Number Theory

Sudip Sinha

2019-04-05

Math Circle @ QTM

Outline

1 Introduction and Logic 3

Section 1

Introduction and Logic

Introduction and motivation

1. What is number theory?
2. Why do we study number theory?
3. Why do we want to *prove* ideas?
4. More importantly, what constitutes a *proof*?
5. Inductive vs deductive reasoning.

Inductive reasoning

- ▷ **Inductive reasoning** derives general propositions from specific examples.
- ▷ **Caution**: *We can never be sure, our conclusion(s) can be wrong!* ☹
- ▷ *Example* 1:

  1. We throw lots of things, very often.
  2. In all our experiments, the things fell down and not up.
  3. So we conclude that likely, things always fall down.

  How we may be wrong:

  1. An iron nail under a big magnet moves up (given that it is sufficiently close).
  2. A helium balloon goes up.

Inductive reasoning: problems

- *Example* 2: You ask your parent for a candy and (s)he buys it for you. You ask for a fancy shoe, and (s)he buys it. Now you ask for a Lamborghini $\cdots$.

- *Example* 3 (*Black swan*): In the 16th century, it was believed (in Europe) that swans are always white. But in 1697, Dutch explorers led by Willem de Vlamingh became the first Europeans to see black swans, in Western Australia.

- *Example* 4: $\frac{1}{1} = 1, \frac{2}{2} = 1, \frac{3}{3} = 1, \cdots$; so clearly $\frac{n}{n} = 1$ for every integer n.

- *Example* 5: Illusions, e.g. drawings by *M. C. Escher*.

