Mathematics for Computer Science

Prof.dr.hab. Viorel Bostan

Technical University of Moldova

viorel.bostan@adm.utm.md

Lecture 2. Part 2

Picture of the day: Raphael, “Scuola di Atene”, Vatican

Math logic joke:

I asked my wife what she wanted for her birthday.

She said, "Nothing would make me happier than diamond earrings."

So, I got her nothing.

Definition

Mathematical logic is concerned with formalizing and analyzing the kinds of reasoning used in mathematics.

Recall the elementary geometry course from high school.

Part of the problem with formalizing mathematical reasoning is the necessity of precisely specifying the language(s) in which it is to be done.

The natural languages spoken by humans won't do:

Natural Language Limitations

Natural languages are complex and continually changing as to be impossible to pin down completely. Moreover, the ambiguities inherent in everyday language can be a real problem.

Natural Languages

Definition (What is a language?)

Language is the (human) capacity for acquiring and using complex systems of communication, or a specific instance of such a system of complex communication.

Languages can be **natural** (English, Romanian, Japanese, Zulu, Esperanto, etc) or **formal.**

Definition (Formal Language)

A language is **formal** if it is provided with a mathematically rigorous representation of its:

- alphabet of symbols,
- formation rules specifying which strings of symbols count as well-formed.

Ambiguity of Natural Language

Example

A boy touches the girl with the flower.

Consider some sequences taken from English language:

1. "You may have cake or you may have ice cream."
2. "If you don't clean your room, then you won't play Counter Strike!"
3. "If pigs can fly, then you can understand the Banach-Tarsky Theorem."
4. "If you can solve any problem we come up with in this class, then you get grade 10 for this course."
5. "Every human has a dream."

Ambiguity of Natural Language

"You may have cake or you may have ice cream."

Can you have both cake and ice cream or must you choose just one desert?

"If you don't clean your room, then you won't play Counter Strike!"

If you aren't playing the game, does it mean that you didn't clean your room?

"If pigs can fly, then you can understand the Banach-Tarsky Theorem."

If this is true, then is the Banach-Tarsky Theorem incomprehensible?

Ambiguity of Natural Language

"If you can solve any problem we come up with in this class, then you get grade 10 for this course."

If you can solve some problems we come up with but not all, then do you get a 10 for the course?

And can you still get a 10 even if you can't solve any of the problems?

"Every human has a dream."

Does the last sentence imply that all humans have the same dream or might they each have a different dream?

Some uncertainty is tolerable in normal conversation. But ...

Imperativ!

We need to formulate ideas precisely as in mathematics.
The ambiguities inherent in everyday language become a real problem!

We can't hope to make an exact argument if we're not sure exactly what the individual words mean.

To get around the ambiguity of English, mathematicians have devised a special language for talking about logical relationships.

This language mostly uses ordinary English words and phrases such as **"and"**, **"or"**, **"implies** and **"for all"**.

But mathematicians endow these words with definitions more precise than those found in an ordinary English dictionary.

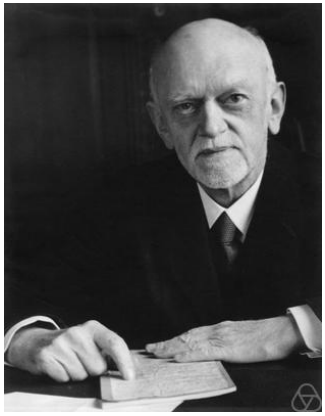
Entscheidungsproblem

Given a set Σ of hypotheses and some statement φ, is there an effective method for determining whether or not the hypotheses in Σ are sufficient to prove φ?

Historically, this question arose out of David Hilbert's scheme to secure the foundations of mathematics by axiomatizing mathematics in 1*st*-order logic, showing that the axioms in question do not give rise to any contradictions, and that they suffice to prove or disprove every statement (which is where the *Entscheidungsproblem* comes in).

