The Role of Mathematical Logic in Computer Science and Mathematics

Summary:

Early developments:
Aristotle (classical), Boole and Frege (formalisation)

Kurt Gödel: Completeness and Incompleteness

The four branches of Mathematical Logic: Set Theory, Model Theory, Computability Theory and Proof Theory

Connections with Computer Science and Mathematics

The Kobe Group: The Foundation of Information Sciences Division of the Department of Information Science

The Development of Mathematical Logic: Aristotle

Aristotle: Concept of *Logical Inference*.

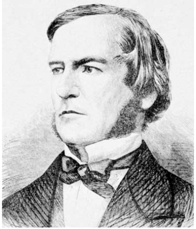
His famous example of a Deduction:
Socrates is a man.
All men are mortal.
Conclusion: Socrates is mortal.

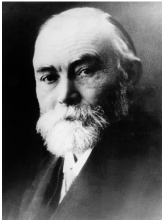
This was expressed “informally” in “natural language”, the language we use to communicate.

The Development of Mathematical Logic: Formalisation

Deductive Logic remained “informal” until the 19th Century!

$\approx$ 1850-1875: Formal Deductive Logic (Boole, Frege)





The Development of Mathematical Logic: Formalisation

Propositional Logic

$A, B, C, \ldots$ are symbols for statements, either True or False

Combine these with Logical Connectives $\wedge, \vee, \rightarrow, \sim, \leftrightarrow, \ldots$

$A \rightarrow A$
$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$
$((A \rightarrow B) \wedge (\sim A \rightarrow B)) \rightarrow B$
$((A \rightarrow B) \wedge (\sim B \rightarrow A)) \rightarrow B$

These are *Tautologies*, always true; but

$(A \rightarrow B) \rightarrow (B \rightarrow A)$

is *not* a Tautology

The Development of Mathematical Logic: Formalisation

Predicate Logic

For some statements we need more than Propositional Logic

Aristotle's example again:

Socrates is a man.

All men are mortal.

Conclusion: Socrates is mortal.

To express this in symbols we need:

Symbol S for Socrates: *Constant Symbol*

Symbols M, Mor for “is a man”,“is mortal”: *Predicate Symbols*

Symbol $\forall$ for “All”: *Quantifier Symbol*

Now we have the *Logical Rule*:

$M(S)$

$\forall x(M(x) \to Mor(x))$

Conclusion: $Mor(S)$

The Development of Mathematical Logic: Axioms and Rules

Important Question: What is Logical Inference?
When does a statement *follow logically* from other statements?

This Question is crucial for the Foundations of Mathematics

To answer this Question we use *Axioms* and *Rules of Inference*

For *Propositional Logic:*

Axioms

1. $\varphi \to (\psi \to \varphi)$
2. $(\varphi \to (\psi \to \gamma)) \to ((\varphi \to \psi) \to (\varphi \to \gamma))$
3. $(\sim \varphi \to \sim \psi) \to ((\sim \varphi \to \psi) \to \varphi)$

Rule of Inference

Given φ and $\varphi \to \psi$, conclude ψ

We have:

Completeness Theorem: Any tautology can be proved using the above Axioms and Rule of Inference

The Development of Mathematical Logic: Axioms and Rules

There is also a good system for *Predicate Logic*; the main new *Axioms* are:

$\forall x(\varphi \rightarrow \psi) \rightarrow (\forall x\varphi \rightarrow \forall x\psi)$

$\forall x\varphi \rightarrow \varphi^x_t$, where φ^x_t is obtained by substituting the term t for the variable x in φ (with certain restrictions)

Gödel's Completeness Theorem: Any Tautology of *Predicate Logic* can be proved using the above Axioms and Rule of Inference

The Development of Mathematical Logic: Axioms and Rules

So far we have only considered systems for proving Tautologies
Now we look at systems for proving statements in Arithmetic

Peano Arithmetic (PA):

Constant Symbol: 0

Function Symbols: S (Successor), $+$ and $\cdot$

Axioms:

$S(x) \neq 0$, $S(x) = S(y) \rightarrow x = y$

$y \neq 0 \rightarrow \exists x(S(x) = y)$

$x + 0 = x$, $x + S(y) = S(x + y)$

$x \cdot 0 = 0$, $x \cdot S(y) = (x \cdot y) + x$

Induction Axioms: $\varphi(0) \rightarrow (\forall x(\varphi(x) \rightarrow \varphi(S(x))) \rightarrow \forall x \varphi(x))$

Completeness Question for Arithmetic: Can every true statement of arithmetic be proved in the above system PA?

