ then the rank of x is smaller than the rank of y.

FOUNDATION, CHOICE HOLD IN $(V(\omega),\in)$

Define $V(0) = \emptyset$. $V(n+1) = POW(V(n))$. $V(\omega) = \cup_n V(n)$.
Extensionality, Pairing, Union, Separation, Power Set hold in $(V(\omega),\in)$.

FOUNDATION: Every nonempty x has an element disjoint from x.

Let $x \in V(\omega)$ be nonempty in the opinion of $V(\omega)$. Then x has an element from $V(\omega)$. Choose y in x of least possible rank. If x,y have a common element z, then the rank of z is smaller than the rank of y. This contradicts the choice of y.

CHOICE: Let A be a set of pairwise disjoint nonempty sets. There is a set that has exactly one element in common with all elements of A.

The elements of $V(\omega)$ are all finite. We apply induction to A. Suppose true for $|A| \leq n$. Let $|A| = n+1$, where in the opinion of $V(\omega)$, A is a set of pairwise disjoint nonempty sets. Apply the induction hypothesis to the result of deleting an element from A. Extend its choice set by one set.

REPLACEMENT HOLDS IN $V(\omega,\in)$

Define $V(0) = \emptyset$. $V(n+1) = POW(V(n))$. $V(\omega) = \cup_n V(n)$. Extensionality, Pairing, Union, Separation, Power Set, Foundation, Choice, hold in $(V(\omega),\in)$.

REPLACEMENT: Suppose $(\forall x \in A)(\exists y)(P(x,y))$. Then $(\exists z)(\forall x \in A)(\exists y \in z)(P(x,y))$.

Let $A \in V(\omega)$. Then A is finite. For each $x \in A$, let n be the least rank of some $y \in V(\omega)$ such that $P(x,y)$ holds in $(V(\omega),\in)$. Let m be the maximum of these n's. Then $(\forall x \in A)(\exists y)$ (y has rank $\leq$ m and $P(x,y)$ holds in $(V(\omega),\in)$). Hence $(\forall x \in A)$ $(\exists y)(y \in V(m)$ and $P(x,y)$ holds in $(V(\omega),\in))$. Set $z = V(m)$. Note that $z \in V(\omega)$.

NOTE: This form of Replacement is a bit stronger than the usual form.

ZFC WITHOUT INFINITY HOLDS IN $(V(\omega),\in)$

Define $V(0) = \emptyset$. $V(n+1) = POW(V(n))$. $V(\omega) = \cup_n V(n)$.
Extensionality, Pairing, Union, Separation, Power Set, Foundation, Choice, Replacement hold in $(V(\omega),\in)$.

ZF consists of the axioms and rules of logic for $\in,\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists,=$, together with Extensionality, Pairing, Union, Separation, Power Set, Foundation, Replacement, Infinity.

ZFC consists of the axioms and rules of logic for $\in,\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists,=$, together with Extensionality, Pairing, Union, Separation, Power Set, Foundation, Replacement, Choice, Infinity.

INFINITY: There exists A, where $\emptyset \in A \wedge (\forall x \in A)(x \cup \{x\} \in A)$.

CHALLENGE: Infinity fails in $(V(\omega),\in)$.

DO MATHEMATICIANS ADHERE TO ZFC?

ABSOLUTELY YES: ZFC is still the gold standard for the axioms used in a proof that do not have to be acknowledged. Rarely, more axioms are used, and sometimes needed. Most commonly, in set theoretic investigations. E.g., the continuum hypothesis, the existence of measurable cardinals. The use of these controversial axioms are required to be acknowledged.

ABSOLUTELY NO: Mathematicians present proofs in free form, and are not tied down to any formalism. ZFC is far too cumbersome for any mathematician to adhere to.

Both are correct. These two answers have been reconciled to a large extent. Very highly sugared forms of ZFC now exist as interactive computer programs. With the help of a computer, absolutely rigorous formal proofs have been created for a large body of theorems - in highly sugared ZFC. See, e.g., MIZAR http://mizar.org/ There are some competitors.