Abstract. We presented a series of four lectures to the Department of Mathematics at Ohio State University, entitled "Adventures in the Foundations of Mathematics". Lecture 1, "The Structure of Proofs", April 28, 2003. Lecture 2, "The Axioms for Mathematics", April 30, 2003. Lecture 3, "Do We Need Less Axioms?", May 5, 2003. Lecture 4, "Do We Need More Axioms?", May 7, 2003. These are the edited notes for the lectures.

VIGRE LECTURES

ADVENTURES IN THE FOUNDATIONS OF MATHEMATICS

LECTURE 1

THE STRUCTURE OF PROOFS

Harvey M. Friedman
Department of Mathematics
Ohio State University
April 28, 2003
http://www.math.ohio-state.edu/~friedman/
friedman@math.ohio-state.edu

In mathematics, we back up our discoveries with rigorous deductive proofs. Mathematicians develop a keen instinctive sense of what makes a proof rigorous. In logic, we strive for a *theory* of rigorous proofs.

In this first lecture, we give an idea of what this theory looks like - in any deductive context.

There are many unexplored issues surrounding this purely deductive aspect of mathematics.

1. PROPOSITIONAL CALCULUS.

But before we talk about proofs, we need to talk about the form of mathematical statements to be considered. After all, a proof is to be a proof of a mathematical statement.

We start with a discussion of a greatly simplified form of mathematical statement. This is usually called the Propositional Calculus, and has many variant names such as the Sentential Calculus, etc.

We will abbreviate the Propositional Calculus as PROP (not a standard abbreviation).

From the point of view of PROP, all mathematical statements are built up from the five connectives

not ($\neg$)
and ($\wedge$)
or ($\vee$)
implies ($\rightarrow$)
iff ($\leftrightarrow$)

Any other part of a mathematical statement is taken as "primitive", or "irreducible".

We need some symbols for these primitive or irreducible parts of mathematical statements.

We use the infinite list $p_1, p_2, \ldots$, called atoms or propositional variables. In practice, we use p,q,r,... until we run out of appropriate letters.

Here are some examples of "formulas" of PROP.

$p \rightarrow p$
$p \quad \neg p$
$p \rightarrow \neg p$
$p \rightarrow q$
$q \rightarrow p$
$(p \rightarrow q) \quad (q \rightarrow p)$
$\neg p \rightarrow q$

Notice that in the last example, $\neg p \rightarrow q$, there is an ambiguity. We might mean either of

$\neg(p \rightarrow q)$
$(\neg p) \rightarrow q$

which are quite different. One has to use enough parentheses. However, too many parentheses are a pain in the ---, and so conventions have arisen that support the use of less parent-theses. The whole business has been carefully worked out in great generality in the theory of formal grammar and parsing algorithms, in theoretical computer science.

All of this is a warm-up to the following inductive definition of the formulas of PROP.

1. every p_n, $n \geq 1$, is a formula of PROP.

2. if A,B are formulas of PROP then so are (¬A), (A ∧ B), (A ∨ B), (A → B), (A ↔ B).
3. formulas of PROP are obtained only by 1,2.

Strictly speaking, none of our seven examples have as many parentheses as is required by this definition. We will not go further into such grammatical issues.

PROP does not adequately reflect statements in real mathematics. E.g., the use of "for all" and "there exists" is an essential component of mathematical statements. We will get to the real thing - predicate calculus - later in the lecture.

These formulas are not meaningless strings of symbols. They have meaning. Let us reexamine the seven:

p → p true no matter what p is
p ∨ ¬p true no matter what p is
p ∧ ¬p false no matter what p is
p → q
q → p this and the previous one have the same status no matter what p,q are
(p → q) ↔ (q → p) true no matter what p,q are
(¬p) → q matters what p,q are

We want a rigorous definition to support such judgments.

The truth values are the items T and F. A truth assignment is a function from the set of atoms into the set of truth values.

Let f be a truth assignment and A be a PROP formula. We inductively define SAT(A,f), which means "A is true under f".

1. SAT(p_n,f) iff f(p_n) = T.
2. SAT(¬A,f) iff not SAT(A,f).
3. SAT(A ∧ B,f) iff SAT(A,f) and SAT(B,f).
4. SAT(A ∨ B,f) iff SAT(A,f) or SAT(B,f).
5. SAT(A → B,f) iff either not SAT(A,f) or SAT(B,f).
6. SAT(A ↔ B,f) iff SAT(A,f),SAT(B,f) both hold, or both fail.

We now return to those seven examples.

p → p. SAT under every truth assignment

p ∨ ¬p. SAT under every truth assignment
p ∧ ¬p. SAT under no truth assignment
p → q.
q → p. this and the previous are SAT under the same truth assignments
(p → q) ↔ (q → p) SAT under every truth assignment
(¬p) → q. SAT under some but not all truth assignments

If SAT(A,f) holds under all truth assignments, then A is said to be a tautology.

We say that A,B are tautologically equivalent iff for all truth assignments f,

SAT(A,f) iff SAT(B,f).

We say that A tautologically implies B iff for all truth assignments f,

if SAT(A,f) then SAT(B,f).

2. HOW TO EARN ONE MILLION DOLLARS OFF OF PROP.

This is generally more than graduate student stipends, even here.

How do we tell whether or not a PROP formula is a tautology?

The obvious way is to try out all truth assignments.

Of course there are infinitely many truth assignments. But there is an easy theorem to the effect that for a given PROP formula, you only have to consider restricted truth assignments which assign only to the atoms that actually occur in the given PROP formula.

If the number of atoms is n, there are exactly 2^n such restricted truth assignments. The PROP formula might well have, say, n distinct atoms, and about n^2 total occurrences of atoms, which is far smaller than 2^n = the number of restricted truth assignments to be looked at.

We would like to have a reasonably efficient computer algorithm that correctly tells us whether we are looking at a tautology. E.g., that runs in computer time bounded by a polynomial in the size of the input.

This kind of talk is made fully rigorous in computational complexity theory. Furthermore, so many problems of this type have shown to be equivalent to each other, that there is a simple name for all such problems, including this one. This problem is called

$$P = NP?$$

It is believed that there is no tautology testing algorithm of the kind we seek, and equivalently,

$$P \neq NP.$$

This problem is among the seven Clay Institute problems, worth 1 million dollars each. See http://www.claymath.org/Millennium_Prize_Problems/

3. PROOFS IN PROP.

We now come to the principal topic in logic - proofs.

We want to discuss proofs of PROP formulas.

Obviously, whatever "proof" means, if a PROP formula has a proof, then it should be a tautology. This is because, in a proof of the kind we are interested in, nothing (substantive) is assumed at the outset, and therefore the atoms could be any assertions whatsoever.

Obviously, the ideal would be for the converse to hold: every tautology has a proof.

We can have this state of affairs in a stupid way - just list all tautologies, and call them axioms. However, we want our solution to reflect only legitimate moves made in actual proofs.

Getting a formal representation that completely and naturally reflects **all** of the moves made in actual mathematical proofs is still very much an open question.

But we don't have to do this. We merely have to reflect enough of them so that every tautology has a proof.

There are almost as many solutions to this problem as there are logic texts. We present one solution.

In this approach, a not too large number of not too complicated tautologies are listed as Axioms. Then the following two rules of inference are provided:

1. Substitution. If a formula A has been proved, then we may consider any substitution instance of A proved. I.e., we can replace equal letters by equal formulas.

2. Modus Ponens. If formulas A and A → B have been proved, then we may consider B proved.

We can think of these proofs as a finite sequence of PROP formulas, each of which is

i) an axiom; or
ii) a PROP formula B, where some A,A → B are previous entries; or
iii) a substitution instance of a previous entry.

THEOREM. (Completeness). Every PROP formula that is an entry in such a proof is a tautology, and every tautology is an entry in such a proof.

We can even be more stringent than i)-iii) and get the same completeness result:

a) a substitution instance of an axiom; or
b) a PROP formula B, where some A,A → B are previous entries.

This is the most elegant solution to the completeness problem, if one is to forget about the fact that the finite list of axioms used is not that small, and some formulas are downright ugly. For an example of such a list of axioms, see the Appendix.

PROBLEM. What is the least n such that there is a finite set of PROP axioms that works under this approach, where each formula in the finite set has at most n occurrences of atoms? Put more generally, how “small” can the finite set of axioms be for completeness?

Normally one wants more from a deductive system. We want to accommodate assumptions.

For this purpose, let S be any set of PROP formulas. An S-proof is a finite sequence of PROP formulas, each of which is

a) a substitution instance of an axiom; or
b) a PROP formula B, where some A, A → B are previous entries; or
c) an element of S.

We say that S tautologically implies a PROP formula A if and only if every truth assignment that satisfies all elements of S also satisfies A.

THEOREM. (Relative completeness). Every PROP formula that is an entry in an S-proof is tautologically implied by S, and every PROP formula tautologically implied by S is an entry in an S-proof.

There is a purely mathematical consequence of this Theorem, that doesn't mention proofs (i.e., is purely semantic).

THEOREM. (Compactness). If S tautologically implies A then some finite subset of S tautologically implies A.

The Compactness theorem can be looked at topologically. The mathematical essence of this situation is equivalent to the fact that the Cantor space is compact. The space of all truth assignments is a copy of the Cantor space.

4. PREDICATE CALCULUS WITHOUT QUANTIFIERS.

All of this is warm-up for the much more subtle Predicate Calculus, written PRED.

The predicate calculus supports "quantification". The two quantifiers are

∀ (for all - universal quantifier)
∃ (there exists - existential quantifier).

But "for all what?" "there exists what?"

We clearly need an apparatus that refers to objects. In PROP we only have the apparatus that refers to statements - i.e., the atoms.

We introduce the apparatus necessary for referring properly to objects, and then postpone dealing seriously with quantifiers until later in the lecture.

Let us start with the example of groups. Groups are based on 0, a binary operation +, a unary operation -, and =. The usual group axioms are

G1. x + 0 = x.
G2. x + (-x) = 0.
G3. (x + y) + z = x + (y + z).

Ordered Abelian groups have more structure. They are based on 0,+,-,<,=, with the axioms

OAG1. x + 0 = x.
OAG2. x + (-x) = 0.
OAG3. (x + y) + z = x + (y + z).
OAG4. x + y = y + x.
OAG5. (0 < x □ 0 < y) □ 0 < x + y.
OAG6. □ 0 < 0.
OAG7. 0 < x 0 < -x x = 0
OAG8. x < y □ 0 < y + (-x).

Here 0 is a constant symbol, + is a binary function symbol, - is a unary function symbol, < is a binary relation symbol, and = is the special binary relation symbol whose meaning is fixed.

Note that these statements are interpreted universally, with the universal quantifiers suppressed.

This motivates the so called free variable predicate calculus, which we will write as FVPRED.

The vocabulary of FVPRED is

1. □, □, , □ , □ .
2. variables x_n, n ≥ 1.
3. constant symbols c_n, n ≥ 1.
4. function symbols F^n_m, n,m ≥ 1.
5. relation symbols R^n_m, n,m ≥ 1.
6. special relation symbol =.
7. comma and parentheses.

As in PROP, we wish to define the FVPRED formulas. But before this, we first have to define the FVPRED terms.

E.g., in the group axioms, we see the terms

x, x + 0, x + (-x), 0, (x + y) + z, x + (y + z).

The terms of FVPRED are defined inductively:

i. every variable is a term.
ii. every constant symbol is a term.
iii. for n,m ≥ 1, if $t_1,...,t_n$ are terms then $F^n_m(t_1,...,t_n)$ is a term.

The formulas of FVPRED are defined inductively:

a. if s,t are terms then s = t is a formula.
b. for n,m ≥ 1, if $t_1,...,t_n$ are terms then $R^n_m(t_1,...,t_n)$ is a formula.
c. if A,B are formulas then (¬A), (A ∨ B), (A ∧ B), (A → B), (A ↔ B) are formulas.

Formulas falling under a,b are called atomic formulas.

Let us come back to groups. It is well known that the group axioms imply

G4. 0 + x = x.
G5. (-x) + x = 0.
G6. --x = x.
G7. -0 = 0.

We want to support such a claim in FVPRED.

Accordingly, let S be a set of formulas of FVPRED, and let A be a formula of FVPRED. We want to define "S universally implies A". As a special case, we want to verify that "The group axioms {G1,G2,G3} universally imply each of G4,G5,G6,G7.

Obviously, this situation is much more involved than the truth assignments of PROP.

The strategy is to first define a structure (as in algebraic structure, such as an ordered group). Then to define variable assignments. Then to define SAT of a formula under a variable assignment in a structure. Then to define universal SAT of a set of formulas in a structure. Finally, define S universally implies A.