Problems with inductive reasoning: Illusion #1

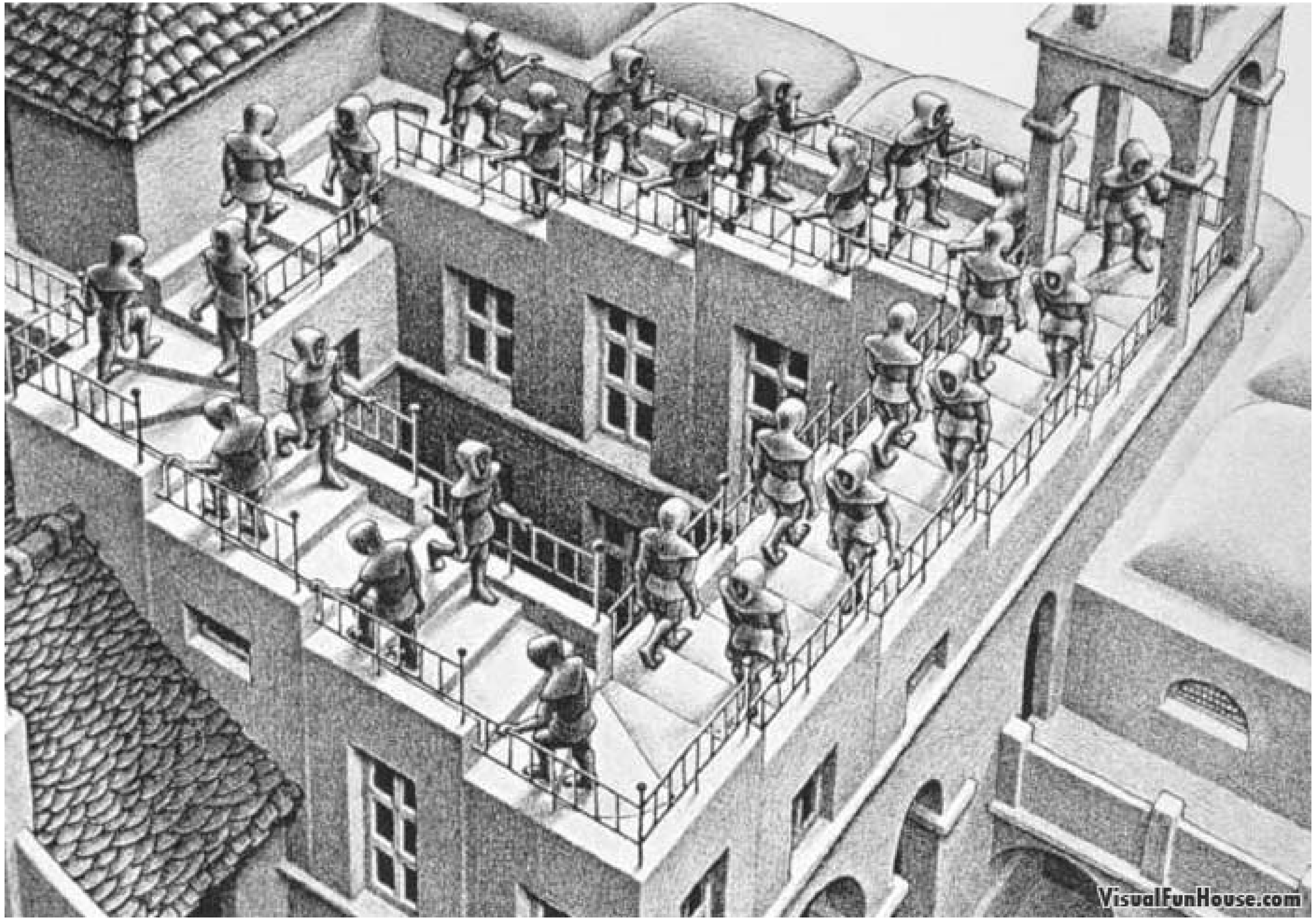

Figure 1 Ascending and Descending, M. C. Escher

Problems with inductive reasoning: Illusion #2

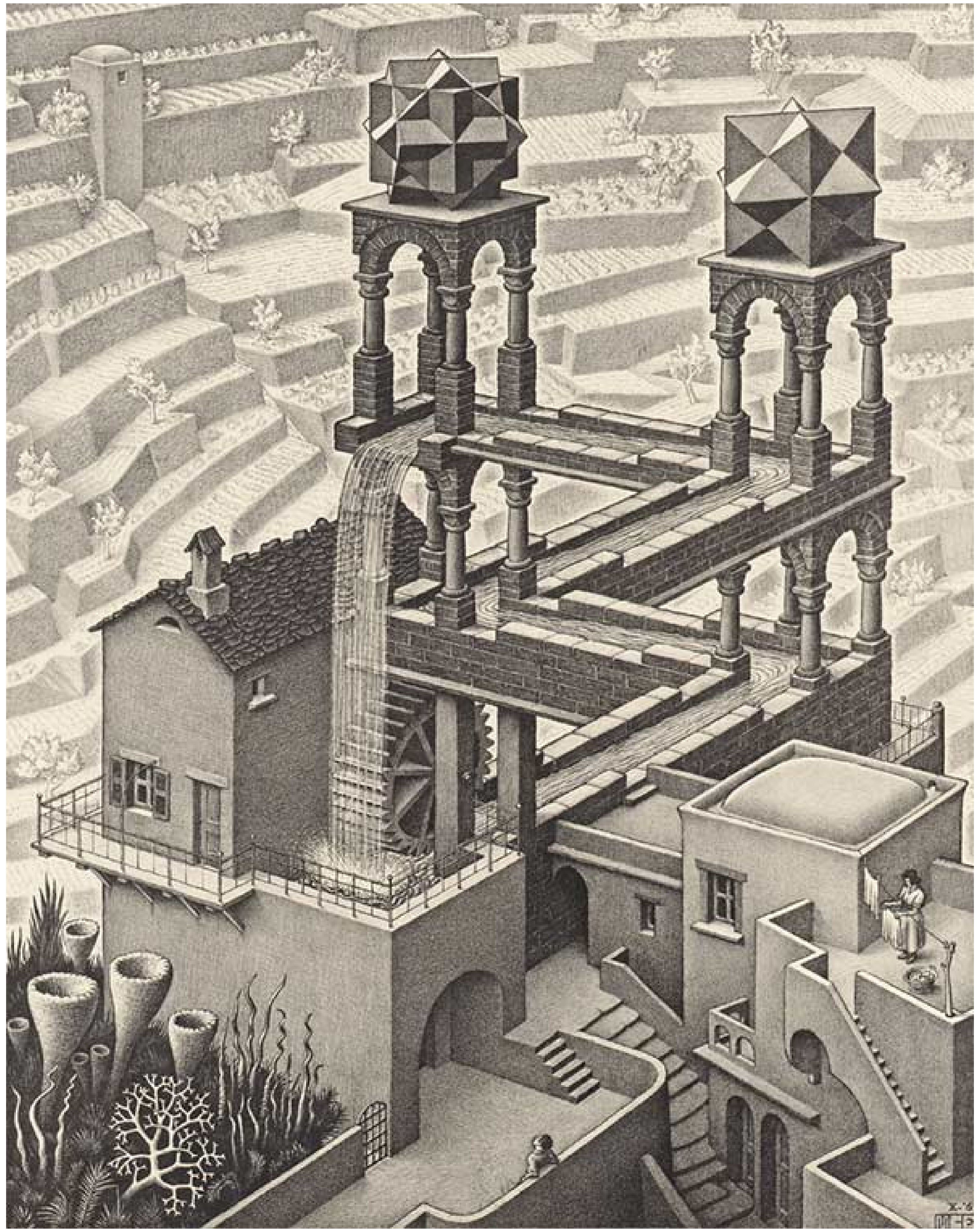

Figure 2 Waterfall, M. C. Escher

Deductive reasoning

- ▷ **Deductive reasoning** is deriving a logically certain conclusion from one or more premises.
- ▷ We do *NOT* question the premises. But *if the premises are correct, then all conclusions are correct.* ☺
- ▷ *Example*: Question: Do $\mathbf{Q_1}$ and $\mathbf{Q_2}$ *imply* $\mathbf{Q_3}$?
  - ∘ ($\mathbf{Q_1}$) All men are mortal. (First premise)
  - ∘ ($\mathbf{Q_2}$) Socrates is a man. (Second premise)
  - ∘ ($\mathbf{Q_3}$) Therefore, Socrates is mortal. (Conclusion)
- ▷ *Example*: Question: Does $\mathbf{P_1}$ and $\mathbf{P_2}$ *imply* $\mathbf{P_3}$?
  - ∘ ($\mathbf{P_1}$) Borogoves are mimsy whenever it is brillig.
  - ∘ ($\mathbf{P_2}$) It is not brillig, and this thing is a borogove.
  - ∘ ($\mathbf{P_3}$) Hence this thing is mimsy.
- ▷ We do not *need* an inherent *meaning* of the terms.

Inductive vs deductive reasoning

Criteria	Inductive reasoning	Deductive reasoning
Basis	evidence	logic
Questions	everything (arguments and premises)	only the arguments, not premises
Direction	*bottom-up*	*top-down*
Natural to humans?	yes	no
Requires *meanings* of terms?	yes	no
Applicability	good in practice	good for theory
Examples	science, statistics and machine learning	logic, mathematics

Logic

- *Logic* is a *language* to formalize deductive reasoning.
- Logic comprises of the following elements.
  - propositions
  - connectives (not, and, or, implies, iff)
  - quantifications (for all, there exists)
  - values (true, false)
  - a way to assign propositions to a value
- **Important**: The propositions in the following section are not necessarily true. Please be mindful.

Logic: elementary *propositions*

- Elementary *propositions*, represented by P, Q, etc, are statements saying something.
