MATHEMATICAL FRONTIERS

The National Academies of SCIENCES ENGINEERING MEDICINE

nas.edu/MathFrontiers

Board on
Mathematical Sciences & Analytics

MATHEMATICAL FRONTIERS

2019 Monthly Webinar Series, 2-3pm ET

February 12: *Machine Learning for Materials Science**

March 12: *Mathematics of Privacy**

April 9: *Mathematics of Gravitational Waves**

May 14: *Algebraic Geometry**

June 11: *Mathematics of Transportation**

July 9: *Cryptography & Cybersecurity**

August 13: *Machine Learning in Medicine**

September 10: *Logic and Foundations*

October 8: *Mathematics of Quantum Physics*

November 12: *Quantum Encryption*

December 10: *Machine Learning for Text*

* Webinar posted

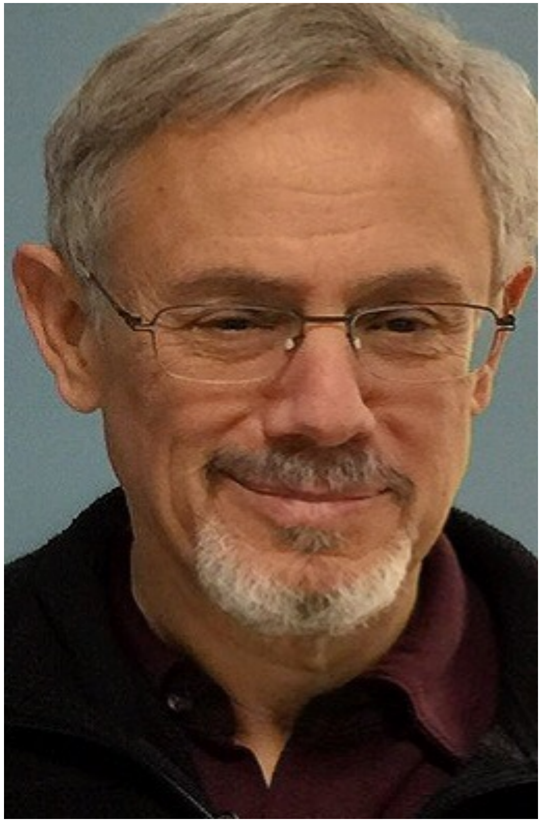
Made possible by support for BMSA from the
National Science Foundation
Division of Mathematical Sciences
and the
Department of Energy
Advanced Scientific Computing Research

View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers

MATHEMATICAL FRONTIERS
Logic and Foundations

Natasha Dobrinen, University of Denver

Julia Knight, University of Notre Dame



Mark Green, UCLA (moderator)

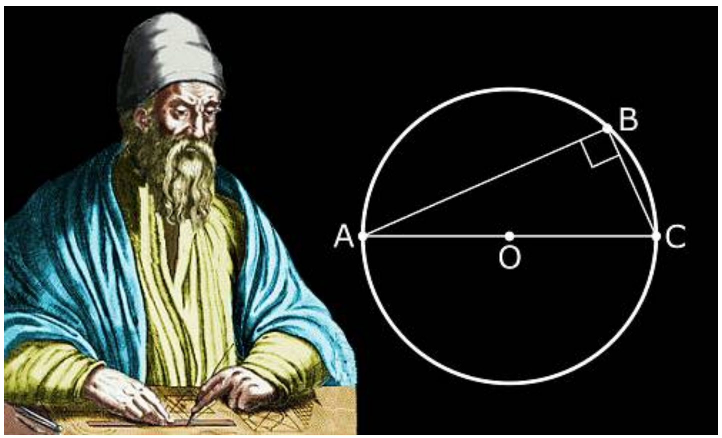
Natasha Dobrinen,
University of Denver

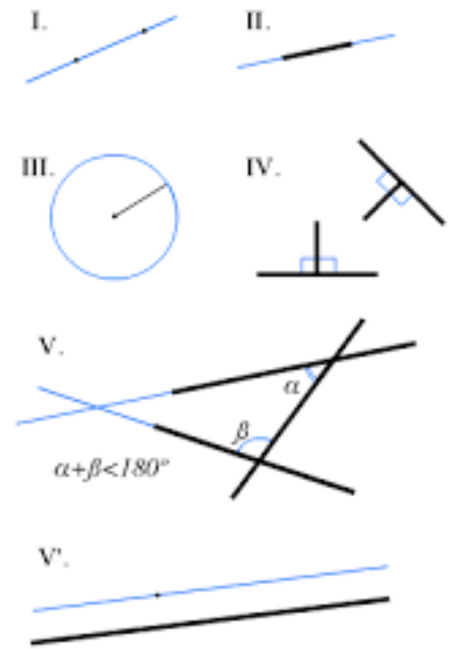
Professor of Mathematics

Logic and Foundations of Mathematics

What is foundations? How did it arise?