Gödel's Big Surprise: No! In fact there is no reasonable system which is complete for Arithmetic

The Development of Mathematical Logic: Gödel Incompleteness

Before Gödel there were two possibilities for a Problem P:

1. Somebody can solve the Problem P
2. No one can solve P; P is a very difficult Problem

Since Gödel we have a third possibility:

3. P is Unsolvable!

In other words:

Provable implies True

But True does NOT imply Provable, no matter what the Axioms are

We can never have enough Axioms to achieve Completeness

The Development of Mathematical Logic: Gödel

Kurt Gödel

1906 born in Brno, Bohemia
From 1924: Studies at the University of Vienna
1930 Ph.D.: The Completeness Theorem for Predicate Logic
1933 Habilitation: The Incompleteness Theorems
1935-37 Set Theory: Axiom of Choice, Continuum Hypothesis

The Father of Modern Logic

The Development of Mathematical Logic: Gödel Incompleteness

Gödel's proof has two main ideas:

1. Arithmetisation
2. Diagonalisation

The Development of Mathematical Logic: Gödel Incompleteness

Idea 1: Arithmetisation

Arithmetical Properties

n is even $(0, 2, 4, 6, \ldots)$
n is a square $(0, 1, 4, 9, \ldots)$
The n-th digit of π $(= 3.14159265...)$ is 1

These can be described with formulas; for example:

$$n \text{ is a square} \Leftrightarrow \exists m(m \cdot m = n)$$

and every formula is a finite sequence of Symbols; for example

$\exists m(m \cdot m = n)$ is the sequence

$$\exists,\ m,\ (,\ m,\ \cdot,\ m,\ =,\ n,\ )$$

The Development of Mathematical Logic: Gödel Incompleteness

Every formula has a code number (*Gödel number*)

n is a square $\Leftrightarrow \exists m(m \cdot m = n)$

1. $\exists$
2. m
3. $($
4. $\cdot$
5. $=$
6. n
7. $)$

So $\exists m(m \cdot m = n)$ is coded as follows:

$(1, 2, 3, 2, 4, 2, 5, 6, 7)$

and the Gödel number of the above formula is 123242567

The Development of Mathematical Logic: Gödel Incompleteness

Every proof has a Gödel number:

A *Proof* P is a finite sequence of Formulas, for example:

$$P = (F_1, F_2, F_3, F_4, F_5).$$

If F_1, F_2, F_3, F_4, F_5 have the Gödel numbers

$$(15762534, 1345772, 134544422, 1232145, 1364234)$$

then the proof P has the Gödel number:

$$157625340134577201345444220123214501364234$$

The Development of Mathematical Logic: Gödel Incompleteness

Idea 2: Diagonalisation

Now we show: True does *not* imply provable

We have:
The Formulas: $F_1, F_2, F_3, \ldots$
The Proofs: $P_1, P_2, P_3, \ldots$
Now write $F_m(n)$ for: n satisfies the formula F_m
Also define Truth $\mathcal{T}$:

$$\mathcal{T}(m, n) \Leftrightarrow F_m(n) \text{ is true}$$

and Provability $\mathcal{P}$:

$$\mathcal{P}(m, n) \Leftrightarrow F_m(n) \text{ is provable}$$

Provable $\Rightarrow$ True

The Development of Mathematical Logic: Gödel Incompleteness

The difference between Provability and Truth:

$\mathcal{P}(m, n)$ *is an arithmetical property:*

$\mathcal{P}(m, n) \Leftrightarrow$
$F_m(n)$ is provable $\Leftrightarrow$
$\exists g(P_g$ is a proof of $F_m(n))$

But $\mathcal{T}(m, n)$ *is not an arithmetical property:*

The Development of Mathematical Logic: Gödel Incompleteness

If $\mathcal{T}(m, n)$ were arithmetical then so would be

$\mathcal{D}(n)$: $F_n(n)$ is false (i.e. $\mathcal{T}(n, n)$ is false)

But:

$\mathcal{D}(0)$ is true $\Leftrightarrow F_0(0)$ is false
$\mathcal{D}(1)$ is true $\Leftrightarrow F_1(1)$ is false
$\mathcal{D}(2)$ is true $\Leftrightarrow F_2(2)$ is false
etc.

$\mathcal{D} \neq F_0, F_1, \ldots$
$\mathcal{D}$ is not an arithmetical property

So $\mathcal{P} \not\Leftrightarrow \mathcal{T}$!
Provable $\not\Leftrightarrow$ True!

Gödel's Conclusion

Provable $\nLeftrightarrow$ True
Provable $\Rightarrow$ True
True $\nRightarrow$ *Provable*!

