Introduction: Mathematical Paradoxes

Intuitive approach. Until recently, till the end of the 19th century, mathematical theories used to be built in an intuitive or axiomatic way.

The historical development of mathematics has shown that **it is not sufficient to base theories on an intuitive understanding** of their notions only.

This fact became especially obvious in **set theory**.

The basic concept of a **set** is certainly taken from reality, for there we come across many examples of various sets, **all of which are finite.**

But in mathematics it is also necessary to consider **infinite sets**, such as the set of all integers, the set of all rational numbers, the set of all segments, the set of all triangles.

Intuitively, by a set, we mean any collection of objects- for example, the set of all even integers or the set of all students in a class.

The objects that make up a set are called **its members (elements)**.

Sets may themselves **be members of sets** for example, the set of all sets of integers has sets as its members.

Most sets are **not members of themselves**.

For example the set of all students is **not a member of itself**, because the set of all students is not a student.

However, there may be sets **that do belong to themselves**.

For example the set of all sets.

A following simple reasoning indicates that **it is necessary to impose some limitations on the concept of a set**.

Russell Paradox, 1902: Consider the **set A of all those sets X such that X is not a member of X.**

Clearly, **A is a member of A if and only if A is not a member of A.**

So, if **A is a member of A, then A is also not a member of A;** and

if **A is not a member of A, then A is a member of A.**

In any case, **A is a member of A and A is not a member of A.**

CONTRADICTION

Russell solution: every object must have a definite non-negative integer as its **type**. An expression **x is a member of the set y** is **meaningful** if and only if the type of y is one greater than the type of x.

Theory of types says that it is meaningless to say that a set belongs to itself, there can not be such set A, as stated in the Russell paradox.

Development: by Whitehead and Russell in years 1910 - 1913. It is successful, but difficult in practice and has certain other drawbacks as well.

LOGICAL PARADOXES or ANTINOMIES

Logical Paradoxes (antinomies) are the paradoxes concerning the **notion of a set**.

Axiomatic Set Theory is a general solution to Logical Paradoxes.

It is one of the most important fields of Modern Mathematics or more specifically **Mathematical Logic and Foundations of Mathematics**.

Zermello, 1908 - first paradoxes free **axiomatic set theory.**

Two of the other most known **logical paradoxes** are Cantor and Burali-Forti antinomies. They were stated at the end of 19th century.

Cantor paradox involves the theory of **cardinal numbers**.

Burali-Forti paradox is the analogue to Cantor's in the theory of **ordinal numbers**.

Cardinal number: $cardX = cardY$ or X and Y are **equinumerous** if and only if there is one-to-one correspondence that maps X and Y).

$cardX \leq cardY$ means that
X is equinumerous with a subset of Y.

$cardX < cardY$ means that
$cardX \leq cardY$ and $cardX \neq cardY$.

Cantor Theorem: For any set X,

$$cardX < card\mathcal{P}(X).$$

Schröder- Berstein Theorem: For any sets X and Y,

If $cardX \leq cardY$ and $cardY \leq cardX$, then $cardX = cardY$.

Ordinal numbers are the numbers assigned to sets in a similar way as cardinal numbers but they deal with **ordered** sets.

Cantor Paradox, 1899: Let C be the **universal set** - that is, the set of all sets. Now, $\mathcal{P}(C)$ is a subset of C, so it follows easily that

$$card\mathcal{P}(C) \leq cardC.$$

On the other hand, by Cantor theorem, $cardC < card\mathcal{P}(C) \leq card\mathcal{P}(C)$, so also

$$cardC \leq card\mathcal{P}(C)$$

and by Schröder- Berstein theorem we have that

$$card\mathcal{P}(C) = cardC,$$

what **contradicts** Cantor Theorem: $cardC < card\mathcal{P}(C)$.

Solution: Universal set does not exist.

Burali-Forti Paradox, 1897 Given any ordinal number, there is a still larger ordinal number. But the ordinal number determined by the set of all ordinal numbers is the largest ordinal number.

Solution: set of all ordinal numbers do not exist.

Semantic Paradoxes another solution: reject the assumption that for every property $P(x)$, there exists a corresponding set of all objects x that satisfy $P(x)$.