Foundations attempts to do for all of math what Euclid did for geometry.





Hilbert's Program: Fix a precise language.

Decide on a set of axioms (premises) which are self-evident.

Build and prove everything from these premises.

A Key Idea in the Development of Logic and Foundations

The Liar Paradox

"I am lying."

Central to this paradox is "self-reference."

This idea is key to several leaps in the development of modern logic and foundations.

Logic: A means of reasoning within a precise language

Rules of reasoning are clearly stated.

No contradictions should arise.

Logic is central to human discourse.

The law and scientific development rely on logic.

Modus Ponens

Sentential Logic is used to model basic arguments.

"If you do your chores, then I will pay you $20."

C = "You do your chores."   P = "I will pay you $20."

The red sentence is C implies P or $C \Rightarrow P$.

This is the rule of inference called modus ponens:

If C implies P and C is true, then P must also be true.

First-Order Logic

First-order logic can talk about "for all".

Variables: $v_1, v_2, v_3, \ldots$ range over all elements of one sort.

Symbols: $\Rightarrow$ (implies), $\neg$ (not), $\forall$ (for all), $=$
and possibly relation and function symbols.

Axioms: Logical and other axioms.

Rule of Inference: Modus Ponens $((A \Rightarrow B) \text{ and } A) \Rightarrow B$

First-Order Logic of Number Theory

Language: $v_1, v_2, \ldots, \neg, \Rightarrow, \forall, =, <, +, x, S, 0$.

Variables are intended to range over 0,1,2,3,4,…

Peano Postulates (12)

- 0 is not the successor of any natural number.

$$\forall v_1 \neg(S(v_1) = 0)$$

- First-Order Induction: For each formula ψ,

$$[\psi(0) \text{ and } \forall v_1 (\psi(v_1) \Rightarrow \psi(S(v_1)))] \Rightarrow \forall v_1 \psi(v_1)$$

- Second-Order Induction: Suppose K is a set containing 0, and whenever n is in K then n+1 is in K. Then K contains all natural numbers.

Set Theory as a Foundation for Math

Language: $v_1, v_2, \ldots, \forall, \neg, \Rightarrow, =, \in$ (membership relation)

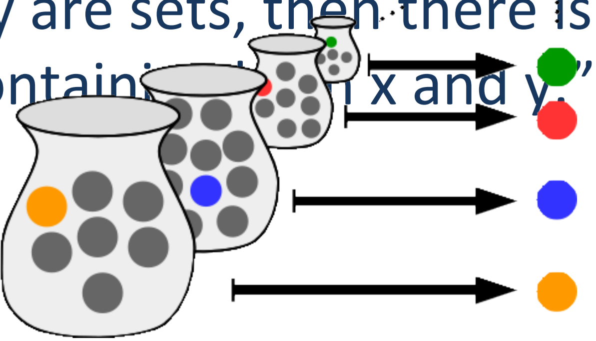
Variables range over sets.

Zermelo and Fraenkel's 9 Axioms = ZFC (1930's)

1. Extensionality Axiom: "Two sets are equal if and only if they have the same members."

4. Axiom of Pairs: "If x and y are sets, then there is a set containi [illegible] x and y."

9. Axiom of Choice:



Much of math can be done in ZFC

Using the ZFC Axioms of Set Theory, we can

- Construct the counting numbers, fractions, real numbers, functions, mathematical structures.
- Develop the majority of mathematics within this first-order logic framework.

Limitations of Formal Systems

Hilbert's Program

Find a complete and consistent set of axioms for all of mathematics.