If the answer to the *Entscheidungsproblem* were "yes" in general, the effective method(s) in question might put mathematicians out of business.

Mathematical Logic. Some history



David Hilbert, 1862-1943

Trying to find a suitable formalization of the notion of **"effective method"**, mathematicians developed abstract models of computation in the 1930's:

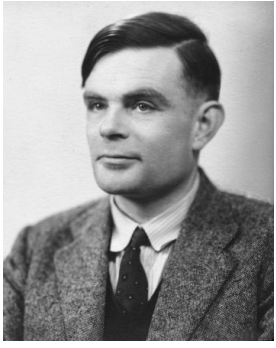
- *Recursive functions*,
- $\lambda-$*calculus*,
- *Turing machines*,
- *Formal grammars*.

These models are very different, but they were all essentially equivalent in what they could do.

Church–Turing Thesis

A function is effectively computable in principle in the real world if and only if it is computable by (any) one of the abstract models mentioned above.

Alonzo Church, 1903–1995



Alan Turing, 1912–1954

Definition

A proposition is a statement that is either true or false.

Proposition

$2 + 3 = 5$.

Proposition

Pigs can fly.

Proposition

Tomorrow is Monday.

Proposition

Chisinau is the capital of Republic Moldova.

Wrong propositions

Definition

A proposition is a statement that is either true or false.

Note that even if this definition is quite general it excludes such sentences as

1. "O Romeo, Romeo! Wherefore art thou Romeo?"
2. "Help me!"
3. "Don't be stupid."
4. "Learn mathematics!"

Proposition?

The northwestern wind through the Groenland.

Proposition

This statement is false.

Proposition A

All Greeks are human.

Proposition B

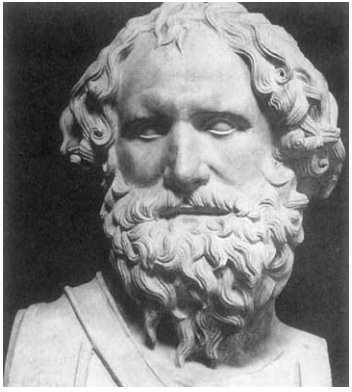
All humans are mortal.

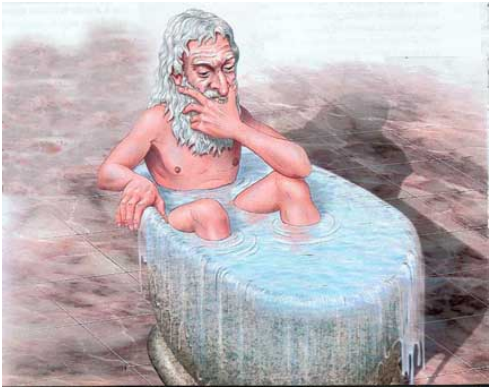
Proposition C

All Greeks are mortal.

Archimedes spent some time playing with such sentences (called logic syllogisms) in the 3*rd* century BC.

If **A** is true, and **B** is true, then **C** is also true!





Archimedes of Syracuse, 287–212 BC

Archimedes developed an early form of logic that he applied in proving rigorously geometrical theorems including the area of a circle, the surface area and volume of a sphere.

Proposition

Let $p(n) = n^2 + n + 41$. Then for every $n \in \mathbb{N}$, $p(n)$ is a prime number.

$$\begin{aligned} p(0) &= 41 : \textit{prime} \\ p(1) &= 43 : \textit{prime} \\ p(2) &= 47 : \textit{prime} \\ p(3) &= 57 : \textit{prime} \end{aligned}$$

So far so good! Let's continue with $4, 5, 6, \ldots, 20$

$$p(20) = 461 : \textit{prime}!$$

Beautiful! Don't stop!

$$p(39) = 1601 : \textit{prime}!$$

Proposition

Let $p(n) = n^2 + n + 41$. Then for every $n \in \mathbb{N}$, $p(n)$ is a prime number.

$$p(40) = 1681 : \textit{Not} \quad \textit{prime}!$$

$$\begin{aligned} p(40) &= 40^2 + 40 + 41 \\ &= 40(40 + 1) + 41 \\ &= 40 \cdot 41 + 41 \\ &= 41 \cdot 41 \end{aligned}$$

Therefore, the above proposition is FALSE!