The Development of Mathematical Logic: Gödel Undecidability

So not every true formula of arithmetic is provable; but is there an algorithm to *test whether or not* a formula is provable?

No, by another Diagonalisation!

Define $F_m^{\mathcal{P}}(n)$: $F_m(n)$ is provable

Gödel Representation Theorem:
If $\mathcal{R}(n)$ is computable then
$\mathcal{R} = F_m^{\mathcal{P}}$ for some m

If $\mathcal{P}(m, n)$ were computable, then so would be

$\mathcal{D}^{\mathcal{P}}(n)$: $F_n(n)$ is unprovable ($F_n^{\mathcal{P}}(n)$ is false)

But $\mathcal{D}^{\mathcal{P}} \neq F_m^{\mathcal{P}}$ for each m

So $\mathcal{D}^{\mathcal{P}}$ is *not* computable

Provability is not Computable (*Gödel Undecidability*)

The Development of Mathematical Logic: Gödel Incompleteness

Gödel's incompleteness work in 1931 implies that the standard system for arithmetic, Peano Arithmetic (PA), is incomplete

Until 1977 it was believed that all “natural” problems in arithmetic could be solved in PA

We now take a closer look at incompleteness in arithmetic.

The Development of Mathematical Logic: Gödel Incompleteness

Example

i. Choose a number; express it in terms of 1's and 2's. For example:

$$8 = 2^{(2+1)}$$

ii. Replace 2 by 3, subtract 1 und express the result in terms of 1's, 2's and 3's:

$$2^{(2+1)} \Rightarrow 3^{(3+1)} = 81 \Rightarrow 80 = 2 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2$$

iii. Replace 3 by 4, subtract 1 and express the result in terms of 1's, 2's, 3's and 4's:

$$2 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2 \Rightarrow$$
$$2 \cdot 4^4 + 2 \cdot 4^2 + 2 \cdot 4 + 2 = 554 \Rightarrow$$
$$553 = 2 \cdot 4^4 + 2 \cdot 4^2 + 2 \cdot 4 + 1$$

Continue

The Development of Mathematical Logic: Gödel Incompleteness

In the above example we get the sequence
8,80,553,6310,93395,1647194,33554570,. . .

Goodstein's Theorem. Eventually we reach 0*!*

a. This Theorem is true
b. It is unprovable in PA (with the usual Induction Principle)!

We need new Axioms

To understand the *finite* numbers we need *Infinity*

The Development of Mathematical Logic: Set Theory

To prove Goodstein's Theorem we need an Induction Principle on the *Ordinal Numbers*:

$$0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega \cdot \omega, \ldots, \omega^{\omega}, \ldots,$$

$$\omega^{\omega^{\omega}}, \ldots, \omega^{\omega^{\omega^{\omega}}}, \ldots, \omega^{\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}} = \epsilon_0$$

What are these "Ordinal Numbers"?

Cantor discovered them in his study of *Infinity*

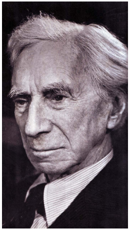
The Development of Mathematical Logic: Set Theory

Theory of Infinity = Set Theory

Georg Cantor

Berlin doctorate 1867 (number theory)
Halle habilitation 1870 (number theory)
Heine ⇒ Study of trigonometric series ⇒ Set Theory
Opposition from Kronecker, Support from Dedekind
Mittag-Leffler: "His work came 100 years too soon"
Cantor's theory was very nice, but had a serious problem:

The Development of Mathematical Logic: Set Theory



Bertrand Russell

Russell's Paradox

Let X be the set of all x such that $x \notin x$
Then $X \in X \leftrightarrow X \notin X$!

What are we going to do?

Ernst Zermelo

Zermelo's proposal: Axiomatic Set Theory

Only use "standard operations" to form new sets from old sets

Z = Axioms of Zermelo Set Theory

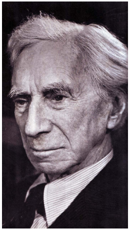
ZFC = Zermelo-Fraenkel Set Theory with the Axiom of Choice

ZFC does for Set Theory what PA does for Arithmetic

The Development of Mathematical Logic

Now our problems with paradoxes in Set Theory are over and we have good news:

ZFC Set Theory gives us a Foundation for all of Mathematics



Principia Mathematica: Reduces mathematics to Set Theory

Mathematical Objects can be regarded as Sets

Mathematical Properties can be expressed in Set Theory

For example:

The natural number n can be viewed as the set $\{0, 1, \ldots, n-1\}$

An ordered pair (m, n) of natural numbers can be viewed as the set $\{\{m\}, \{m, n\}\}$

A function from $\mathcal{N}$ to $\mathcal{N}$ is a set f of ordered pairs such that $(m, n_0), (m, n_1) \in f$ implies $n_0 = n_1$

Etcetera: $\mathcal{Q}$ (rationals), $\mathcal{R}$ (reals), functions from $\mathcal{R}$ to $\mathcal{R}$, $\cdots$

The Development of Mathematical Logic: Gödel again

But Gödel Incompleteness also applies to ZFC Set Theory

Is there a nice example of ZFC incompleteness like Goodstein's example for PA?