Gödel's Incompleteness Theorem (1931)

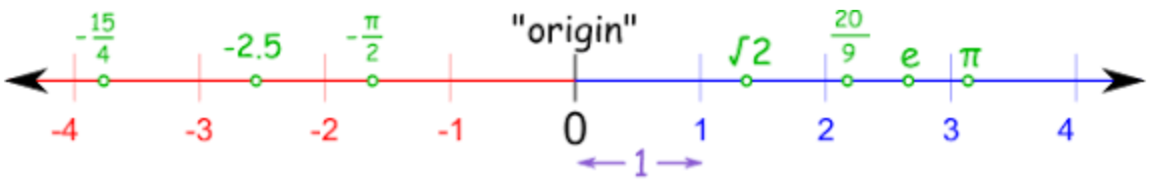
Any computable set of axioms strong enough to do arithmetic has statements which cannot be proved or disproved.

"I am not provable."

An unprovable statement

Cantor's Continuum Hypothesis (1873)

There is no set of real numbers with size intermediate between the integers and the real numbers.



"Is the Continuum Hypothesis true?"

(on Hilbert's List of Problems of the 20th Century)

Gödel (1938): There is a model of the Axioms of Set Theory in which CH is true.

Cohen (1962): There is a model of the Axioms of Set Theory in which CH is false.

What has been achieved?

- Firm footing for mathematics. Precision in the logic and axioms. No contradictions arising.
- Given axioms, some sentences cannot be proved or disproved; true/false is not always decidable by a computer.
- But, we have rigorous methods for proving statements are unprovable from some set of axioms.

Modern Foundations and Logic

- Maps out what is and what is not provable from a given set of axioms.
- Classifies precisely the relative strengths of mathematical statements.
- Applies techniques to solve tough problems in general mathematics, computer science, philosophy, linguistics, …

MATHEMATICAL FRONTIERS
Logic and Foundations

Julia Knight,
University of Notre Dame

Professor of Mathematics

Computability and Definability

Outline

- Computability—why we need a definition.
- Two ideas of Turing, with applications.
- Connection between recursion-theoretic complexity and complexity of definitions in the natural numbers.
- Results of Tarski on computability and definability in the reals, with applications.

Need for a definition of computability

When we describe an algorithm, or machine-like method for deciding or computing something, we don't need a definition.

We need a definition in order to show that there is no algorithm.

Defining computability

Several different-looking, but provably equivalent definitions were proposed Turing's definition involved an abstract machine.

The "Church-Turing Thesis" is the claim that the definitions are correct.

Useful Definition for Today. Something (a partial function) is *computable* if we can write a program to compute it.

The universal machine

- Turing had the theoretical idea of a machine that could take a program as part of its input.

Turing himself had in mind practical applications.

Relative computability

A second theoretical idea of Turing was the "oracle machine."

This is implemented today by equipping a computer with a CD-rom, or using an interactive program.

Definition. A is *computable relative to* B if there is a program for deciding membership in A, given answers to questions about membership in B.

Computably enumerable sets

- A set is *computably enumerable (c.e.)* if we can effectively list the elements; equivalently, it is the domain of a partial computable function.

- **Fact**: A set is computable if and only if it and its complement are both c.e.

Halting set

- The *halting set* K is the set of numbers n such that program number n, with input n, will halt.
- **Fact**: K is c.e. but not computable.
- The existence of such a set has applications in several branches of mathematics.

Jumps

- For any set X, the *jump* is the set X' consisting of numbers n such that program number n halts given oracle X and input n.

- **Fact**: X' is c.e. relative to X but not computable relative to X.

Arithmetical sets

- The *arithmetical* sets and relations are the ones definable in the "standard model" of arithmetic ($\mathbb{N}$,+,x,0,1,<).

- We get a proper hierarchy, based on the number of alternations of existential and universal quantifiers in the defining formula.

This hierarchy is important to me, for measuring complexity in algebraic structures.

True Arithmetic

- True Arithmetic (TA) is the set of elementary first order sentences true in the standard model.

- It follows from Gödel's Incompleteness Theorem that this set is not computable.

Fact: We have elementary first order sentences saying that n **ε** K, n **ε** K', n **ε** K'', etc.

Hence, TA is much more complicated than K.

Tarski and the reals

- The ordered field of reals is $(\mathbb{R},+,\times,0,1,<)$.
- We have seen that the theory TA is very complicated.

Theorem (Tarski): The elementary first order theory of the reals is computable—decidable.

Tarski's proof

- Tarski gave a computable set of axioms sufficient to show every formula equivalent to one that is quantifier-free, and to prove all true quantifier-free sentences.