A relational structure consists of a nonempty set D called the domain, together with interpretations of all constant, function, and relation symbols. Constant symbols are interpreted as elements of D. Function symbols with superscript n are interpreted as n-ary functions from D into D. Relation symbols with superscript n are interpreted as n-ary relations on D.

= is understood to be special, always being interpreted as equality on D.

Typically, we only care about the interpretations of just some of the constant, relation, and function symbols. E.g., an ordered group (G,0,+,-,<) is a relational structure where we only care about the interpretations of one constant symbol, one binary function symbol, one unary function symbol, and one binary relation symbol. We take = for granted in FVPRED, with its usual meaning.

Let M be a relational structure. A variable assignment in M, or an M-assignment, is a function f from the set of variables into the domain of M, dom(M).

Let A be a formula. We wish to define SAT(M,A,f). This is read "M satisfies A under f", or "A holds in M under f".

Before we can define SAT(M,A,f), we must first define the values of terms.

We define VAL(M,t,f), the value in M of t under f", inductively as follows.

1. $Val(M,x_n,f) = f(x_n)$.
2. $Val(M,c_n,f)$ is the interpretation of c_n in M.
3. $Val(M,F^n_m(t_1,...,t_n),f) = F(Val(M,t_1,f),...,Val(M,t_n,f))$, where F is the interpretation of F^n_m in M.

We are now prepared to inductively define SAT(M,□,f) as follows.

a. SAT(M,s = t,f) iff VAL(M,s,f) = VAL(M,t,f).
b. $SAT(M,R^n_m(t_1,...,t_n),f)$ iff $R(VAL(M,t_1,f),...,VAL(M,t_n,f)$, where R is the interpretation of R^n_m in M.
c. SAT(M,(□A),f) iff not SAT(M,A,f).
d. SAT(M,(A □ B),f) iff SAT(M,A,f) and SAT(M,B,f).
e. SAT(M,(A B),f) iff SAT(M,A,f) or SAT(M,B,f).

f. SAT(M,(A → B),f) iff either not SAT(M,A,f) or SAT(M,B,f).
g. SAT(M,(A ↔ B),f) iff either SAT(M,A,f),SAT(M,B,f) both hold, or SAT(M,A,f),SAT(M,B,f) both fail.

We now define SAT(M,A). Here we have suppressed the f. This means that for all M-assignments f, SAT(M,A).

More generally, let S be a set of formulas and f be an M-assignment.

We take SAT(M,S,f) to mean that SAT(M,A,f) holds for all A ∈ S. We take SAT(M,S) to mean that SAT(M,A) holds for all A ∈ S.

We come back to groups and ordered Abelian groups. A group is simply a structure M such that SAT(M,{G1,G2,G3}). In M, we suppress the interpretations of all but 0,+,-.

An ordered group is obviously a structure M such that SAT(M,{OAG1,OAG2,OAG3,OAG4,OAG5,OAG6,OAG7,OAG8}). In M, we suppress the interpretations of all but 0,+,-,<.

Finally, we define "S universally implies A". This means that for all structures M, if SAT(M,S) then SAT(M,A).

Consider the correct statement "in every group G, 0 + x = x holds universally". This is obviously equivalent to "{G1,G2,G3} universally implies 0 + x = x".

5. PROOFS IN FREE VARIABLE PREDICATE CALCULUS.

There is a fundamental theorem to the effect that for all sets of formulas S in FVPRED and formulas A in FVPRED, S universally implies A iff there is a proof of A from S in some appropriate deductive system.

We will make use of an obvious extension of the notion of tautology to the context of FVPRED.

We have already defined the formulas of FVPRED. An atomic formula is a formula of FVPRED that has no connectives.

A truth assignment for FVPRED is a function from the set of atomic formulas into the set of truth values {T,F}.

Using this definition, we define SAT(A,h) for truth assignments h, exactly as we did for PROP.

We say that A is a tautology in FVPRED iff SAT(A,h) holds for all truth assignments h.

Do not confuse SAT(A,h) with our earlier notion SAT(M,A,f).

We now present a proof system for FVPRED. It will be convenient to leverage off of PROP.

The equality axioms consist of the following formulas.

1. x = x, where x is a variable.
2. x = y → t = t', where x,y are variables and t' is the result of replacing zero or more occurrences of x in t by y.

Let S be a set of formulas of FVPRED. An S-proof is a finite sequence of formulas of FVPRED such that every entry is

i. a tautology; or
ii. an equality axiom; or
iii. an element of S; or
iv. a term substitution instance of a previous entry; or
v. a formula B where some A,A → B are earlier entries.

Here term substitution instances result in the replacement of variables by terms, the same variables being replaced by the same terms.

We can be more restrictive as follows:

i. a tautology; or
ii. an equality axiom; or
iii'. a term substitution of an element of S; or
v. a formula B where some A,A → B are earlier entries.

THEOREM. (Relative completeness). S logically implies A iff A is an entry in some S-proof (using i-v or using i,ii,iii',v).

As in PROP, we have the following consequence, which does not involve proofs (i.e., is purely semantic).

THEOREM. (Compactness theorem). If S universally implies A then some finite subset of S universally implies A.

Will you get a check for a million dollars if you find an efficient procedure for testing whether A universally implies B in FVPRED?

Definitely, since this is known to be impossible.

THEOREM. There is no algorithm for testing whether A universally implies B, in FVPRED.

6. PREDICATE CALCULUS.

We now discuss the full Predicate Calculus, PRED.

Let L(x,y) be "x loves y". We need to support such statements as

1. Everybody loves somebody.
2. Somebody loves everybody.
3. Everybody is loved by somebody.
4. Somebody is loved by everybody.

We want to know, rigorously, what the logical relationships are here.

2 logically implies 3. 4 logically implies 1. There are no other logical implications.

1. Everybody loves somebody. $(\forall x)(\exists y)(L(x,y))$.
2. Somebody loves everybody. $(\exists x)(\forall y)(L(x,y))$.
3. Everybody is loved by somebody. $(\forall x)(\exists y)(L(y,x)$.
4. Somebody is loved by everybody. $(\exists x)(\forall y)(L(y,x))$.

The vocabulary of PRED is the same as for FVPRED except that we also have the two quantifiers $\forall, \exists$, read "for all", "there exists".

The terms of PRED are the same as the terms of FVPRED. In the definition of formulas, we have to add this additional clause for the quantifiers:

d. If A is a formula and x is a variable, then $(\forall x)(A)$, $(\exists x)(A)$ are formulas.

We define relational structures, M-assignments (variable assignments), and VAL(M,t,f) as before.

The inductive definition of SAT(M,t,f) needs two additional clauses to take care of the quantifiers.

h. SAT(M,($\forall x_n$)(A),f) iff for all d $\in$ D, SAT(M,A,f[x_n/d]).
i. SAT(M,($\exists x_n$)(A),f) iff there exists d $\in$ D such that SAT(M,A,f[x_n/d]).

Here f[x_n/d] is the same as f except that it is forced to be d at the argument x_n.

We define SAT(M,A) iff for all M-assignments f, SAT(M,A,f). We define SAT(M,S,f) iff for all A $\in$ S, SAT(M,A,f). We define SAT(M,S) iff for all A $\in$ S, SAT(M,A). Finally, we say that A is valid iff SAT(M,A) holds for all relational structures M.

Note that all of the definitions in the previous paragraph read exactly the same as those made for FVPRED, but take into account a wider class of formulas (same structures and same assignments).

We say that S universally implies A iff for all relational structures M, if SAT(M,S) then SAT(M,A). This also reads the same as for FVRED.

The tautologies of PRED are defined the same way as the tautologies of FVPRED, except that instead of just using the atomic formulas as the "basis", we also use the formulas of PRED that begin with a quantifier. So the h's now have domain the set of all formulas of PRED that either atomic or begin with a quantifier.

A formula A of PRED is said to be valid if and only if for all structures M, SAT(M,A). This notion is crucially important in the development of PRED, but not in FVPRED. This is because in FVPRED, a formula is valid if and only if it is a tautology.

7. PROOFS IN PREDICATE CALCULUS.

Of course, there are almost as many solutions to Completeness as there are logic books. Here is one well known solution.

A proof is a finite sequence of formulas such that each entry is

1. a tautology; or
2. an equality axiom; or
3. of the form $(\forall x)(A) \rightarrow A[x/t]$; or
4. of the form $A[x/t] \rightarrow (\exists x)(A)$; or
5. of the form $A \rightarrow (\forall x)(B)$ where $A \rightarrow B$ is a previous entry; or
6. of the form $(\exists x)(A) \rightarrow B$ where $A \rightarrow B$ is a previous entry; or
7. a formula B, where some $A, A \rightarrow B$ are previous entries.

Here A,B are formulas of PRED and A[x/t] is the result of replacing all free (i.e., unquantified) occurrences of x in A by the term t.

There are technical restrictions needed on 3-6. We give these restrictions in the Appendix.

Here are some illustrative examples as to what can go very wrong without these technical restrictions on 3-6.

In 3, $(\forall x)(\exists y)(R(x,y)) \rightarrow (\exists y)(R(y,y))$ is bad, using t = y.

In 4, $(\exists y)(R(y,y)) \rightarrow (\forall x)(\exists y)(R(x,y))$ is bad, using t = y.

In 5, $R(x) \rightarrow (\forall x)(R(x))$ from $R(x) \rightarrow R(x)$ is bad.

In 6, $(\forall x)(R(x)) \rightarrow R(x)$ from $R(x) \rightarrow R(x)$ is bad.

THEOREM. (Completeness). A formula in PRED is valid iff it is an entry in some proof.

Let S be a set of formulas of PRED. An S-proof is the same as a proof except that an entry is allowed to be any element of S.

THEOREM. (Relative completeness). S universally implies A in PRED iff A is an entry in some S-proof.

THEOREM. (Compactness). In PRED, S universally implies A iff some finite subset of S universally implies A.

8. SOME OPEN ISSUES.

The complete and relatively complete systems we have presented fall into the category of what are called Hilbert systems. Although they serve the limited purposes we have discussed quite well, they are not set up to closely reflect what is going on, logically, in actual mathematical proofs, polished or otherwise.

Other breeds of systems called sequent calculi and natural deduction systems, are at least partially intended to more closely reflect actual logical reasoning.

A number of important results concerning these alternative systems establish that certain of the rules can be eliminated. The focus has been on “cut elimination” and the related normalization. However, I am confident that a systematic study of just what rules can or cannot be eliminated, and at what cost, driven by the examination of actual mathematical proofs, will be quite interesting.

Another issue is more pragmatic. There is the problem of developing a deductive system that makes it easy to read and write mathematical proofs. There is a lot to do in this direction, even if we restrict our attention to the rigorous presentation of mathematical assertions - before we even consider proofs.

It is commonly believed among logicians that completely formal proofs can be constructed for even the deepest and most complex state of the art mathematics. Put differently, that completely formal proofs of the entire mathematical corpus, put on paper in a normal sized font, could fit into a large hall.

Mathematicians are perhaps skeptical, with some underlying feeling that since proofs have to be “felt” to be understood, there may be substantial “jumps” made that are clear to humans, but which, when fully unraveled, could exponentiate the size of a formal proof.

I side with the logicians on this, but developing the tools to make this convincing is an interesting problem.

APPENDIX

A well known complete formal system for PROP based on only the two connectives $\Box, \Box$, is as follows. We follow standard

conventions concerning the elimination of unnecessary parentheses.

Axioms.

$p \to (q \to p)$
$(p \to (q \to r)) \to ((p \to q) \to (p \to r))$
$(\neg q \to \neg p) \to ((\neg q \to p) \to q)$.

Rules.

from A and $A \to B$, derive B.
from A derive any substitution instance of A.

Alternatively,

from A and $A \to B$, derive B.
from any axiom derive any substitution instance.

This system was taken from Elliot Mendelson, Introduction to Mathematical Logic, Van Nostrand, 1964.

The remaining connectives $\wedge$, $\leftrightarrow$, $\vee$, can be introduced as abbreviations in the well known way, or we can expand the set of axioms to accommodate them. A crude but systematic expansion of the set of axioms is as follows.

$p \to (q \to p)$
$(p \to (q \to r)) \to ((p \to q) \to (p \to r))$
$(\neg q \to \neg p) \to ((\neg q \to p) \to q)$
$(p \to q) \to \neg(p \to \neg q)$
$\neg(p \to \neg q) \to (p \to q)$
$(p \leftrightarrow q) \to ((\neg p) \to q)$
$((\neg p) \to q) \to (p \leftrightarrow q)$
$(p \to q) \to \neg((p \to q) \to \neg(q \to p))$
$\neg((p \to q) \to \neg(q \to p)) \to (p \to q)$.