- Examples:
  - $P_1 \equiv n$ is an integer
  - $P_2 \equiv n$ is *not* an integer
  - $P_3 \equiv 2n$ is even
  - $P_4 \equiv n = \frac{1}{2}$
  - $Q_1 \equiv$ Socrates is a man
  - $Q_2 \equiv$ Socrates is smart

Logic: compound *propositions*

- Compound *propositions* are elementary propositions connected by connectives.

- *Connectives*:
  - not ($\neg$, or $\sim$): $\neg P$ is called the negation of P.
  - and ($\wedge$)
  - or ($\vee$)
  - implies ($\rightarrow$, or $\Longrightarrow$)
  - iff ($\leftrightarrow$, or $\Longleftrightarrow$, or $\equiv$)

- Examples:

1. $(\neg P_1) \equiv$ not (n is an integer) $\equiv$ n is *not* an integer
2. $(P_1 \vee P_2) \equiv$ (n is an integer) or (n is *not* an integer)
3. $(Q_1 \wedge Q_2) \equiv$ (Socrates is a man and) and (Socrates is smart)
4. $((\neg P_1) \leftrightarrow P_2) \equiv$ not (n is an integer) if and only if (n is *not* an integer)
5. $(P_1 \rightarrow P_3) \equiv$ (n is an integer) implies ($2n$ is even)
6. $(P_4 \rightarrow P_3) \equiv$ ($n = \frac{1}{2}$) implies ($2n$ is even)

Truth tables

- Question: How do we find the value of a compound propositions?
- Exercise: Fill up the table. Think carefully about what the ‘?’s should be.

P	Q	$(\neg P)$	$(P \wedge Q)$	$(P \vee Q)$	$(P \rightarrow Q)$	$(Q \rightarrow P)$	$((P \rightarrow Q) \wedge (Q \rightarrow P))$	$(P \leftrightarrow Q)$
T	T							
T	F					?		
F	T				?			
F	F				?	?		

Truth tables

P	Q	$(\neg P)$	$(P \wedge Q)$	$(P \vee Q)$	$(P \rightarrow Q)$	$(Q \rightarrow P)$	$((P \rightarrow Q) \wedge (Q \rightarrow P))$	$(P \leftrightarrow Q)$
T	T	F	T	T	T	T	T	T
T	F	F	F	T	F	T	F	F
F	T	T	F	T	T	F	F	F
F	F	T	F	F	T	T	T	T

- ▷ Such tables are called truth tables. They evaluate the expression for all values of the elementary propositions.
- ▷ Two propositions are equivalent if their truth table values are the same. Can you find if any of the above expressions are equivalent?