- He remarked that the sets definable in the reals are just the finite unions of intervals.

Building on Tarski's remark

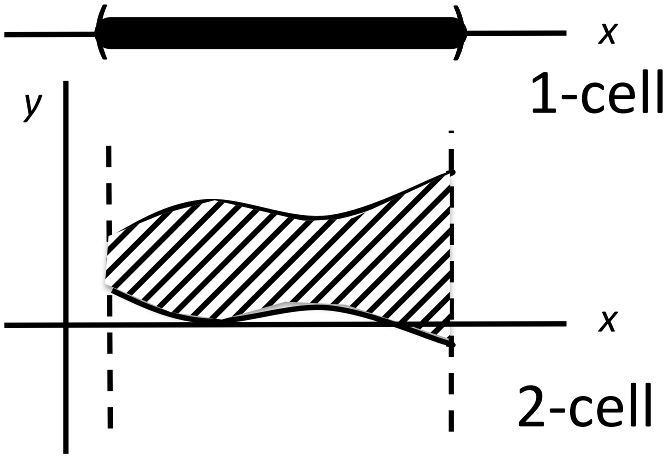
van den Dries, and Pillay-Steinhorn began a study of "o-minimality."

Wilkie showed that when we add to the reals the exponential function and pieces of other analytic functions, the structure remains o-minimal.

There are now many applications of o-minimality.

Lafferriere, Pappas, and Sastry

- A *hybrid system* has discrete aspects and continuous aspects.
- With luck, there are formulas defining the regions of good behavior of the system in some o-minimal expansion of the reals.
- By o-minimality, each definable region is a finite union of nice "cells."
- We may then treat the whole system as discrete, admitting control by a finite automaton.

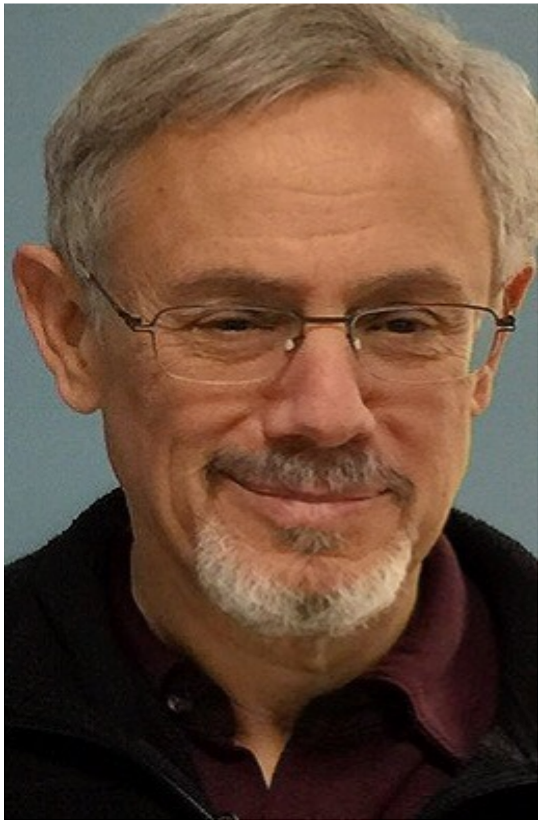


MATHEMATICAL FRONTIERS

Logic and Foundations

Natasha Dobrinen, University of Denver

Julia Knight, University of Notre Dame



Mark Green, UCLA (moderator)

View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers

MATHEMATICAL FRONTIERS
2019 Monthly Webinar Series, 2-3pm ET

February 12: *Machine Learning for Materials Science**

March 12: *Mathematics of Privacy**

April 9: *Mathematics of Gravitational Waves**

May 14: *Algebraic Geometry**

June 11: *Mathematics of Transportation**

July 9: *Cryptography & Cybersecurity**

August 13: *Machine Learning in Medicine**

September 10: *Logic and Foundations*

October 8: *Mathematics of Quantum Physics*

November 12: *Quantum Encryption*

December 10: *Machine Learning for Text*

** Webinar posted*

Made possible by support for BMSA from the
National Science Foundation
Division of Mathematical Sciences
and the
Department of Energy
Advanced Scientific Computing Research

View webinar videos and learn more about BMSA at www.nas.edu/MathFrontiers