Again we can use either of the two versions of the rules.

We give the restrictions that have to be made in the following complete axiomatization for PRED.

1. a tautology; or
2. an equality axiom; or
3. of the form $(\exists x)(A) \to A[x/t]$; or
4. of the form $A[x/t] \to (\exists x)(A)$; or

5. of the form A → (∀x)(B) where A → B is a previous entry; or
6. of the form (∃x)(A) → B where A → B is a previous entry; or
7. a formula B, where some A,A → B are previous entries.

Here A[x/t] is the result of replacing each free occurrence of x in A by the term t.

We require the following.

a. In 3,4, t is substitutable for x in A, in the sense that no free occurrence of x lies within the scope of a quantifier that uses a variable appearing in t.
b. In 5, x is not free in A.
c. In 6, x is not free in B.

For the definitions of free variable, free occurrence, scope, and substitutability (of terms for variables), consult any logic text or any logician.

LECTURE 2
THE AXIOMS FOR MATHEMATICS

Harvey M. Friedman
Department of Mathematics
Ohio State University
April 30, 2003
http://www.math.ohio-state.edu/~friedman/
friedman@math.ohio-state.edu

In logic, mathematics is viewed as proceeding by rigorous deduction starting with certain axioms for mathematics. Such axioms are needed in order to support the varied constructions of mathematical objects that occur throughout mathematics. The most effective way known to achieve such unified foundations for mathematics is through the axioms for set theory, and the set theoretic interpretation of mathematics. In this second lecture, we discuss the standard ZFC axioms (Zermelo Frankel set theory with the axiom of choice). On one hand, ZFC seems like overkill, since so little of its power is really used in typical mathematical contexts. On the other hand, ZFC is known to be insufficient in certain kinds of mathematical contexts.

The set theoretic interpretation of mathematics uses what is called pure set theory, where absolutely every object is a set and the only relations between sets are that of

membership and equality. Even natural numbers must be defined as certain sets.

1. HEREDITARILY FINITE SETS.

We begin with a discussion of the finite part of (pure) set theory. In this section we will proceed purely mathematically, taking the natural numbers as given, as well as standard mathematical concepts such as "finite".

However, in set theory, everything is a set, including natural numbers. All concepts must be defined in terms of sets. In section 2, we fill in these gaps.

A particularly fundamental principle of set theory asserts that two sets are equal iff they have the same elements. When we discuss axioms (later), this will be called the Axiom of Extensionality.

The set with no elements is called the empty set, and is denoted by $\emptyset$. If $x_1,...,x_n$ are any objects whatsoever, we write $\{x_1,...,x_n\}$ for the set whose elements are exactly $x_1,...,x_n$. By extensionality, repetitions don't count.

We are now going to define an infinite sequence of particular sets, indexed along the natural numbers, by recursion.

$$V(0) = \emptyset.$$
$$V(n+1) \text{ is the set of all subsets of } V(n).$$

We use S for the power set. Thus we can rewrite the above as

$$V(0) = \emptyset.$$
$$V(n+1) = S(V(n)).$$

The V(n)'s are rather intricate, and enjoy a number of interesting properties which can be verified by induction on n.

We "compute" a few of these V(n)'s as follows.

$$V(1) = \{\emptyset\}.$$
$$V(2) = \{\emptyset, \{\emptyset\}\}.$$
$$V(3) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

We call a set transitive iff every element of an element is an element. We use |x| for the cardinality of the finite set x.

EXERCISE. For all nonnegative integers n,
i) $|V(n+1)| = 2^{|V(n)|}$;
ii) $V(n) \subseteq V(n+1)$;
iii) V(n) is transitive;
iv) $V(n) \in V(n+1)$;
v) $V(n) \notin V(n)$;
vi) every element of V(n) is finite.

A set is said to be hereditarily finite iff it is a member of some V(n).

We will henceforth abbreviate the adjective “hereditarily finite” by HF. (HF is my initials, but I can assure you that this is totally accidental).

Let x be a set. We say that y is an $\in$ minimal element of x iff

a) y lies in x;
b) no element of x lies in y.

We say that y is an $\in$ maximal element of x iff

c) y lies in x;
d) no element of x has y in it.

EXERCISE. Every nonempty HF set has an $\in$ minimal element.

EXERCISE. Every nonempty HF set has an $\in$ maximal element.

EXERCISE. Every element of an HF set is HF. Every subset of an HF set is HF. Every finite set of HF sets is HF.

The existence of the set of all HF sets is a major step that we don’t take just yet. We will come back to this later.

EXERCISE. The set of all HF sets, if it exists, is not an HF set.

There is a way of characterizing the HF sets without building the V(n)’s. The transitive closure of a set is the

least transitive superset of that set. (We won't worry about the existence of the transitive closure right now).

EXERCISE. A set is HF iff its transitive closure is finite.

Finally, recall the common set theoretic operations:

$x \cup y = \{z: z \in x \text{ or } z \in y\}$.
$x \cap y = \{z: z \in x \text{ and } z \in y\}$.
$x \backslash y = \{z: z \in x \text{ and } z \notin y\}$.

EXERCISE. If x,y are HF, then so are $x \cup y$, $x \cap y$, $x \backslash y$.

2. FINITE MATHEMATICS IN HEREDITARILY FINITE SET THEORY.

Recall that in the (set theoretic) foundations of mathematics, everything is going to be a set, and the only relations between sets are going to be that of membership and equality.

Correspondingly, in the (set theoretic) foundations of finite mathematics, everything is an HF set, and the only relations between such sets are that of membership and equality.

We now discuss several of the constructions that are used for the foundations of finite mathematics in the HF sets.

First, we need a workable way to interpret the natural numbers as HF sets. A very convenient way was discovered by von Neumann.

Here are the first five von Neumann natural numbers:

$$\emptyset$$
$$\{\emptyset\}$$
$$\{\emptyset, \{\emptyset\}\}$$
$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$
$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}.$$

These five are denoted by 0,1,2,3,4.

We can define these "numbers" by recursion on the natural numbers from ordinary mathematics, as follows. $0^* = \emptyset$. $(n+1)^* = n^* \cup \{n^*\}$.

We say that x is a NN (natural number) if and only if x is some n*.

EXERCISE. For all n,
i) |n*| = n;
ii) n* = {0*,1*,...,(n-1)*};
iii) n* is transitive;
iv) n* $\in$ (n+1)*;
v) n* $\subseteq$ n*;
vi) n* is HF.

EXERCISE. For all n,m, n < m $\leftrightarrow$ n* $\in$ m*. For all n,m, n* $\subseteq$ m* $\vee$ m* $\subseteq$ n* $\leftrightarrow$ n* = m*.

Note that not every subset of a NN is a NN. E.g., {1*} is not a NN.

EXERCISE. The set of all NN, if it exists, is not HF.

There is a way of characterizing the NN without building them by induction.

We say that a set x is $\in$ connected iff

for all y,z $\in$ x, y $\in$ z or z $\in$ y or y = z.

EXERCISE. A set is a NN iff it is transitive, $\in$ connected, and finite.

Ordered pairs are essential. For HF x,y, we define

$$\langle x,y\rangle = \{\{x\},\{x,y\}\}.$$

The crucial fact that makes this work is this.

EXERCISE. For HF x,y,z,w, $\langle x,y\rangle = \langle z,w\rangle \leftrightarrow (x = z \wedge y = w)$.

Now we can introduce functions. Let x be HF. We say that x is a function if and only if

i) every element of x is an ordered pair;
ii) if $\langle y,z\rangle,\langle y,w\rangle \in x$ then z = w.

For HF x, we define

$$dom(x) = \{y: (\exists z)(\langle y,z\rangle \in x)\}.$$

For HF x, we define

$$rng(x) = \{y: (\exists z)(\langle z,y\rangle \in x).$$

EXERCISE. If x,y are HF, then dom(x),rng(x) are HF.

We define

$$x(y) = z \leftrightarrow \langle y,z\rangle \in x.$$

We write

$$x:y \to z \leftrightarrow (x \text{ is a function } \wedge dom(x) = y \wedge rng(x) \subseteq z).$$

Let x,y be HF. We define

$$x \bullet y = \{\langle z,w\rangle: z \in x \wedge w \in y\}.$$

EXERCISE. Let x,y be HF. $x \bullet y$ is HF. The set of all functions from x into y is HF.

Let x be HF. We say that x is a finite sequence iff x is a function whose domain is a NN.

We need the theory of cardinality for HF sets.

EXERCISE. Let x be HF. There is a one-one function from x onto a unique NN. We write |x| for this unique NN.

EXERCISE. Let x be HF. Every function from x onto x is one-one, and every one-one function from x into x is onto.

We now indicate how we develop the usual number systems with the usual arithmetic operations and order. In finite mathematics, we have, principally, the ordered ring of integers, and the ordered field of rationals.

The essence of this is addition and multiplication on the NN.

We made the following definitions by recursion. Define $S(n^*) = n^* \cup \{n^*\}$. It is easy to see that $S(n^*) = (n+1)^*$, $S(n^*) = S(m^*) \leftrightarrow n^* = m^*$, and $S(n^*) \neq 0^* = \emptyset$. Also we define

$$n^* + 0^* = n^*.$$

$$n^* + S(m^*) = S(n^* + m^*).$$

$$n^* \cdot 0^* = 0^*.$$
$$n^* \cdot S(m^*) = (n^* \cdot m^*) + n^*.$$

Some serious argument is needed to support these two definitions by recursion.

For the first pair of equations, we prove that for all n^*, there exists a unique function f_n with domain NN such that $f(0^*) = n^*$ and each $f(S(m^*)) = S(f(m^*))$. To prove this, fix n. Then prove by induction that for all r, there is such a unique function that works for m^* from 0 through r. Then these functions can be put together into the desired single function.

Using these unique functions f_n, we prove that for all n^*,m^*, there exists a unique function g with domain $n^* \bullet m^*$ such that $g(n^*,m^*) = f_n(m^*)$.

The second pair of equations is handled similarly, with the help of g from the previous paragraph.

Armed with these equations, we can proceed by induction to prove many facts about the NN under addition and multiplication, including the commutativity and associativity of addition and multiplication, and distributivity.

We will now leave the *'s off. We already have the order $\in$ on NN. We write $<$ for $\in$ between NN's. We write $n \leq m$ for $(n < m \vee n = m)$. By induction, we have

$(n < m \wedge r \in s) \Rightarrow n + r < m + s$
$(n < m \wedge 0 < r \in s) \Rightarrow n \cdot r < m \cdot s$
$n + m = n + r \Rightarrow m = r$
$n \neq 0 \Rightarrow (n \cdot m = n \cdot r \Rightarrow m = r)$
$<$ is a linear ordering on NN
$n \in m \Leftrightarrow (\exists k)(n = k = m)$.

We can now move to the ring of integers. An integer is an ordered pair (i,n), where $i = 0$ or 1 (0 is $\emptyset$, 1 is $\{\emptyset\}$), and n is a NN. We stipulate that $(0,0)$ is an integer, but not $(1,0)$.

We define addition and multiplication explicitly for integers, as well as the order.

EXERCISE. Addition, multiplication, and order on the integers forms a discrete ordered group. Furthermore, every nonempty finite set of integers has a smallest and largest element.

EXERCISE. Let n,m be integers, m nonzero. We can find unique n',m' with no common divisors other than +-1, m' > 0, where for some integer d, we have n = d•n', m = d•m'.

We now define the rationals. These are ordered pairs (n,m) such that m > 0 and there are no common divisors of n,m other than +-1.

We then define addition, multiplication using the last Exercise. We also definition <.

EXERCISE. Addition, multiplication, and order on the rationals forms a densely ordered field.

3. AXIOMS FOR HEREDITARILY FINITE SET THEORY.

We have seen how to develop hereditarily finite set theory within ordinary mathematics, taking a number of concepts from mathematics for granted. We now want to develop hereditarily finite set theory without any prior mathematics.

We do this by writing down a number of axioms about HF sets, which use only the concepts of HF set, $\in$, and =. These axioms are presented in PRED (predicate calculus with equality), discussed in Lecture 1.

As mathematicians, we can recognized the truth of each axiom in the structure consisting of all HF sets where $\in$,= have their usual mathematical meaning.

These axioms about the HF sets are very powerful. They are sufficient for us to redo everything we have done up to now about the HF sets, without resorting to any other concepts or reasoning.

So let's start over completely from scratch when thinking about the HF sets. To make these axioms easier to read, we freely use some standard abbreviations.