Eurler Conjecture

Proposition

Equation $a^4 + b^4 + c^4 = d^4$ has no solutions in nonnegative natural numbers.

In logical notations (mathematicians like notations a lot!) it says

$$\forall a \in \mathbb{Z}^+, \forall b \in \mathbb{Z}^+, \forall c \in \mathbb{Z}^+, \forall d \in \mathbb{Z}^+, a^4 + b^4 + c^4 \neq d^4.$$
$$\forall a, b, c, d \in \mathbb{Z}^+, a^4 + b^4 + c^4 \neq d^4.$$

Euler made this **conjecture** in 1769.
For 218 years no one knew whether this proposition was true or false.

Finally, in 1987 Noam Elkies from Harvard University found a solution to the equation:

$$a = 2682440, b = 15365639, c = 18796760, d = 20615673.$$

So the proposition is False!

Theorem, lemma, corollary, conjecture

Definition

Proposition is a statement that is either true or false.

Definition

Important propositions are called **theorems**.

Definition

A **lemma** is a preliminary proposition useful for proving later propositions/theorems.

Definition

A **corollary** is a proposition that follows in just a few logical steps from a theorem.

Definition

A **conjecture** is a proposition that is not yet proved or disproved.

Propositions

Proposition

$313(x^3 + y^3) = z^3$ has no solution when $x, y, z \in \mathbb{N}$.

This proposition is false, but the smallest counterexample has more than 1000 digits!

Proposition (Goldbach Conjecture)

Every even integer greater that 2 is the sum of two primes!

For example, $4 = 2 + 2$, $10 = 3 + 7$, $22 = 17 + 5$, $40 = 37 + 3$. This is the famous "Goldbach Conjecture," which dates back to 1742. No one knows whether this proposition is true or false. It was checked for all numbers up to 10^{16}.

Proposition

The original Pentium chip divided properly.

Intel's "proofs" by authority and by sampling turned out to be invalid.

Why do you believe that $3 + 3 = 6$?

Is it because your primary school teacher, *Dna Maria*, told you so?

She might have been lying, you know.

Or are you trusting life experience?

If you have 3 apples and someone gives you 3 more apples, then you have aha! 6 apples.

If that is the true basis for your belief, then why do you believe that

$$3\,000\,000\,000 + 3\,000\,000\,000 = 6\,000\,000\,000?$$

Surely you've never actually counted six billion of anything!

Maybe $3 + 3 = 6$ is just "intuitively obvious", and we shouldn't talk about it anymore.

What is a Proof?

- **Jury Trial:** Truth is ascertained by twelve people selected at random.
- **Word of God:** Truth is ascertained by communication with God, perhaps via a third party.
- **Word of ~~Bostan~~ Boss:** Truth is ascertained from someone with whom it is unwise to disagree.
- **Experimental Science:** The truth is guessed and the hypothesis is confirmed or refuted by experiments.
- **Sampling:** The truth is obtained by statistical analysis of many bits of evidence. For example, public opinion is obtained by polling only a representative sample.
- **Inner Conviction/Mysticism:** "My program is perfect. This is true."
- **I don't see why not**...: Claim something is true and then shift the burden of proof to anyone who disagrees with you.

Axiomatic method

Definition

A formal **proof** of a proposition is a chain of logical deductions leading to the proposition from a base set of axioms.

A standard procedure for establishing truth in mathematics first used by Euclid, who started with five geometry assumptions, which were drawn from direct experience (reality).

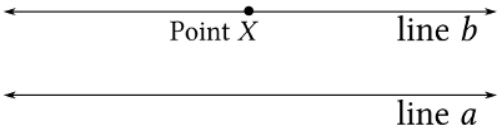
Propositions like these that are simply accepted as true are called **axioms**.