The Development of Mathematical Logic: The Continuum Problem

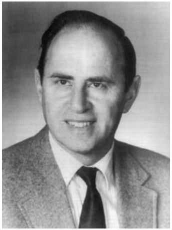
Cantor's Continuum Problem: How many real numbers are there?

Cantor's Continuum Hypothesis (CH): Any two uncountable sets of real numbers have the same size.

ZFC is not strong enough to answer this question!

ZFC does not prove the negation of CH (Gödel Constructibility)

The Development of Mathematical Logic: The Continuum Problem



Paul Cohen

ZFC does not prove CH

The Development of Mathematical Logic: Summary

1. Aristotle: Logic in natural language
2. Boole, Frege: Formal Predicate Logic
3. Gödel Completeness for Predicate Logic
4. Gödel Incompleteness for Arithmetic (PA)
5. Goodstein's natural example of incompleteness for PA
6. Cantor's Set Theory
7. Zermelo's axiomatic Set Theory
8. Russell's *Principia*: Mathematics reduced to Set Theory
9. Gödel, Cohen: Incompleteness in Set Theory (CH)

The Development of Mathematical Logic: Four Fields

Gödel's work led to the four main fields of Mathematical Logic today:

Gödel Completeness $\rightarrow$ *Model Theory*
Gödel Incompleteness $\rightarrow$ *Proof Theory*
Gödel Undecidability $\rightarrow$ *Computability Theory*
Gödel Constructibility $\rightarrow$ *Modern Set Theory*

How are these fields connected with Mathematics and Computer Science?

Mathematical Logic and Mathematics

Set Theory and Mathematics

Independence results: Statements like CH which cannot be decided in ZFC

Example (Shelah): Is every Whitehead group free?

Unclassifiability results: Natural classes of mathematical objects have no nice classification

Example (Thomas): There is no reasonable classification of torsion-free Abelian groups of finite rank

Model Theory and Mathematics

New results in algebra, number theory

Example (Hrushovski): Mordell-Lang Conjecture for function fields

Mathematical Logic and Mathematics

Computation Theory and Mathematics

Algorithmically unsolvable problems

Example (Matijasevich) There is no algorithm for solving Diophantine equations

Proof Theory and Mathematics

Improved results in mathematics through the analysis of proofs

Example (Kohlenbach) Effective bounds in functional analysis through proof mining

Mathematical Logic and Computer Science

The connections between Mathematical Logic and Computer Science are numerous; for example:

Propositional Logic and SAT Solvers
Predicate Logic and Software Micromodels
Temporal Logic and Model Checking
Hoare Logic, Dynamic Logic and Program Verification
Modal Logic and Multi-Agent Systems
Type Theory and Programming Languages
Finite Model Theory and Computational Complexity
Finite Descriptive Set Theory and Computational Complexity
Automatic Theorem Proving
Logic Programming

The Kobe Group

Set Theory: S.Fuchino, J.Brendle, H.Sakai

Large Cardinals, Combinatorial Set Theory, Forcing Theory and Descriptive Set Theory

Saturated Ideals and Combinatorical Principles
Ideals on the Real Line
Applications to Group Theory, Topology and Functional Analysis

Model Theory: H.Kikyo

Central questions in Shelah's Stability Theory

Homogeneous groups
Generic automorphisms and structures
Amalgamation properties

The Kobe Group

Proof Theory: M.Kikuchi

Incompleteness Theorems, Design Theory

New proofs of Gödel Incompleteness
Abstract Design Theory
Non-deductive Inference

Logic and Computer Science: N.Tamura, M.Banbara

Logic Programming, SAT Solvers, Constraint Satisfaction

Heterogeneous Constraint Solving
Linear Logic Theorem Provers
The Strip Packing Problem

Mathematical Logic is very well-represented in Kobe!

Best Wishes

I offer my best wishes for a bright future for the new

Kobe Graduate School of System Informatics!