Also, in the English presentations, “sets” always means “HF sets”.

1. EXTENSIONALITY. If two sets have the same elements then they are equal. $(\forall z)(z \in x \leftrightarrow z \in y) \rightarrow x = y$.

2. PAIRING. There is an set consisting of any two given sets. $(\exists z)(\forall w)(w \in z \leftrightarrow (w = x \vee w = y))$.

3. UNION. There is an set consisting of the elements of the elements of any given set. $(\exists y)(\forall z)(z \in y \leftrightarrow (\exists w \in x)(z \in w))$.

4. POWER SET. There is an set consisting of all subsets of any given set. $(\exists y)(\forall z)(z \in y \leftrightarrow z \subseteq x)$.

5. CHOICE. For every set of nonempty sets there is a set which has exactly one element in common with each of the nonempty sets. $(\forall y,z \in x)(y \neq \emptyset \wedge y \neq z = \emptyset) \rightarrow (\exists z)(\forall y \in x)(\exists!w)(w \in y \wedge z)$.

6. FOUNDATION. Every nonempty set has an $\in$ minimal element. $x \neq \emptyset \rightarrow (\exists y \in x)(\forall z \in x)(z \notin y)$.

7. SEPARATION. There is a set consisting of the elements of any given set that satisfy some given condition. $(\exists y)(\forall z)(z \in y \leftrightarrow (z \in x \wedge A))$, where A is any formula of PRED using only $\in$,=, in which y does not appear.

8. REPLACEMENT. If every element of a given set is related to exactly one set by a given condition, then there is a set consisting of the sets such that some element of the given set is related to it. $(\forall y \in x)(\exists!z)(A) \rightarrow (\exists w)(\forall z)(z \in w \leftrightarrow (\exists y \in x)(A))$, where A is any formula of PRED using only $\in$,=, in which w does not appear.

9. FINITENESS. Every nonempty set has an $\in$ maximal element. $x \neq \emptyset \rightarrow (\exists y \in x)(\forall z \in x)(y \notin z)$.

Specifically note that 7 and 8 are made up of infinitely many axioms, as there are infinitely many formulas of PRED using only $\in$,=.

It is easy to see that Replacement implies Separation, and so we can remove Separation. However, it is standard to include both.

All of these axioms are useful. Mathematicians want them for immediate use.

THEOREM 3.1. Extensionality, pairing, union, foundation, separation, finiteness, logically implies the remaining ones: power set, choice, replacement. However, if we drop finiteness, then we cannot obtain any of these remaining three.

We can do finite mathematics entirely within these axioms. We define x is a NN $\leftrightarrow$ (x is $\in$ connected $\wedge$ x is transitive), where

$$x \text{ is } \in \text{ connected} \leftrightarrow (\forall y,z \in x)(y \in z \quad z \in y \quad y = z).$$
$$x \text{ is transitive} \leftrightarrow (\forall y,z \in x)(x \in y \in z \rightarrow x \in z).$$

We can prove all of the basic facts about the NN within these axioms.

EXERCISE. We can prove from 1-9 that $\emptyset$ is a NN, and for all NN x,y,
i) $x \in y \quad y \in x \quad x = y$;
ii) $x \in y \quad y \in x$;
iii) $x \cup \{x\}$ is a NN;
iv) $(\forall z \in x)(z \text{ is a NN})$;
v) $x \neq \emptyset \leftrightarrow (\exists!z)(x = z \cup \{z\})$;
vi) every transitive set of NN's is an NN.

Let n be a NN. We define $n+1 = n \cup \{n\}$.

We want to make sense of the original definition of the HF sets:

$$V(0) = \emptyset,$$
$$V(n+1) = S(V(n)).$$

Here S(u) denotes the power set of u, which is the set of all subsets of u.

EXERCISE. We can prove this in 1-9. Let x be a NN. There is a unique function f such that
i) dom(f) = x;
ii) $f(\emptyset) = \emptyset$,
iii) $(\forall y \in x)(f(y \cup \{y\}) = S(f(y)))$.

Using this exercise, for NN x, we define V(x) as f(x), where f is the unique function satisfying these three clauses for the NN x+1.

EXERCISE. We can prove from 1-9 that (∀x)(∃y)(y is a NN ∧ x ⊆ V(y)). I.e., we can prove from 1-9 that "every set is hereditarily finite".

EXERCISE. We can prove from 1-9 that every x is in one-one correspondence with a unique NN.

We can continue the development of the HF sets entirely within 1-9.

4. ZERMELO FRANKEL SET THEORY WITH THE AXIOM OF CHOICE.

This system is denoted by ZFC, and is the gold standard for mathematical proofs. In fact, it is such a widely accepted gold standard that it is practically never pulled out to settle disputes. In any case, disputes are invariably based on some mistake or misunderstanding, and not misuses of the axioms, or failure to stay within the axioms.

ZFC is the same as 1-9 except that 9 is dropped and replaced by a new 9. Thus ZFC is

1. EXTENSIONALITY.
2. PAIRING.
3. UNION.
4. POWER SET.
5. CHOICE.
6. FOUNDATION.
7. SEPARATION.
8. REPLACEMENT.

9′. INFINITY. (∃x)(∅ ∈ x ∧ (∀y ∈ x)(y ∪ {y} ∈ x)).

The usual definition of finite set in ZFC is a set which is in one-one correspondence with an element of ω.

Recall the definition of NN in 1-9 given in the previous section:

x is a NN ⇔ (x is ∈ connected ∧ x is transitive).

This definition is not operative in 1-9′. Instead, the right side is the definition of ordinal in ZFC. I.e., we define

x is an ordinal $\leftrightarrow$ (x is $\in$ connected $\wedge$ x is transitive).

EXERCISE. (ZFC). If x,y are ordinals, then
i) $x \in y \quad y \in x \quad x = y$;
ii) $x \subseteq y \quad y \subseteq x$;
iii) $x \cup \{x\}$ is an ordinal;
iv) every element of an ordinal is an ordinal;
v) every transitive set of ordinals is an ordinal;
vi) every set of ordinals is a subset of an ordinal;
vii) every nonempty set of ordinals has a unique least element;
viii) the ordinals are exactly the transitive sets of transitive sets.

$x \cup \{x\}$ is called the successor of x, written x+1. A limit ordinal is an ordinal which is not the successor of any ordinal.

The natural numbers are developed in ZFC as follows.

Using power set, separation, and infinity, we obtain a least set x obeying the property in infinity. I.e., least in the sense that it is a subset of any set x satisfying the property in 9'.

This least x is normally denoted by ω and forms the set theoretic version of the set of all natural numbers.

EXERCISE. (ZFC). ω is an ordinal. ω is the least limit ordinal.

We can easily develop the real number system in ZFC, but not in 1-9. Using the approach due to Dedekind, we define a real number as a left cut of rationals; i.e.,

x is a real number $\leftrightarrow$ (x $\subseteq$ Q $\wedge$ x $\neq \emptyset \wedge$
$(\exists y,z \in Q)(y < z \rightarrow x \rightarrow y \rightarrow x)$).

Using power set, we obviously have the set of all real numbers, denoted by $\neg$.

Addition, multiplication, minus, reciprocal, and order can be appropriately defined on $\neg$ to form the ordered field of real numbers.

A critical property of ¬ is the least upper bound property. This asserts that every nonempty x ⊆ ¬ with an upper bound has a least upper bound. This upper bound is simply the union of x, in the sense of the union axiom.

The Cauchy sequence construction is definitely more involved from our viewpoint, but it has compensating advantages that are well known to analysts.

Obviously ordinals come in three varieties. There is the least one, ∅. There are the successors ordinals, which are of the form α ∪ {α}, normally written α+1. Finally, there are the limit ordinals, which are the remainder of the ordinals.

It is customary to write α < β for ordinals α,β where α ∈ β.

We want to build the V's on all ordinals by the following transfinite recursion:

$$V(0) = \emptyset,$$
$$V(\alpha+1) = S(V(\alpha)),$$
$$\text{for limit ordinals } \lambda,\ V(\lambda) = \bigcup\{V(\alpha): \alpha \in \lambda\}.$$

How do we justify this definition?

EXERCISE. (ZFC). Let α be an ordinal. There is a unique function f such that
i) dom(f) = α;
ii) f(∅) = ∅, assuming α ≠ ∅;
iii) (∀β < α)(f(β+1) = S(f(β)));
iv) (λ limits λ < α)(f(λ) = ⋃{V(β): β ∈ λ}).

The above uses power set and replacement in essential ways.

Using this exercise, for ordinals α, we define V(α) as f(α), where f is the unique function satisfying these three clauses for the ordinal α+1.

These V(α)'s are of crucial importance in set theory, and form what is called the cumulative hierarchy.

EXERCISE. (ZFC). (∀x)(∃α)(x ∈ V(α)).

In ZFC, we define the HF sets as the elements of V(□). Note that we have the set of all HF sets available to us in ZFC, something we didn't have in 1-9.

THEOREM. (ZFC). Every set is in one-one correspondence with an ordinal.

This theorem uses the Axiom of Choice in an essential way.

For every set x, the least ordinal in one-one correspondence with x is called the cardinal of x.

5. BIG ISSUES.

There is a remarkable relationship between axioms 1-9 and ZFC. Axioms 1-9 form an appealing and useful set of axioms that a mathematician immediately recognizes as holding of the HF sets. ZFC is exactly the same as 1-9 except that the one axiom that obviously focuses on finiteness - axiom 9 - is replaced by an axiom of infinity, 9'.

This naturally suggests that we should be able to say just what kind of statement true about the hereditarily finite sets lift to the full set theoretic universe.

Obviously, not every kind of statement can be so lifted. Look at axiom 9, which is false of □ - i.e., □ has no □ maximal element. Nobody has been able to find such a transfer principle from HF sets to arbitrary sets.

The identification of natural numbers with any particular sets is going to have to be ad hoc. Same with real numbers.

We can acknowledge this state of affairs by saying that the usual set theoretic foundations for mathematics forms an ***interpretation*** of mathematics in set theory.

We can ask for a foundation for mathematics that is more literal. For instance, mathematicians often take the concept of natural number as primitive, and only care about its properties. Or mathematicians may only consider *natural number systems*, instead of natural numbers. One can ask for a foundation for mathematics that is directly sensitive to these viewpoints.

There have been some attempts to create an alternative foundation for mathematics along these lines. One approach

is called *categorical foundations of mathematics*. However, there are serious difficulties involved in making this an autonomous foundation for mathematics, since one tends to define categories set theoretically. Attempts to rid categorical foundations of set theory entirely wind up slavishly transporting the axioms of set theory into a categorical context, resulting in an equivalent but more cumbersome form of set theoretic foundations. These issues are controversial.

Two other big issues form the topics of the next two lectures. These regard the senses in which ZFC is overkill (too powerful), and senses in which ZFC is underkill (too weak).

LECTURE 3
DO WE NEED LESS AXIOMS?

Harvey M. Friedman
Department of Mathematics
Ohio State University
May 5, 2003
http://www.math.ohio-state.edu/~friedman/
friedman@math.ohio-state.edu

In the first two lectures, we have laid the basic groundwork that is needed for an appreciation of the work in the foundations of mathematics that began in the 1930's and continues to this day.

The material presented in the first two lectures concerned rather spectacular results from the point of view of philosophy and history of mathematics.

In these last two lectures, we will relate this basic material to focused topics in mathematics.

1. PURELY ADDITIVE NUMBER THEORY.

By purely additive number theory, we will mean the study of the integers and rationals and reals, where we allow only the order and addition. We explicitly exclude multiplication.

This is an interesting, yet extremely well understood mathematical context, where, in a very precise sense, absolutely every question can be answered.

In fact, in this context, absolutely everything can be answered within a very weak fragment of ZFC.

How do we convey this? Consider the structure, in the sense of the first lecture,

$$(\neg, Q, Z, <, +, -, 0, 1).$$

Here the domain is the set of all reals, $\neg$. We have a 1-ary relation Q, a 1-ary relation Z. We have the binary relation $<$ on $\neg$, and the binary function + from $\neg$ into $\neg$. We have the unary function - from $\neg$ into $\neg$. We have the constants 0 and 1.

What are we allowed to say? I.e., what problems are we allowed to pose?

As in the first lecture, we use PRED. We can say anything grammatical involving:

1. $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$. (Not, and, or, implies, iff).
2. $\forall$, $\exists$. (For all reals, there exists a real).
3. Q(_), Z(_). (Being a rational, being an integer).
4. <. (One real less than another).
5. +. (The addition of two reals).
6. -. (The negative of a real).
7. 0, 1. (Two specific reals).
8. =. (Two reals are equal).