Russell's Paradox then simply proves that there is no set A of all sets that do not belong to themselves.

Cantor Paradox shows that there is no universal set.

Burali-Forti Paradox shows that there is no set that contains all ordinal numbers.

A more radical interpretation of the paradoxes has been advocated by Brower and his **intuitionist** school.

Intuitionists refuse to accept the universality of certain basic logical laws, such as the law of **excluded middle**: A or not A.

For intuitionists excluded middle law is true for finite sets, but it is invalid to extend it to all sets.

The intuitionists' concept of infinite set differs from that of classical mathematicians.

Infinite set for the intuitionists is something which is constantly in a state of formation.

Example: set of positive integers is infinite because to any given finite set of positive integers it is always possible to add one more positive integer.

For intuitionists The notion of the set of all subsets of the set of all positive integers is not regarded meaningful.

Intuitionists' mathematics is different from that of most mathematicians in their research.

The basic difference lies in the interpretation of the word **exists**.

Example: let $P(n)$ be a statement in the arithmetic of positive integers. For the mathematician the sentence **the exists n, such that P(n)** is true if it can be **deduced** (proved) from the axioms of arithmetic by means of classical logic.

In classical mathematics proving **existence** of x does not mean that one is able to indicate a method of **construction** of a positive integer n such that $P(n)$ holds.

For the intuitionist the sentence **the exists n, such that P(n)** is true only if he is able to **construct** a number n **such that** $P(n)$ **is true.**

In general in the intuitionists' universe we are justified in asserting the existence of an object having a certain property only if we know an effective method for constructing or finding such an object.

In intuitionist' mathematics the paradoxes are, in this case, not derivable (or even meaningful).

Intuitionism because of its **constructive** flavor, has found a lot of applications in **computer science**, for example theory of programs correctness.

Intuitionists logic reflects intuitionists ideas in a form formalized deductive system.

The axiomatic theories solved some but not all problems.

Consistent set of axioms does not prevent the occurrence of another kind of paradoxes, called **Semantic Paradoxes**.

SEMANTIC PARADOXES

Berry Paradox, 1906: Let

> **A denote the set of all positive integers which can be defined in the English language by means of a sentence containing at most 1000 letters.**

The set **A** is **finite** since the set of all sentences containing at most 1000 letters is finite.
Hence, **there exist positive integer which do not belong to A.**

The sentence:

n is the least positive integer which cannot be defined by means of a sentence of the English language containing at most 1000 letters

contains less than 1000 letters and **defines** a positive integer n.

Therefore n **belongs to A.** But n **does not belong to A** by the definition of n.

CONTRADICTION!

Berry Paradox Analysis: The paradox resulted entirely from the fact that **we did not say precisely** what notions and sentences **belong to the arithmetic** and what notions and sentences **concern the arithmetic**, examined as a fix and closed deductive system.

And on the top of it we also **mixed the natural language with mathematical language.**

Solution: (Tarski) we must always **distinguish the language of the theory** we talk about (arithmetic) and the **language which talks about the theory**, called **a metalanguage**.

In general we must distinguish a **theory** from the **meta-theory**.

The Liar Paradox (Greek philosopher Eubulides of Miletus, 400 BC)

A man says: **I am lying.**

If **he is lying**, then what he says is true, and so **he is not lying**.

If **he is not lying**, then what he says is not true, and so **he is lying**.

In any case, **he is lying and he is not lying.**

CONTRADICTION

Löb Paradox (1955)

Let **A be any sentence**. Let B be a sentence: **If this sentence is true, then A.** So, B asserts: **If B is true then A.**

Now consider the following argument: **Assume B is true.** Then, by B, since B is true, **A is true**.

This argument shows that, **if B is true, then A**. But this is exactly what B asserts. Hence, B is true. Therefore, by B, since B is true, A is true. **Thus every sentence is true**.

CONTRADICTION

TARSKI solution: these paradoxes arise because the concepts of " **I am true**", **this sentence is true**, " **I am lying**" should not occur in the **language** (**theory**). It belong to a **metalanguage** (**meta-theory**).

The Liar Paradox is a corrected version of a following paradox stated in antiquity by a Cretan philosopher Epimenides.