Thinking *logic*ally about mathematical statements

- Every mathematical statement can be broken down into their constituent propositions.
- Example

  1. Original statement: if the product of two integers is even, then each of them is even.
  2. Analysis: if the product of two integers n and m is even, then m is even and n is even.
  3. Writing this down logically.
     - $P_1 \equiv$ the product of two integers n and m is even
     - $P_2 \equiv m$ is even
     - $P_3 \equiv n$ is even
     - Statement $\equiv (P_1 \rightarrow (P_2 \land P_3))$
  4. Question: is the above statement true or false? How can you prove it?
  5. Note: The part before the implication is called the antecedent, and the part after is called the consequent. In this example, P_1 is the antecedent and $(P_2 \land P_3)$ is the consequent.

- Exercise

Quantifiers

There are two quantifiers.

- ▷ Universal quantifier a.k.a. for every ($\forall$).
  Example 1: Every man has a head.
  Example 2: Every natural number is even.

- ▷ Existential quantifier a.k.a. there exists ($\exists$).
  Example 1: There is a man who can survive without breathing for an hour.
  Example 2: There exists a natural number which is the sum of its factors (except itself).

Exercise: Analyze the following statements logically.

1. Every odd number has a odd factor.

2. (Fermat's last theorem) No three positive integers a, b, and c satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2.

Tautologies

Let P, Q, and R be propositions. Verify the following using truth tables.

- ▷ (idempotence) $(P \leftrightarrow (P \wedge P))$, and $(P \leftrightarrow (P \vee P))$.
- ▷ (commutativity) $((P \wedge Q) \leftrightarrow (Q \wedge P))$, and $((P \vee Q) \leftrightarrow (Q \vee P))$.
- ▷ (associativity) $(((P \wedge Q) \wedge R) \leftrightarrow (P \wedge (Q \wedge R)))$, and $(((P \vee Q) \vee R) \leftrightarrow (P \vee (Q \vee R)))$.
- ▷ (distributivity) $((P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R)))$, and $((P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R)))$.
- ▷ (identity) $((P \wedge T) \leftrightarrow P)$, $((P \vee F) \leftrightarrow P)$; $((P \wedge F) \leftrightarrow F)$, $((P \vee T) \leftrightarrow T)$.
- ▷ (involution) $((\neg(\neg P)) \leftrightarrow P)$.
- ▷ (implication) $((P \rightarrow Q) \leftrightarrow ((\neg P) \vee Q))$.
- ▷ (de Morgan's laws) $((\neg(P \wedge Q)) \leftrightarrow ((\neg P) \vee (\neg Q)))$, and $((\neg(P \vee Q)) \leftrightarrow ((\neg P) \wedge (\neg Q)))$.
- ▷ (contrapositive) $((P \rightarrow Q) \leftrightarrow ((\neg Q) \rightarrow (\neg P)))$.

The *converse* of $(P \rightarrow Q)$ is $(Q \rightarrow P)$, and they have no relation to each other.
Exercise: Find an example for which the proposition is true but its converse is not.

Proof methods

- ▷ Direct proof of $P \rightarrow Q$: Start with P and logically arrive at Q.
- ▷ Proof by contrapositive of $P \rightarrow Q$: Direct proof of $((\neg P) \rightarrow (\neg Q))$.
- ▷ Proof by contradition of a general proposition P: Consider that P is false. Logically show that this leads to an absurdity.
- ▷ Proof by induction (more on this later).
- ▷ Proof by construction.
- ▷ Proof by exhaustion.
- ▷ Probabilistic proof
- ▷ Combinatorial proof.
- ▷ Nonconstructive proof.

Guidelines for proofs

Note: Proving a proposition is an art. There is no algorithms, only rules of thumb.

- To prove an existential proposition true, we need to find just one instance (*example*) for which the proposition is true.
- To prove an universal proposition false, we need to find just one instance (*counterexample*) for which the statement is false.
- It is sometimes easier to prove the contrapositive of a proposition.
- To prove a uniqueness proposition, proofs by contradiction is usually more convenient.
- Sometimes it is pragmatic to break down a proof into two or more cases.

Appendix

Laplace principle and equivalence to LDP

Definition (Laplace principle) (X_n) is said to satisfy the Laplace principle on $\mathcal{X}$ with rate function I if for all bounded continuous functions h, we have

$$\lim \frac{1}{n} \log \mathbb{E} \exp(-nh(X_n)) = \inf_{\mathcal{X}} (h + I)$$

Theorem (X_n) satisfies LP on $\mathcal{X}$ with rate function I if and only if (X_n) satisfies LDP on $\mathcal{X}$ with the same rate function I.

Some important results

- Uniqueness of the rate function.
- Continuity principle.
- Superexponential approximation preserves Laplace principle.

Thank you!

Bibliography