Here are some examples of allowable sentences.

$(\forall x,y)(x < y \rightarrow (\exists z)(x < z < y \wedge Q(z))).$
$(\forall x)(\exists y)(x = y + y).$
$(\forall x,y)((Z(x) \wedge Z(y)) \rightarrow Z(x + y)).$
$(\forall x)(\exists y)(x = y + y).$
$(\forall x)(Q(x) \rightarrow (\exists y)(Q(y) \wedge x = y + y)).$
$(\forall x)(Z(x) \rightarrow (\exists y)(Z(y) \wedge x = y + y)).$

All but the last are true in $(\neg, Q, Z, <, +, -, 0, 1)$. Here is a fix for the last one.

$(\forall x)(Z(x) \rightarrow (\exists y)(Z(y) \wedge (x = y + y \vee x = (y + y) + 1))).$

THEOREM 1.1. Every sentence in PRED about $(\neg, Q, Z, <, +, -, 0, 1)$ can be proved or refuted within a very small fragment of ZFC.

So we need far less axioms than ZFC in this limited mathematical context.

Things are rather delicate, because if we throw in multiplication, then things go haywire. In particular, things are very bad for $(Z,+,\bullet)$ and also for $(Q,+,\bullet)$.

THEOREM 1.2. There are sentences in PRED about $(Z,+,\bullet)$ that cannot be proved or refuted within ZFC. The same holds for $(Q,+,\bullet)$.

Actually, things are much worse than even Theorem 1.2 suggests. Recall from the second lecture that ZFC was axiomatized by finitely many axioms and axiom schemes. It is clear intuitively what an axiom scheme is, and there is a comprehensive definition of what an axiom scheme is that we do no have time to go into here.

We say that a set of axioms of PRED is consistent iff it does not prove a contradiction. By the fundamental completeness theorems from the first lecture, this is the same as the existence of a structure in which the set of axioms holds.

THEOREM 1.3. Let T be any consistent extension of ZFC by finitely many new axioms and axiom schemes. There is a sentence in PRED about $(Z,+,\bullet)$ that cannot be proved or refuted in T. The same holds for $(Q,+,\bullet)$.

There is a very special but familiar family of sentences about $(Z,+,\bullet)$ known as Diophantine problems. A Diophantine problem is to determine the existence of a solution in integers to an equation of the form

$$P(x_1,...,x_n) = 0$$

where P is a polynomial in the n variables shown with integer coefficients.

THEOREM 1.4. Let T be any consistent extension of ZFC by finitely many new axioms and axiom schemes. There is a Diophantine problem with a "no" answer which cannot be proved in T to have a "no" answer.

Theorem 1.4 is essentially the same as the negative solution of Hilbert's 10th problem. The original problem concerns algorithms and not formal systems such as ZFC.

THEOREM 1.5. (Negative solution to Hilbert's 10th problem). There is no computer algorithm that correctly answers any given Diophantine problem.

However, do not get discouraged by this kind of negative result. Here are some reasons for keeping a happy face.

1. All statements in PRED about the structure $(\neg, Q, Z, <, +, -, 0, 1)$ and many other important structures can be proved or refuted in even very weak fragments of ZFC. We will give more examples later.

2. Nobody knows whether all Diophantine problems for $(Q,+,\bullet)$ can be answered (with proofs!) in ZFC or even in a very weak fragment of ZFC.

3. Even for Diophantine problems in $(Z,+,\bullet)$, nobody has been close to being able to give a reasonable example that has "logical difficulties"; i.e., cannot be answered in ZFC or even weak fragments of ZFC.

The following result comes immediately from work of number theorists.

THEOREM 1.6. Every quadratic Diophantine problem for $(Z,+,\bullet)$ and for $(Q,+,\bullet)$ can be answered within a very small fragment of ZFC.

It is open whether Theorem 1.6 holds for cubics in two variables over Z. Same with Theorem 1.5.

Where do Theorems 1.5 and 1.6 kick in, with respect to the number of variables and the degree?

This problem has been studied intensively over $(N,+,\bullet)$ rather than $(Z,+,\bullet)$, where the negative results kick in earlier than they do for $(Z,+,\bullet)$.

For $(N,+,\bullet)$, some known results are that Diophantine problems of degree n in m variables cannot be solved and cannot all be answered within ZFC, where, e.g.,

i) $n = 1.6 \times 10^{45}$, $m = 9$;
ii) $n = 4$, $m = 58$;
iii) $n = 24$, $m = 26$.

To convert these to (Z,+,•), it is easy to see that it suffices to multiply n by 2 and m by 4 using Lagrange's theorem that every natural number is the sum of four squares of integers.

We now come back to (¬,Q,Z,<,+,-,0,1).

We can say much more about the principles needed to answer any question in PRED about this structure.

We can list some simple and obvious statements in PRED that are obviously true in this structure, and show that every sentence in PRED about this structure can be proved or refuted from these simple and obvious statements.

1. The ordered Abelian group axioms for (¬,<,+,-,0).
2. 0 < 1.
3. Z(0) ∧ Z(1).
4. Z(x) → Q(x).
5. Z(x) → (x ∧ 0 x ≥ 1).
6. (Q(x) ∧ Q(y)) → Q(x + y).
7. (Z(x) ∧ Z(y)) → Z(x + y).
8. Z(x) → Z(-x).
9. Q(x) → Q(-x).
10. (∀x,y)(x < y → (∃z,w)(Q(z) ∧ Z(w) ∧ x < z < y < w)).
11. (∀x)(∃y)(y + ... + y = x), where there are any finite number of one or more y's.
12. (∀x)(Q(x) → (∃y)(Q(y) ∧ y + ... + y = x)), where there are any finite number of one or more y's.
13. (∀x)(Z(x) → (∃y)(∃r)(Z(y) ∧ Z(r) ∧ x = y + ... + y + r ∧ 0 ∧ r < 1 + ... + 1)), where there are d y's and d 1's, d ≥ 1.

13 is the formalization of the quotient remainder theorem, and consists of infinitely many axioms.

It can be shown that 1-13 cannot be given a finite axiomatization; i.e., is not logically equivalent to a finite set of axioms in PRED.

THEOREM 1.7. A sentence of PRED is true in (¬,Q,Z,<,+,-,0,1) iff it has a proof from 1-13. We can algorithmically decide whether a sentence of PRED is true in (¬,Q,Z,<,+,-,0,1).

The method of proof for such results is what is called quantifier elimination.

We say that a set T of axioms (like 1-13 above) admits quantifier elimination (QE) if and only if for every formula A in PRED using only the symbols used in T, there is a quantifier free formula B in PRED using only the symbols used in T, such that

$$T \text{ proves } A \leftrightarrow B.$$

An important related concept is that of a structure M admitting QE. This means that for every formula A in PRED using only the symbols used in M, there is a quantifier free formula B in PRED using only the symbols used in N, such that

$$SAT(M, A \leftrightarrow B).$$

In the case of the set of axioms 1-13 and the structure $(\neg, Q, Z, <, +, -, 0, 1)$, we don't have quantifier elimination as things stand. However, if we add the new unary relation symbols $P_1, P_2, \ldots$ with the axioms

$$P_i(x) \leftrightarrow (\exists y)(Z(y) \wedge y + \ldots + y = x)$$

to 1-13, then this expansion of 1-13 admits QE. Also if we expand $(\neg, Q, Z, <, +, -, 0, 1)$ to $(\neg, Q, Z, <, +, -, 0, 1, P_1, P_2, \ldots)$, where each P_i is the unary relation

$$P_i(x) \text{ iff } x \text{ is an integer divisible by } i$$

then $(\neg, Q, Z, <, +, -, 0, 1, P_1, P_2, \ldots)$ admits QE.

We now give a very easy example of QE, and show how it is used to obtain results like Theorem 1.7. Let us consider the structure $(Z, 0)$.

QE for $(Z, 0)$ means that every formula A in PRED about $(Z, 0)$ is equivalent in $(Z, 0)$ to a formula B in PRED about $(Z, 0)$. (Recall that = is a freebie in PRED).

So what? If we have any sentence about $(Z, 0)$, then it is equivalent to a quantifier free formula. Hence by obvious trickery, it is equivalent to a quantifier free sentence (just plug in 0 for all variables).

But the quantifier free sentences are trivial. They are just combinations of $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$, and $0 = 0$. These can

be proved or refuted. Hence the original sentence about (Z,0) can be proved or refuted.

We now write down axioms that support the QE. The usual axioms for equality are taken for granted, as in Lecture 1. The only other axioms that we will need are the axioms

$$*) \quad (\exists x_1)\ldots(\exists x_n)(x_1,\ldots,x_n \text{ are all unequal})$$

where n is any positive integer. The inside is a conjunction of inequalities of quadratic length.

Now how does the QE work? A big induction shows that we just have to eliminate a single quantifier. We can also tidy things up a bit using propositional calculus. So things boil down to looking at formulas of the form

$$(\exists x)(y_1 = z_1 \wedge \ldots \wedge y_n = z_n \wedge w_1 \neq u_1 \wedge \ldots \wedge w_m \neq u_m)$$

where the y's, z's, w's, u's are variables or 0, some of which may be x.

By purely logical reasoning in PRED, we can move all of the equations and inequations that don't mention x outside the scope of the quantifier:

$$(\exists x)(x = a_1 \wedge \ldots \wedge x = a_p \wedge x \neq b_1 \wedge \ldots \wedge x \neq b_q) \wedge A$$

where $p,q \geq 0$ and A is a conjunction of equations and inequations that don't mention x. We can also assume that none of the a's and none of the b's are x. There are still degenerate cases here, but they cause no trouble.

If $p > 0$ then we can simply remove the quantifier and replace every occurrence of x by a_1. Then QE is done.

So we can assume that we have

$$(\exists x)(x \neq b_1 \wedge \ldots \wedge x \neq b_q) \wedge A$$

with A as before, and none of the b's are x.

However, the first conjunct is obviously provable from our axioms *). Hence we are left with A, and again QE is done.

This argument establishes QE for the axioms *) and for the structure (Z,0). Moreover, the QE has been algorithmically

achieved. One can easily draw the conclusions of Theorem 1.7 for *) and (Z,0).

2. THE REAL AND COMPLEX FIELDS.

The method of QE has been applied to the structure (¬,<,+,-,•,0,1), the ordered field of real numbers. This result of Tarski has been historically viewed as the beginning of real algebraic geometry.

It was also successfully applied by Tarski to the structure (**C**,+,-,•,0,1), and this is easier than the real case. These QE results immediately give the following.

THEOREM 2.1. Every sentence of PRED about (¬,<,+,-,•,0,1) is provable or refutable in a weak fragment of ZFC. The same holds for (**C**,+,-,•,0,1).

The axioms for (**C**,+,-,•,0,1) are as follows.

1. (**C**,+,-,•,0,1) is a commutative field with unit.
2. $1 + \ldots + 1 \neq 0$, where there are any finite nonzero number of 1's. (Characteristic zero).
3. $(\exists z)(z^n + c_{n-1}z^{n-1} + \ldots + c_1 z + c_0 = 0)$, where $n \geq 1$, and the c's are variables other than z. (Algebraically closed).

Note that in 3, we have used powers of z to abbreviate the result of multiplying z with itself many times. There are obviously infinitely many axioms in 3. We can use one for every positive n.

THEOREM 2.2. 1-3 above and (**C**,+,-,•,0,1) admit QE. Every sentence in PRED holds in (**C**,+,-,•,0,1) iff it is provable from 1-3.

COROLLARY 2.3. Every sentence of PRED that holds about one algebraically closed field of characteristic zero holds about all algebraically closed fields of characteristic zero.

Actually, these results also hold in any finite characteristic. The characteristic of a field is the least $p \geq 1$ such that $1 + \ldots + 1 = 0$, with p 1's. If none exists, the characteristic is considered 0. If p exists, then p can be shown to be a prime.

We use these axioms, for any particular prime p.

1(p). (**C**,+,-,•,0,1) is a commutative field with unit.
2(p). 1 + ... + 1 = 0, where there are p 1's.
3(p). 1 + ... + 1 ≠ 0, where there are fewer than p 1's.
4(p). $(\exists z)(z^n + c_{n-1}z^{n-1} + ... + c_1z + c_0 = 0)$, where $n \geq 1$, and the c's are variables other than z. (Algebraically closed).

THEOREM 2.4. Let p be a prime. 1(p)-4(p) admits QE. Every sentence in PRED that holds in some algebraically closed field of characteristic p holds in all algebraically closed fields of characteristic p, and is provable from 1(p)-4(p).