Starting from these axioms, Euclid established the truth of many additional propositions by providing "proofs." A proof is a sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in question.

Euclid's axiom-and-proof approach is called the **axiomatic method**, and it is the foundation for mathematics today.

Axiom (5th Postulate)

Given a line a and a point X not on line a, there is exactly one line through X which is parallel with a.



Eukleides of Alexandria, 325–287 BC

Axioms

Definition

An **axiom** is a proposition that is **assumed** to be always true.

Axiom

If $a = b$, and $b = c$, then $a = c$.

Axiom

$\forall x \in \mathbb{R}, \quad x + 0 = x.$

Axiom

$\forall x, y, z \in \mathbb{R}, \quad (x + y) \cdot z = x \cdot z + y \cdot z.$

Axiom?

The capital of Republic Moldova is Chișinău.

Axiom. Euclidean geometry

Given a line a and a point X not on line a, there is **exactly one** line through X which is parallel with a.

Axiom. Spherical geometry

Given a line a and a point X not on line a, there is **no line** through X which is parallel with a.

Axiom. Hyperbolic geometry

Given a line a and a point X not on line a, there are **infinitely many lines** through X which are parallel with a.

Zermelo-Fraenkel with Choice Axioms

Essentially all mathematics can be derived from just a few axioms called ZFC coupled together with a several logical principles.

ZFC stands for Zermelo-Fraenkel with Choice.

This does not completely settle the question of truth in mathematics, but it greatly focuses the issue.

You can still deny a mathematical theorem, but only if you reject one of the elementary ZFC axioms or find a logical error in the proof.

The ZFC Axioms are the axioms of Zermelo-Fraenkel set theory with some technicalities omitted. The variables denote distinct sets.

Essentially all of mathematics can be derived from these axioms together with a few principles of logic.

ZFC Axioms

Extensionality.

Two sets are equal if they have the same members:

$$(\forall z.\ z \in x \text{ IFF } z \in y) \text{ IMPLIES } x = y.$$

Pairing.

For any two sets x and y, there is a set $\{x, y\}$, with x and y as its only elements:

$$\forall x, y.\ \exists u.\ \forall z.\ [z \in u \text{ IFF } (z = x \text{ OR } z = y)].$$

Union.

The union u of a collection z of sets is also a set:

$$\forall z.\ \exists u.\ \forall x.\ (\exists y.\ x \in y \text{ AND } y \in z) \text{ IFF } x \in u.$$

Infinity.

There is an infinite set. Specifically, there is a nonempty set, x, such that for any set $y \in x$, the set $\{y\}$ is also a member of x.

Subset.

Given any set, x ,and any definable property of sets, there is a set containing precisely those elements $y \in x$ that have the property.

$$\forall x.\ \exists z.\ \forall y.\ y \in z \text{ IFF } [y \in x \text{ AND } \phi(y)],$$

where $\phi(y)$ is any assertion about y definable in set theory.

Power set.

All the subsets of a set form another set:

$$\forall x.\ \exists p.\ \forall u.\ u \subseteq x \text{ IFF } u \in p.$$

Foundation.

There can not be an infinite sequence

$$\cdots \in x_n \in \cdots \in x_1 \in x_0$$

of sets each of which is a member of the previous one. This is equivalent to saying every nonempty set has a "member-minimal" element. Namely, define

$$\text{member-minimal}(m, x) = [m \in x \text{ AND } \forall y \in x. y \notin m].$$

Then the fountation axiom is

$$\forall x.\ x \neq \emptyset \text{ IMPLIES } \exists m.\ \text{member-minimal}(m, x).$$

Choice.