Cretan " Paradox" (The Cretan philosopher Epimenides paradox, 600 BC)

Epimenides, a Cretan said: All Cretans are liars. If what he said is true, then, since Epimenides is a Cretan, **it must be false**. Hence, what he said is false. Thus, **there must be some Cretan who is not a liar**.

Note that the conclusion that there must be some Cretan who is not a liar is not logically impossible, so we do not have a genuine paradox.

General Remarks

First task of building mathematical logic, foundations of mathematics or computer science is to define their **symbolic language**. This is called a **syntax.**

Second task is to extend the syntax to include **a notion of a proof.** It allows us to find out what can and cannot be proved if certain axioms and rules of inference are assumed. This part of syntax is called a **proof theory.**

Third task is to define what does it mean that **formulas of our language are true**, i.e. to define a **semantics for the language**.

For example the notion of truth for classical and intuitionistic approaches are different; classical and intuitionistic semantics are different.

Fourth task is to investigate the relationship between **proof theory** (part of the syntax) and **semantics**.

This relationship is being established by proving fundamental theorems:
Soundness, Completeness, Consistency.

Role of Classical and Non-classical Logics in Computer Science

Classical Logic The use of classical logic on computer science is known, undisputable, and well established. The existence of PROLOG and Logic Programming as a separate field of computer science is the best example of it.

Intuitionistic Logic in the form of Martin-Löf's theory of types (1982), provides a complete theory of the process of program specification, construction , and verification. A similar theme has been developed by Constable (1971) and Beeson (1983).

Modal Logic: In 1918, an American philosopher, C.I. Lewis proposed yet another interpretation of lasting consequences of the logical implication. In an attempt to avoid, what some felt, the paradoxes of implication (**a false sentence implies any sentence**) he created a **modal logic**.

The idea was to distinguish two sorts of truth: **necessary truth** and a mere **possible (contingent) truth**.

A possibly true sentence is one which, though true, could be false.

Modal Logic in Computer Science is used as as a tool for analyzing such notions as **knowledge, belief, tense**.

Modal logic has been also employed in form of *Dynamic logic* (Harel 1979) to facilitate the statement and proof of properties of programs.

Temporal Logics were created for the specification and verification of concurrent programs (Harel, Parikh, 1979, 1983), for a specification of hardware circuits Halpern, Manna and Maszkowski, (1983), to specify and clarify the concept of causation and its role in commonsense reasoning (Shoham, 1988).

Fuzzy logic, Many valued logics were created and developed to reasoning with incomplete information.

The development of different logics and the applications of logics to different areas of computer science or even artificial intelligence only is beyond the scope of class.

In class we will define and study the basic properties of some of the most standard non-classical logics: **many valued, intuitionistic, and modal**.

Computer Science Puzzles
Reasoning in Distributed Systems

Grey, 1978, Halpern, Moses, 1984: Two divisions of an army are camped on two hilltops overlooking a common valley. In the valley awaits the enemy.

If both divisions attack the enemy simultaneously they will win the battle.

If only one division attacks it will be defeated.

The divisions do not initially have plans for launching an attack on the enemy, and the commanding general of the first division wishes to coordinate a simultaneous attack (at some time the next day).

Neither general will decide to attack unless he is sure that the other will attack with him.

The generals can only communicate by means of a messenger.

Normally, it takes a messenger one hour to get from one encampment to the other.

However, it is possible that he will get lost in the dark or, worst yet, be captured by the enemy.

Fortunately, on this particular night, everything goes smoothly.

Question: How long will it take them to coordinate an attack?

Suppose the messenger sent by General A makes it to General B with a message saying *Attack at dawn.*

Will B attack? No, since A does not know B got the message, and thus may not attack.

General B sends the messenger back with an acknowledgment. Suppose the messenger makes it.

Will A attack? No, because now A is worried that B does not know A got the message, so that B thinks A may think that B did not get the original message, and thus not attack.

General A sends the messenger back with an acknowledgment.

This is not enough. No amount of acknowledgments sent back and forth will ever guarantee agreement. Even in a case that the messenger succeeds in delivering the message every time. All that is required in this (informal) reasoning is the **possibility** that the messenger doesn't succeed.

Solution: Halpern and Moses (1985) created a **Propositional Modal logic with m agents.** They proved this logic to be essentially a multi-agent version of the modal logic S5.