We now come to the ordered field of reals, (¬,<,+,-,•,0,1). The axioms for (¬,<,+,-,•,0,1) are as follows.

i. (¬,<,+,-,•,0,1) is a commutative ordered field with unit.
ii. $x > 0 \rightarrow (\exists y)(y \cdot y = x)$. Positives have square roots.
iii. $(\exists x)(x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0 = 0)$, where $n \geq 1$ is odd, and the c's are variables other than x.

Note that there are infinitely many axioms in iii. We can take one for each odd n.

THEOREM 2.5. i-iii above and (¬,<,+,-,•,0,1) admit QE. Every sentence in PRED holds in (¬,<,+,-,•,0,1) iff it is provable from i-iii.

There are many other important axiomatizations for this vitally important structure, that are logically equivalent. Here are two, which we present informally.

i. (¬,<,+,-,•,0,1) is a commutative ordered field with unit.
iv. Intermediate value for polynomials.

Here is the other.

i. (¬,<,+,-,•,0,1) is a commutative ordered field with unit.
v. Least upper bound principle for all formulas in PRED about (¬,<,+,-,•,0,1).

There has been considerable work on the structure (¬,<,+,-,•,exp,0,1), where $\exp(x) = e^x$. It is not known whether

every sentence true about this structure is provable or refutable in ZFC or in a weak fragment of ZFC.

This is known if we can prove Schanuel's Conjecture (SCT). Alternatively, we know that this is true for ZFC + SCT.

SCT asserts the following. If $z_1,...z_n \in \mathbf{C}$ are linearly independent over Q, then some n of the 2n numbers $z_1,...,z_n,e^{z_1},...,e^{z_n}$ are algebraically independent.

SCT implies the (unknown) algebraic independence of e and π by taking $z_1 = 1$ and $z_2 = \pi i$. (Note $e^{\pi i} = -1$).

THEOREM 2.6. Every sentence of PRED about $(\neg,<,+,-,\bullet,\exp,0,1)$ is true if it is provable in a weak fragment of ZFC together with SCT.

3. FINITE MATHEMATICS.

Many mathematicians think that the essence of mathematics is finite, and that infinite objects are around just for convenience. How can we construct foundations for such a point of view?

In lecture 1, we had given an axiom system 1-9 for the hereditarily finite sets, or HF sets. We developed a fair amount of basic finite mathematics in this system.

Obviously there can be no direct treatment of infinitary objects such as real numbers in a system like 1-9, which proves "every set is finite".

Can we support the mathematician who wishes to use real analysis but fundamentally believes only in finite objects?

The current approach to this issue is to create weak fragments of ZFC that allow for much real analysis to be done without major modification.

We then show that any theorem of such a fragment of ZFC that is just about finite objects can already be proved in 1-9. This allows the mathematician who only believes in finite objects to engage in real analysis and other kinds of higher mathematics with confidence.

I will give one example of such a result. Recall 1-9, which is generally acceptable to the mathematician who only believes in finite objects:

1. EXTENSIONALITY.
2. PAIRING.
3. UNION.
4. POWER SET.
5. CHOICE.
6. FOUNDATION.
7. SEPARATION.
8. REPLACEMENT.
9'. FINITENESS.

We now introduce another axiom system that accommodates infinite sets. I don't mean the replacement of 9' with 9 (infinity), as this is ZFC, and is much too strong for what we want to do.

We say that x is an elemental set if and only if x is an element of some set. Of course, using Pairing we can prove that every set is an elemental set.

But in this system I am about to introduce, the conceptual framework is different, and we will only have a modified Pairing axiom. We should now think of the sets as

the sets that consist entirely of HF sets.

Under this conceptual framework, the elements are just the HF sets. This is not all sets in this new conceptual framework, since the set of all HF sets will be among the sets in this new conceptual framework.

Here are the axioms.

1. EXTENSIONALITY.

2*. ELEMENTAL PAIRING. There is a elemental set consisting of any two given elemental sets.

3*. ELEMENTAL UNION. There is an elemental set consisting of the elements of the elements of any given elemental set.

4*. ELEMENTAL POWER SET. There is an elemental set consisting of all subsets of any given elemental set.

5. CHOICE.

6. FOUNDATION.

7*. WEAK SEPARATION. There is a set consisting of the elements of any given set that satisfy some given condition, provided that in that given condition, all quantifiers range over elemental sets only.

8*. ELEMENTAL REPLACEMENT. If every element of a given elemental set is related to exactly one elemental set by a given condition, then there is an elemental set consisting of the elemental sets such that some element of the given set is related to it, provided that in that given condition, all quantifiers range over elemental sets only.

9*. ELEMENTAL FINITENESS. Every nonempty elemental set has an □ maximal element.

Let us call this system (1-9)*. Note that we have left axioms 1,5,6 untouched.

Note that (1-9)* proves the existence of lots of infinite sets, and in fact the existence of a largest set. For by 7*, we have the set of all elemental sets, which is clearly the largest set.

It can be seen that (1-9)* nicely accommodates much elementary analysis because of its reasonably flexible ability to construct infinite sets.

THEOREM 3.1. Let A be a sentence in PRED with □,= only, in which all quantifiers range over elemental sets only. Then A is provable in (1-9)* if and only if A is provable in 1-9.

Some interesting examples have surfaced of theorems about finite objects, that cannot be proved in 1-9 (and therefore not even in (1-9)*). Moreover, these examples cannot be proved in rather far reaching strengthenings of 1-9. In fact, such theorems have surfaced about finite objects, where, in some appropriate sense, all proofs must involve consideration of uncountably many objects.

The original examples concern embeddings between finite trees. This is a classical topic in combinatorics, and one of the early results is Kruskal's theorem.

There are several ways to define finite trees, and we will take the partial ordering approach. A finite tree is a pair $(T,\preceq)$, where

i) T is a nonempty finite set;
ii) $x \preceq x$;
iii) $(x \preceq y \wedge y \preceq x) \rightarrow x = y$;
iv) $(x \preceq y \wedge y \preceq z) \rightarrow x \preceq z$;
v) $x,y \preceq z \rightarrow (x \preceq y \vee y \preceq x)$;
vi) there is a $\preceq$ least element, called the root.

In the mind's eye, a tree is visualized so that its root is at the bottom.

Note that in a finite tree $(T,\preceq)$, any two elements have a greatest lower bound, called the inf.

Let T and T' be finite trees. We abuse notation by suppressing the $\preceq$'s.

An inf preserving embedding $h:T \rightarrow T'$ is a one-one function $h:dom(T) \rightarrow dom(T')$ such that for all $x,y \in dom(T)$,

$$h(x \inf y) = h(x) \inf h(y).$$

This is essentially the same as having a topological embedding in the sense of topological spaces, where line segments connect appropriate vertices.

THEOREM 3.1. Let $T_1,T_2,...$ be finite trees. There exists $i < j$ such that T_i is inf preserving embeddable into T_j.

It is known that, in an appropriate sense, the only way to prove Theorem 3.1 is to work with infinite sequences of finite objects as objects themselves.

The statement of Theorem 3.1 is not fully in finite mathematics. But there is a finite form of Theorem 3.1 that asserts the following:

In any tree with vertices labeled from an r element set, which is fully k splitting up to a sufficiently large maximum uniform height, there are two uniform height truncations, where the lower one is inf and label preserving embeddable into the higher one, sending the top

level of the lower one into the top level of the higher one.

It is known that even to prove this finite statement, one must go way beyond 1-9 in far reaching ways into infinite mathematics.

On the other hand, I have conjectured that all of the famous number theory to date can be done within even weak fragments of 1-9. This is far from being established.

4. COUNTABLE MATHEMATICS.

Countable mathematics is another significant, and much more liberal, kind of mathematics. Here all objects are to be countable.

Real numbers are to be viewed as countable objects - sets of rationals, and rationals are finite objects.

The real line itself is uncountable, and it seems that in countable mathematics, one cannot manipulate, say, complete separable metric spaces as objects.

However, from the logical point of view, any complete separable metric space is really a countable object. That is because it can be coded as a countable metric space - i.e., a metric space on one of its countable dense sets. We then define the notion of a point in its completion without having the completion itself: points are Cauchy sequences in the countable metric space. Of course, generally every Cauchy sequence is equivalent to many others, but that is not a problem. E.g., we can take preferred Cauchy sequences, using the enumeration of the countable dense set, or simply ignore the problem, choosing instead to define equality.

Now once we have an entirely countable presentation of Polish spaces and their “points”, we can go on to define the Borel measurable sets and functions in and between Polish spaces.

Recall that the Borel measurable subsets of a Polish space form the least σ algebra containing the open sets. We don’t even want to try to use this definition in countable mathematics.

Instead, we use the well known development of Borel sets in terms of countable well founded trees. The terminal nodes are labeled by open sets.

Each nonterminal node is labeled by “complement” or “union” or “intersection”. Of course, if “complement” is the label then there must be no splitting.

We can represent open subsets of Polish spaces by using the set of all pairs (x,q), where x lies in the countable dense subset and q is a positive rational such that the open ball about x with radius q is a subset of the open subset being coded. Under this representation, open subsets of Polish spaces are countable objects, and this allows us to use them as labels of the terminal nodes in the countable well founded trees discussed above.

Borel measurable functions can be handled by working with the inverse images of open balls with center from the countable dense set, with positive rational radius.

There is a convenient fragment of ZFC that easily supports the development of countable mathematics as outlined above. I will put a big fat DELETE sign against the single axiom that we are going to delete from ZFC for this purpose. Recall the axioms of ZFC from lecture 2:

1. EXTENSIONALITY.
2. PAIRING.
3. UNION.
4. POWER SET. **DELETE!**
5. CHOICE.
6. FOUNDATION.
7. SEPARATION.
8. REPLACEMENT.
9’. INFINITY.

Incidentally, this is far more than enough to do Kruskal’s tree theorem from the previous section.

In fact, this system, ZFC without the power set axiom, written ZFC\P, is strong enough to do an overwhelming preponderance of mathematics in the uniform, direct, and natural way indicated above.

On the other hand, there are now a number of interesting theorems of ZFC whose statements lie in countable

mathematics, but where we know that there is no proof in ZFC\P.

We will now discuss some examples concerning Borel measurable functions.

Historically, the first example was the Borel diagonalization theorem.

Cantor's theorem (there are uncountably many reals) can be put in the form: in any infinite sequence of reals, some real is missing. We want to talk about "finding" a missing real.

THEOREM 4.1. There is a Borel measurable function F from the Polish space ¬ into ¬ such that for all x □ ¬ , F(x) is missing from x.

Note that the value of this "diagonalizer" F at a sequence may vary if we use another sequence with the same range.

THEOREM 4.2. For all range independent Borel F:¬ □ ¬ there exists x □ ¬ such that F(x) is a coordinate of x.

Theorem 4.2 can be proved in ZFC but not in ZFC\P. The proof uses the Baire category theorem.

The Baire category theorem applied to Polish spaces is not problem in ZFC\P. However, in the proof of Theorem 4.2, the Baire category theorem is applied to a very nonseparable space - namely, ¬ , where ¬ is given the ***discrete*** topology!

We have to work with the Borel measurable subsets in this crazy topology, and such sets cannot be given countable substitutes as we were able to do for Borel measurable subsets of Polish spaces.

The proof of Theorem 4.2 doesn't need too much more than ZFC\P. For instance the following is enough:

1. EXTENSIONALITY.
2. PAIRING.
3. UNION.
4. POWER SET. REPLACE BY "POWER SET OF SOME INFINITE SET EXISTS".
5. CHOICE.
6. FOUNDATION.

7. SEPARATION.
8. REPLACEMENT.
9′. INFINITY.

We now move on to even greater uses of ZFC. There is an important fragment of ZFC called ZC (Zermelo set theory with the axiom of choice). Here it is:

1. EXTENSIONALITY.
2. PAIRING.
3. UNION.
4. POWER SET.
5. CHOICE.
6. FOUNDATION. DELETE.
7. SEPARATION.
8. REPLACEMENT. DELETE.
9′. INFINITY.

ZC is sufficient for the direct, coding free treatment of the vast preponderance of mathematics.

Although there is no logical implication between ZC and ZFC\P, ZC is much stronger in various senses. E.g., any statement about Borel measurable sets/functions in and between Polish spaces provable in ZFC\P, is provable in ZC, but not vice versa.

THEOREM 4.3. Let E be a Borel subset of $\neg^2$ which is symmetric about the line y = x. There is a Borel function F:¬ □ ¬ such that either (□x)((x,F(x) □ E) or (□x)((x,F(x)) □ E).