Given a set, s, whose members are nonempty sets no two of which have any element in common, then there is a set, c, consisting of exactly one element from each set in s.

$$\forall s.\ [\forall x \in s.\ x \neq \emptyset \text{ AND } \forall x, y \in s.\ x \neq y \text{ IMPLIES } x \cap y = \emptyset.]$$
$$\text{IMPLIES}$$
$$\exists c.\ \forall x \in s.\ \exists!\ z \in c \cap x.$$

Proving theorems in ZFC is a little like writing programs in byte code instead of a full-fledged programming language.

For example, a formal proof in ZFC that $2 + 2 = 4$ requires more than 20 000 steps!

Consistency and Completeness

Definition

A set of axioms is **consistent** if no proposition can be proven to be both true and false.

This is an absolute must.

One would not want to spend years proving a proposition true only to have it proven false the next day! Proofs would become meaningless if axioms were inconsistent.

Definition

A set of axioms is **complete** if it can be used to prove or disprove every proposition.

Completeness is an attractive property; we would like to believe that any proposition could be proven or disproven with sufficient work and insight.

Surprisingly, making a complete, consistent set of axioms is not easy.

Consistency and Completeness

Definition

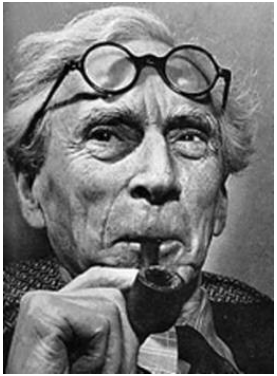
A set of axioms is **consistent** if no proposition can be proven to be both true and false.

Definition

A set of axioms is **complete** if it can be used to prove or disprove every proposition.

Surprisingly, making both a complete and consistent set of axioms is not easy.

Modern foundation (Russel and Whitehead)



Bertrand Russel, 1872-1970

Alfred Whitehead, 1861-1947

Bertrand Russell and Alfred Whitehead tried during their entire careers to find such axioms for basic arithmetic and failed.

Modern foundation (Kurt Godel)

Kurt Godel, 1906-1978

In his doctoral dissertation Godel showed:

- The **completeness** of predicate logic, namely that **all** true propositions that might arise in predicate logic (1st order logic) can be proven.
- The **consistency** of predicate logic, namely that **only** true propositions from predicate logic can be proven.

Kurt Godel and Hilbert 2nd Problem

After Godel was done with completeness and consistency of predicate logic, he tackled the Hilbert 2nd problem: completeness and consistency of formal arithmetic axioms (foundation of mathematics).

Godel took the axioms of Peano. Some of them:

1. 0 is a natural number;
2. Every natural number n has a successor that is also a natural number;
3. No natural number has 0 as its successor;
4. Different natural numbers have different successors;
5. If for some property P, P holds for 0, and if P holds for a natural number n, implies P also holds for n's successor, then P holds for all natural numbers

Kurt Godel and Hilbert 2nd Problem

In his *Habilitationsschrift* Kurt Godel proved:

- The incompleteness of formal arithmetic;
- If formal arithmetic is consistent, then that consistency cannot be proven within the formal arithmetic itself.

Moreover he showed that no set of axioms can be both consistent and complete!

Godel Theorem Idea

Any set of consistent axioms (an absolute must) can not be complete; there will be true statements that can not be proven.

For example, it might be that Goldbach's conjecture is true, but there is no proof!

Decidability Problem

Is there an algorithm that determines of any given statement whether it or its negation is provable?

Lecture 2 Summary

- Cardinality of power set;
- Uncountable sets;
- Uncountability of real numbers;
- Mathematical Logic; Proposition.
- What is a proof?
- Axioms; ZFC Axioms;
- Consistency and Completeness of Axioms.

Next lecture will start with a quiz!

Homework 1 is due September 21 at 18:00!

Joke

A physicist, a biologist, and a mathematician are sitting on a bench across from a house.

They watch as two people go into the house, and then a little later, three people walk out.

The physicist says, "The initial measurement was incorrect."

The biologist says, "They must have reproduced."

And the mathematician says,

"If exactly one person enters that house, it will be empty."