They proved that common knowledge (formally defined!) not attainable in systems where communication is not guaranteed

Also it is also not attainable in systems where communication *is guaranteed*, as long as there is some uncertainty in message delivery time.

In distributed systems where communication is not guaranteed common knowledge is not attainable.

But we often do reach agreement!

They proved that common knowledge (as formally defined) is attainable in such models of reality where we assume, for example, events can be guaranteed to happen simultaneously.

Moreover , there are some variants of the definition of common knowledge that are attainable under more reasonable assumptions.

So, we can prove that in fact we often do reach agreement!

Reasoning in Artificial Intelligence

Flexibility of reasoning is one of the key property of intelligence.

Commonsense inference is defeasible in its nature; we are all capable of drawing conclusions, acting on them, and then retracting them if necessary in the face of new evidence.

If Computer programs are to act intelligently, they will need to be similarly flexible.

Goal: development of formal systems that describe commonsense flexibility.

Flexible Reasoning Examples

Reiter, 1987 Consider a statement *Birds fly*. Tweety, we are told, is a bird. From this, and the fact that birds fly, we conclude that Tweety can fly.

This is defeasible: Tweety may be an ostrich, a penguin, a bird with a broken wing, or a bird whose feet have been set in concrete.

Non-monotonic Inference: on learning a new fact (that Tweety has a broken wing), we are forced to retract our conclusion (that he could fly).

Non-monotonic Logic is a logic **in which the introduction of a new information (axioms) can invalidate old theorems.**

Default reasoning (logics) means **drawing of plausible inferences from less-then- conclusive evidence in the absence of information to the contrary.**

Non-monotonic reasoning is an **example of the default reasoning**

Moore, 1983 Consider my reason for believing that I do not have an older brother. It is surely not that one of my parents once casually remarked, *You know, you don't have any older brothers*, nor have I pieced it together by carefully sifting other evidence.

I simply believe that if I did have an older brother I would know about it;

therefore, since I don't know of any older brothers of mine, I must not have any.

"The brother" reasoning is not a form of default reasoning nor non-monotonic. It is reasoning about one's own knowledge or belief. Hence it is called an **auto-epistemic reasoning**.

Auto-epistemic reasoning models the reasoning of an ideally rational agent reflecting upon his beliefs or knowledge.

Auto- Logics ate logics which **describe the reasoning of an ideally rational agent reflecting upon his beliefs.**

Missionaries and Cannibals Revisited

McCarthy, 1985 revisits the problem: **Three missionaries and three cannibals come to the river. A rowboat that seats two is available. If the cannibals ever outnumber the missionaries on either bank of the river, the missionaries will be eaten. How shall they cross the river?**

Traditionally the puzzler is expected to devise a strategy of rowing the boat back and forth that gets them all across and avoids the disaster.

Traditional Solution: A state is a triple comprising the number of missionaries, cannibals and boats on the starting bank of the river.

The initial state is 331, the desired state is 000,

A solution is given by the sequence: 331, 220, 321, 300,311, 110, 221, 020, 031, 010, 021, 000.

Imagine now giving someone a problem, and after he puzzles for a while, he suggests going upstream half a mile and crossing on a bridge.

What a bridge? you say. *No bridge is mentioned in the statement of the problem.*

He replies: *Well, they don't say the isn't a bridge*.

So you modify the problem to **exclude the bridges and pose it again.**

He proposes a helicopter, and after you exclude that, **he proposes a winged horse or that the others hang onto the outside of the boat while two row.**

Finally, you tell him the solution.

He attacks your solution on the grounds **that the boat might have a leak or lack oars.**

After you rectify that omission from the statement of the problem, he suggests that **a see monster may swim up the river and may swallow the boat.**

Finally, you must **look for a mode of reasoning that will settle his hash once and for all.**

McCarthy proposes **circumscription** as a technique for solving his puzzle.

He argues that it is a part of common knowledge that **a boat can be used to cross the river unless there is something with it or something else prevents using it**.

If our facts do not require that there be something that prevents crossing the river, **circumscription** will generate the conjecture that there isn't.

Lifschits has shown in 1987 that in some special cases the circumscription is equivalent to a first order sentence. item[In those cases], we can go back to our secure and well known classical logic.