The hypothesis means that (x,y) □ E □ (y,x) □ E.

Theorem 4.3 is provable in ZFC but not in ZC. The proof necessarily uses every countable initial segment of the cumulative hierarchy.

LECTURE 4
DO WE NEED MORE AXIOMS?

Harvey M. Friedman
Department of Mathematics
Ohio State University
May 7, 2003
http://www.math.ohio-state.edu/~friedman/
friedman@math.ohio-state.edu

The ZFC axioms are known to be insufficient to settle a variety of mathematical questions. In this fourth and final lecture, we survey a number of examples, and give some indication of the techniques used to establish such independence results.

Most of the examples are of a distinctly more "set theoretic" flavor than what is usually encountered in mathematics.

However, there are now some new kinds of examples involving Borel measurable sets/functions, and even sets/functions in the natural numbers.

1. THE AXIOM OF CHOICE.

At one time, the axiom of choice was regarded as extremely controversial, since it differs so much from the other axioms of ZFC. Now it is generally regarded as roughly on a par with the other axioms of ZFC.

The axiom of choice asserts the following: given any set of pairwise disjoint nonempty sets, there is a set which has exactly one element in common with each (of these pairwise disjoint nonempty sets).

Recall the axioms of ZFC yet again:

1. EXTENSIONALITY.
2. PAIRING.
3. UNION.
4. POWER SET.
5. CHOICE.
6. FOUNDATION.
7. SEPARATION.
8. REPLACEMENT.
9'. INFINITY.

Note that every axiom except extensionality and foundation is a set existence axiom.

In all of the set existence axioms, with the sole exception of the axiom of choice, we have an explicit description of the set that is being constructed.

So from the beginning, the axiom of choice stood out as rather special.

The axiom of choice is used in order to get any kind of decent theory of cardinality:

THEOREM 1.1. (ZF). Choice is equivalent to "given two sets, there is a one-one map from the first into the second, or a one-one map from the second into the first".

How do we get this comparability from choice? This is through the crucial notion of a well ordering. A well ordering of a set A is a strict linear ordering on A in which every nonempty subset of A has a least element. I.e.,

i) $(\forall x,y \in A)(\neg(x < x) \wedge (x < y \vee y < x \vee x = y))$;
ii) $(\forall x,y,z \in A)((x < y \wedge y < z) \rightarrow x < z)$;
iii) $(\forall x \subseteq A)(x \neq \emptyset \rightarrow (\exists y \in x)(\forall z \in x)(\neg(z < y)))$.

THEOREM 1.2. (ZF). Choice is equivalent to "every set can be well ordered".

A countable set A is a set such that there exists a one-one function $f:A \rightarrow \omega$. Recall that $\omega = \{0,1,...\}$ is the least limit ordinal.

Obviously, if A is countable then we have a well ordering of A by

$$x <' y \text{ iff } f(x) < f(y).$$

So countable sets can be well ordered without using choice. But how do we well order the real line, $\neg$?

THEOREM 1.3. ZF does not prove that $\neg$ can be well ordered (assuming ZF is consistent).

There are much stronger and more dramatic results than Theorem 1.3.

THEOREM 1.4. ZF does not prove that "$\neg$ cannot be decomposed into a countable union of countable sets". I.e., ZF + "$\neg$ can be decomposed into a countable union of countable sets" is consistent (assuming ZF is consistent).

EXERCISE. Show in ZF that "$\neg$ can be well ordered" implies "$\neg$ cannot be decomposed into a countable union of countable sets".

An infinite set is a set that is not finite; i.e., not in one-one correspondence with any bounded initial segment of N.

THEOREM 1.5. ZF does not prove that every infinite set of reals contains a countably infinite subset (assuming ZF is consistent).

EXERCISE: Show in ZF that a) every infinite set of reals has a limit point (maybe not in the set); b) every infinite set of reals can be split into an infinite sequence of distinct pairwise disjoint infinite sets of reals.

If we go beyond just sets of reals, we might have an infinite set whose subsets are completely impoverished:

THEOREM 1.6. ZF does not prove that every infinite set can be split into two disjoint infinite subsets (assuming ZF is consistent).

Of course, we cannot have such an impoverished infinite set that is a set of reals. But how simple can such a set be?

THEOREM 1.7. ZF does not prove that every set of countable sets of reals can be split into two disjoint infinite subsets (assuming ZF is consistent).

Enough of this. The main reason why working on ZF is no longer fashionable is that there is an unorganized jungle of consistent pathology, and nobody has been able to put any overarching structure into the subject.

For instance, one would like a good answer to the question: what does it mean to say that the axiom of choice is violated whenever possible or as much as possible? This would be interesting even in restricted contexts.

2. CONSISTENCY OF THE AXIOM OF CHOICE.

In the days when the axiom of choice was controversial, a major issue was whether the adjoining of the axiom of choice to ZF to form ZFC was dangerous. Dangerous - not in the sense that it would cause illness or death - but in the far worse sense that it might allow a contradiction.

THEOREM 2.1. If ZF is consistent then ZFC is consistent.

This is called a relative consistency result, and it is ideal for such a result to be proved using only the most unimpeachable of reasoning. In fact, the proof of Theorem 2.1 was ultimately couched in terms of rudimentary symbol manipulation.

We explain the ideas behind the proof of Theorem 2.1. Recall the cumulative hierarchy of sets:

$$V(0) = \emptyset,$$
$$V(\alpha+1) = S(V(\alpha)),$$
$$V(\lambda) = \bigcup\{V(\alpha): \alpha < \lambda\}.$$

Here α,β are ordinals, λ is a limit ordinal, and S is used for the power set. In particular, $S(V(\alpha))$ is the set of all subsets of $V(\alpha)$.

In ZF, we can prove that every set is an element of some $V(\alpha)$. So this cumulative hierarchy of sets is exhaustive, demonstrably in ZF.

The thing about the cumulative hierarchy that prevents us from really getting a handle on the structure of sets within ZF, is the monstrous power set construction, S.

Actually, this is the cause of our lack of understanding even with the axiom of choice, AxC.

(As we go more deeply into set theory, we start to complain about the ordinals, also. Of course, once Einstein went deeply into physics, he started to complain about classical space/time.)

So we need a thinner, more manageable, more down to earth substitute for the cumulative hierarchy that avoids use of the power set construction.

$$L(0) = \emptyset,$$
$$L(\alpha+1) = FODO(L(\alpha)),$$
$$L(\lambda) = \bigcup\{L(\alpha): \alpha < \lambda\}.$$

Here FODO means “first order definable over”. In particular, $FODO(L(\alpha))$ is the set of all subsets of $L(\alpha)$ of the form

$$\{x \in L(\alpha): A(x) \text{ holds in } (L(\alpha),\in)\}$$

where A is a formula of PRED using $\in$,= only, with parameters from L(α) allowed.

It turns out that this is a nicely behaved hierarchy of sets, even from the point of view of ZF.

We call a set constructible iff it appears in this hierarchy; i.e., is an element of some L(α).

So, we are sitting in ZF, without the axiom of choice, and we make this hierarchical construction of the constructible sets.

We don't know in ZF whether every set is constructible. In fact, many years later it was shown that even in ZFC you can't tell if every set is constructible.

Now sitting in ZF, and looking at the constructible sets, it turns out that we can prove that every single axiom of ZF (taken individually) holds in the constructible sets. In other words, if we take any axiom of ZF, and restrict the quantifiers in it to constructible sets only, then it becomes a theorem of ZF.

Now here's the clincher. Let us look at the axiom of choice, something that we have no reason to be able to think that we can prove in ZF. (In fact, many years later it was shown that the axiom of choice cannot be proved in ZF).

It turns out that when we relativize the axiom of choice to the constructible sets, then we also get a theorem of ZF!

Putting this together, we can now see how to convert any contradiction in ZFC = ZF + AxC into a contradiction in ZF. How? Just relativize all quantifiers in the supposed contradiction in ZFC to the constructible sets, and you get a contradiction in ZF (by filling in the missing steps with the proofs of the relativizations of the axioms of ZFC to the constructible sets).

So Theorem 2.1 has been established.

3. THE CONSISTENCY OF THE CONTINUUM HYPOTHESIS.

The two featured problems left open by Cantor as he created (developed, discovered) set theory were

A. The Axiom of Choice (AxC).
B. The Continuum Hypothesis (CH).

CH asserts the following. Every uncountable set of reals is in one-one correspondence with the set of all reals.

The CH is normally asked in a context where one assumes the AxC (although it is also interesting otherwise). We will follow this norm.

As I said earlier, Gödel showed that every axiom of ZFC becomes a theorem of ZF if we relativize all quantifiers to the constructible sets.

Gödel also tackled CH. With yet more clever ideas, he also showed that CH becomes a theorem of ZF when all quantifiers are relativized to the constructible sets.

This establishes the consistency of ZFC + CH, assuming ZF if consistent.

THEOREM 3.1. If ZF is consistent then ZFC + CH is consistent.

The generalized continuum hypothesis, GCH, asserts the following. For any sets A,B, either there is a one-one map from A into B or a one-one map from S(B) into A.

It is easy to see that GCH for B = $\aleph_0$ is just CH.

Gödel also showed that GCH becomes a theorem of ZF when all quantifiers are relativized to the constructible sets.

THEOREM 3.2. If ZF is consistent then ZFC + GCH is consistent.

4. ADJOINING ELEMENTS TO A MODEL OF SET THEORY.

We want to sketch some of the ideas surrounding P.J. Cohen's proof that if ZF is consistent then ZF + $\neg$AxC and ZFC + $\neg$CH are consistent.

The method is called forcing, but the basic information I am going to tell you is quite memorable and easy to understand, and does not involve a discussion of forcing.

Of course, a modern polished version of forcing is what is normally used to prove this basic information. But don't worry about that.

There are lots of kinds of models of set theory; here we will use only this kind:

$$(L(\alpha),\in)$$

where α is a countable ordinal, in which ZFC holds.

There are lots of $L(\alpha) = (L(\alpha),\in)$, α countable, satisfying ZFC, assuming a bit more set theory than ZF has available to us.

If we stay within ZF, we can prove in ZF that there are lots of $L(\alpha)$, α countable, satisfying any given specified finite fragment of ZF. This will turn out to be good enough for our purposes.

We would like to adjoin a new set x to $L(\alpha)$ to get something we call $L(\alpha,x)$, and hope that $L(\alpha,x)$ remains a model of ZFC.

What should $L(\alpha,x)$ be? Recall the relevant part of the constructible hierarchy (up through α):

$$L(0) = \emptyset,$$
$$L(\alpha+1) = FODO(L(\alpha)),$$
$$L(\lambda) = \bigcup\{L(\alpha): \alpha < \lambda\}$$

where λ is a limit ordinal, $\alpha,\lambda \in \alpha$.

Now let x be a set. What should $L(\alpha,x)$ be?

$$L(0,x) = \{x\},$$
$$L(\alpha+1,x) = FODO(L(\alpha,x)),$$
$$L(\lambda,x) = \bigcup\{L(\alpha,x): \alpha < \lambda\}$$

where λ is a limit ordinal, $\alpha,\lambda \in \alpha$.

But how do we know that $L(\alpha,x)$ satisfies ZFC? It is not hard to find even $x \in \alpha$ such that $L(\alpha,x)$ does not satisfy ZFC. It turns out that there are lots of $x \in \alpha$ that work, but you can't get your hands on a good description of any!

THEOREM 4.1. Let $L(\alpha)$ satisfy ZFC, α countable, and $\alpha < \beta$ be infinite. Then $\{x \subseteq \alpha: L(\alpha,x)$ satisfies ZFC$\}$ is of full category and full measure in the Cantor space $S(\alpha)$.

Why is $S(\alpha)$ a Cantor space? Because $\alpha < \beta$ is a countably infinite ordinal.

Just to get one $x \subseteq L(\alpha)$ to work, we apparently need to get lots of them.

5. UNPROVABILITY OF THE CONTINUUM HYPOTHESIS IN ZFC.

Again let $L(\alpha)$ be a model of ZFC, where α is countable. There are a number of sharpened versions of Theorem 4.1.

THEOREM 5.1. Let $L(\alpha)$ satisfy ZFC, α countable, and assume that $L(\alpha)$ thinks that β is uncountable. Then $\{x \subseteq \alpha: L(\alpha,x)$ satisfies ZFC + $\neg$CH$\}$ is of full category and full measure in the Cantor space $S(\alpha)$.

So we now have the following.

THEOREM 5.2. If there exists $L(\alpha)$ satisfying ZFC, α countable, then ZFC + $\neg$CH is consistent.

Unfortunately, the hypothesis of Theorem 5.2 cannot be obtained from "ZF is consistent". So we work with finite fragments of ZF.

LEMMA 5.3. There exists $L(\alpha)$ satisfying any given specified finite fragment of ZFC, with α countable. This is provable in ZF for any specific finite fragment of ZFC.

LEMMA 5.4. Let T be a finite fragment of ZFC. Let $L(\alpha)$ satisfy a sufficiently large finite fragment of ZFC, where α is countable, and assume that $L(\alpha)$ thinks that $\alpha < \beta$ is uncountable. Then $\{x \subseteq \alpha: L(\alpha,x)$ satisfies T + $\neg$CH$\}$ is of full category and full measure in the Cantor space $S(\alpha)$.

THEOREM 5.5. If ZF is consistent then ZFC + $\neg$CH is consistent.

6. UNPROVABILITY OF THE AXIOM OF CHOICE IN ZF.

Again let $L(\alpha)$ satisfy ZFC, α countable. Let $x_1,x_2,...$ be an infinite sequence of sets. We define $L(\alpha,x_1,...)$ as expected:

$$L(0,x_1,\ldots) = \{x_1,\ldots\},$$
$$L(\alpha+1,x_1,\ldots) = FODO(L(\alpha,x_1,\ldots)),$$
$$L(\lambda,x_1,\ldots) = \bigcap\{L(\alpha,x_1,\ldots): \alpha < \lambda\}$$

where λ is a limit ordinal, $\alpha,\beta \in \lambda$.

THEOREM 6.1. Let $L(\lambda)$ satisfy ZFC, λ countable. Then $\{(x_1,\ldots) \in S(\lambda) : L(\lambda,x_1,\ldots)$ satisfies ZF + "$\neg$ is not well ordered"$\}$ is of full category and full measure in the Cantor space $S(\lambda)$.

Arguing as before, using finite fragments of ZFC, we get the following.

THEOREM 6.2. If ZF is consistent then ZF + "$\neg$ is not well ordered" is consistent. In particular, ZF + $\neg$AxC is consistent (if ZF is consistent).

7. APPLICATIONS OF FORCING.

The method of forcing is what is behind these category/ measure results. They can be proved without resorting to forcing,. However, it turns out to be too cumbersome to directly do category/measure arguments in more complicated situations without the machinery of forcing.

The technique is exquisitely applicable for a great many but not all set theoretic problems. The area is largely mined out, but what is missing is organizational results of an imaginative and striking character.

Let me mention just a small sample of attractive statements that are known to be neither provable nor refutable in ZFC (assuming ZF is consistent). (Item i needs a bit more than ZF is consistent).

i. All sets of reals that are set theoretically definable from a real and an ordinal are Lebesgue measurable (alternatively have the property of Baire; i.e., differ from an open set by a meager set).

ii. All sets of reals of cardinality less than $\neg$ are of measure zero (alternatively meager).

iii. Every dense linear ordering in which every set of pairwise disjoint open intervals is countable has a countable dense subset. (Souslin's hypothesis).

iv. All homomorphisms from the Banach algebra of continuous complex valued functions on [0,1] are continuous. (A conjecture of Kaplansky).

v. Every set of reals, all of whose homeomorphic images are of measure zero, is countable. (A conjecture of E. Borel).

8. LIMITATIONS OF FORCING.

Although CH is a monumentally important question for set theory, it has not proved to be so vital for mathematics.

One key reason is that the problem has been answered positively for "nice" sets of reals, long ago:

THEOREM 8.1. Every uncountable Borel measurable set of reals is in one-one correspondence with the set of all reals. In fact, the one-one correspondence can be taken to be Borel measurable.

The Borel measurable world - i.e., Borel measurable sets/functions in and between Polish spaces - is more than sufficient for the vast preponderance of current mathematical activity. So when a mathematician who is couching things in unusual generality, gets into logical trouble, he/she will generally find comfort in hiding out within (what amounts to) the Borel measurable world (or less). For instance, the world of finitely generated algebraic structures lies well within the Borel measurable world.

Let's see what happens to our five other examples of statements that are known to be neither provable nor refutable in ZFC.

i. All sets of reals that are set theoretically definable from a real and an ordinal are Lebesgue measurable (alternatively have the property of Baire). FOR BOREL SETS, OBVIOUSLY PROVABLE, SINCE BOREL SETS ARE MEASURABLE AND HAVE THE PROPERTY OF BAIRE.

ii. All sets of reals of cardinality less than ¬ are of measure zero (alternatively meager). FOR BOREL SETS OBVIOUSLY PROVABLE SINCE THEY MUST BE COUNTABLE.

iii. Every dense linear ordering in which every set of pairwise disjoint open intervals is countable has a countable dense subset. (Souslin's hypothesis). IF THE ORDERING IS BOREL THEN THIS HAS BEEN PROVED.

iv. All homomorphisms from the Banach algebra of continuous complex valued functions on [0,1] are continuous. (A conjecture of Kaplansky). IN VERY GENERAL SETTINGS, EVERY BOREL HOMOMORPHISM IS CONTINUOUS.

v. Every set of reals, all of whose homeomorphic images are of measure zero, is countable. (A conjecture of E. Borel). SINCE EVERY UNCOUNTABLE BOREL SET HAS A PERFECT SUBSET, IT HAS A HOMOEOMORPHIC IMAGE OF POSITIVE MEASURE. HENCE PROVABLE.

We now mention some general limitations to forcing.

First of all, an ultimate for a logician, something totally out of reach, is to show that some specific notorious standard looking statements in very finite mathematics cannot be proved or refuted in ZFC.

EXAMPLE: Show that "□^□^□^□ is rational" is neither provable nor refutable in ZFC, assuming ZF is consistent.

Forcing is powerless to deal with a problem like this. The same is true of Gödel's inner model technique (constructible sets).

Of course, I am powerless to deal with a problem like this. But in the case of forcing and constructible sets, we know by the following general Remark just why.

REMARK. For any model of ZFC, all of its forcing extensions and all of its inner models have isomorphic rings of integers, and so obey the same sentences of finite set theory.

The situation is much worse than this. Consider sentences of the form

$$(\Box x \in N)(\Box y \in N)(A(x,y))$$

where A involves only quantification over N. Concrete mathematics tends to involve only quantification over N. And when it goes beyond this, it tends to involve only one quantifier over subsets of N. Here we have two such quantifiers.

THEOREM 8.1. For any model of ZFC, all of its forcing extensions and all of its inner models obey the same sentences with at most two quantifiers over subsets of N (as above).

9. AN EXAMPLE FROM THE BOREL UNIVERSE.

Let S be a set of ordered pairs and A be a set. We say that f is a selection for S on A iff dom(f) = A and for all x $\in$ A, (x,f(x)) $\in$ S.

PROPOSITION. Let S $\subseteq$ ¬ x ¬ be Borel and E $\subseteq$ ¬ be Borel. If there is a Borel selection for S on every compact subset of E, then there is a Borel selection for S on E.

THEOREM 9.1. The Proposition cannot be proved or refuted in ZFC, assuming a bit more than ZF is consistent.

This Proposition is due to some functional analysts with a great deal of expertise in descriptive set theory at Paris VII, Debs and Saint Raymond. They were knowledgeable enough to have proved it using some well known candidate axioms going well beyond ZFC.

10. AN EXAMPLE FROM DISCRETE MATHEMATICS.

We have just seen that there are statements about the Borel universe being considered by analysts in the natural course of their research, that cannot be proved or refuted in ZFC.

There is a great deal of skepticism that there are statements in discrete mathematics being considered by mathematicians in the natural course of their research, that cannot be proved or refuted in ZFC - or at least, that logicians have any serious chance of showing cannot be proved or refuted in ZFC.

However, a new area of discrete mathematics, with a clear thematic purpose, is emerging. The new area has attractive

statements, delicate proofs, connections with various parts of mathematics, and a vast array of deep open problems.

But some of the sharp results in the area cannot be proved or refuted in ZFC, but can be proved using well known candidates for new axioms.

This new area of discrete mathematics is called BOOLEAN RELATION THEORY (BRT).

In fact, BRT is not at all restricted to discrete mathematics. It makes sense as a project in virtually any interesting mathematical context. We view BRT as a new kind of mathematical investigation.

We begin with a description of BRT in its most elemental forms. We will use N for the set of all nonnegative integers; i.e., $\mathbb{N}$.

In what we are going to call elemental BRT, one first identifies an interesting class V of multivariate functions, as well as an interesting class K of sets.

Let f be a multivariate function and A be a set. We write fA for the set of all values of f at arguments drawn from A. Thus fA is a convenient notation for the forward image of a multivariate function on a set.

E.g., let f be binary addition from N into N and A be the set of odd elements of N. Then fA is the set of even elements of N without 0.

Now one considers statements of the following form.

For all f $\in$ V there exists A $\in$ K such that some given Boolean relation holds between A and fA.

Let’s fix on two kinds of “Boolean relations”. A Boolean equation (inequation) is an equation (inequation) between Boolean combinations of A and fA.

To take complements, we need a universal set, which we take to be the union of the elements of K. (Remember, your mother told you never to take an unrestricted complement of a set! It’s way too big!! Don’t put more food on your plate than you can eat, your eyes are bigger than your stomach,

don’t go out without a jacket or you’ll catch a cold, etc.).

Standard Boolean algebra (or PROP) tells us that the number of formal Boolean equations (inequations), up to formal equivalence, in the two variables A,fA, is 16.

The simplest example that is rather important and deep is the following. Let MF(N) be the class of all functions of several variables from N into N (range contained in N), and INF(N) be the class of all infinite subsets of N.

THIN SET THEOREM. For all f ∈ MF(N) there exists A ∈ INF(N) such that fA ≠ N.

Unless you are adept at just the right branch of combinatorics, you will find this very difficult to prove.

All 16 statements in elemental inequational and equational BRT for MF(N) and INF(N) have been completely analyzed. For an interesting example of elemental equational BRT, we use the class SD(N) of all strictly dominating elements of MF(N). I.e., we require that for all x ∈ dom(f),

$$f(x) > \max(x).$$

COMPLEMENTATION THEOREM. For all f ∈ SD(N) there exists A ∈ INF(N) such that fA = N\A. Furthermore, A is unique.

This is a fixed point theorem that can be obtained from scratch, or by applying the contraction mapping theorem.

All 16 statements in elemental equational and inequational BRT for SD(N) and INF(N) have been completely analyzed. In (full blown) BRT we consider all statements of the following form:

For all $f_1,...,f_n \in V$ there exists $A_1,...,A_m \in K$ such that some given Boolean relation holds between the A’s and their forward images under the f’s.

The number of such statements is 2^2^m(n+1). Even for n = 1 and m = 2 (one function and two sets) this amounts to 2^{16}. The analysis of all these statements has yet to be done.

We have analyzed some special corner of equational BRT with 2 functions and 3 sets, and there is a big surprise. (The

number of statements with n = 2 and m = 3 is 2^{512}, quite a large number!).

In this corner of BRT, we use a natural subclass of MF(N) called the functions of expansive linear growth, ELG(N). Here we require that there exists constants c,d > 1 such that for all but finitely many x ∈ dom(f),

$$c|x| \leq f(x) \leq d|x|.$$

Here |x| is just max(x).

We use the standard disjoint union notation. We write X ⊔. Y (the disjoint union of X,Y) for X ∪ Y together with the commitment that X,Y are disjoint. For example,

$$X \sqcup. Y \sqcup Z \sqcup. W$$

means

$$X \sqcup Y \sqcup Z \sqcup W \sqcup X \cap Y = \emptyset \sqcup Z \cap W = \emptyset.$$

We have analyzed all statements of the following form:

PROPOSITION. For all f,g ∈ ELG(N) there exist A,B,C ⊆ INF(N) such that

$$X \sqcup. fY \sqcup Z \sqcup. gW$$
$$S \sqcup. fT \sqcup U \sqcup. gV$$

where X,Y,Z,W,S,T,U,V are among the letters A,B,C.

Obviously there are exactly $3^8 = 6561$ such statements.

It turns out that, up to obvious symmetry, all but ONE of these 6561 statements can be proved or refuted within a very weak fragment of ZFC. The ONE exception, up to symmetry, cannot be proved or refuted in ZFC.

The ONE exception, up to symmetry, can be proved using some well known candidate axiom - the existence of Mahlo cardinals of every finite order.

Here is the ONE exception, up to symmetry.

PROPOSITION*. For all f,g ∈ ELG(N) there exist A,B,C ⊆ INF(N) such that

A □. fA □ C □. gB
A □. fB □ C □. gC.