Logic and Proofs

(A brief summary)

Why Study Logic:

- To learn to prove claims/statements rigorously
- To be able to judge better the soundness and consistency of (others') arguments
- To gain the foundations of how to program (teach) computers to reason. That is called *automated reasoning*, which is part of Artificial intelligence (AI).

Propositions:

- A *proposition* is a declarative statement (sentence) that is true or false. For example, "Mars is a planet" is a proposition that is true, and "Jupiter is a star" is a proposition that is false. Questions, commands and exclamations are examples of sentences that are not propositions.
- *Truth values*: They are the values "true" (denoted *T*) and "false" (denoted *F*).
- A proposition that conveys a single fact is called a *simple proposition*.
- Simple propositions can be combined and/or negated, using so-called *logical connectives*, to form more elaborate propositions called *compound propositions*.
- *Logical connectives*: They are the logical operations "and", "or", and "not". The first two are binary operations, that is, they take two operands where each operand is a proposition. The "not" is a unary operation in that it takes a single operand.
- Examples of compound propositions:
  - Mars is a planet and Jupiter is a star
  - Mars is a planet or Jupiter is a star
  - not (Jupiter is a star). In plain English, this statement means "Jupiter is not a star".
  - Mars is a planet and (Jupiter is a star or not(Pluto is a comet))
- Notations:
  - The operation "and" is denoted $\wedge$. (In Boolean algebra, it is denoted by the dot ".").
  - The operation "or" is denoted $\vee$. (In Boolean algebra, it is denoted by +).
  - The operation "not" is denoted $\neg$, $\sim$, $\bar{}$ (overbar), or $'$.
- Logic is concerned much more about the truth values of propositions than about their meanings.
- Therefore, and for convenience and efficiency, propositions are often denoted with single-letter symbols such as *p*, *q*, *r*, etc. And the focus is on whether a proposition *p* is true or false, rather than on what *p* means/designates. For example, we can denote "Mars is a planet" by *p*, "Jupiter is a star" by *q*, and "Pluto is a comet" by *r*. Then the above examples of compound statements can be succinctly represented as:
  - "Mars is a planet and Jupiter is a star": $p \wedge q$. This (i.e., $p \wedge q$) is called a *conjunction*.
  - "Mars is a planet or Jupiter is a star": $p \vee q$. This (i.e., $p \vee q$) is called a *disjunction*.
  - "not (Jupiter is a star)": $\neg p$, $\sim p$, $\bar{p}$, or p'.

- “Mars is a planet and (Jupiter is a star or not(Pluto is a comet))”: $p \wedge (q \vee \neg s)$.

Truth Tables:

- A *truth table* for a compound proposition gives the truth value of the proposition for each possible combination of the truth values of the simple propositions that make up the compound proposition. Truth tables have many applications, including determining (1) when a proposition is true, (2) whether two propositions are logically equivalent, (3) when a given proposition implies another given proposition, (4) constructing and optimizing digital circuits (hardware), etc.
- The most basic truth tables, which form our foundation of logic and reasoning, are the truth tables for the three logical connectives:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \wedge q}$
T	T	T
T	F	F
F	T	F
F	F	F

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \vee q}$
T	T	T
T	F	T
F	T	T
F	F	F

$\boldsymbol{p}$	$\boldsymbol{\neg p}$
T	F
F	T

- Examples of truth tables:
  - Truth table for $p \wedge (q \vee r)$: The table will list the 8 different combinations of the truth values of the propositions p, q and r. Also, because it needs the $(q \vee r)$ values, a separate column will be added to the table for $(q \vee r)$. Finally, to fill the column of $p \wedge (q \vee r)$, we apply the $\wedge$ operation to the column of p and the column of $q \vee r$:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{q \vee r}$	$\boldsymbol{p \wedge (q \vee r)}$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

  - Truth table for $(p \wedge q) \vee (p \wedge r)$:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{p \wedge q}$	$\boldsymbol{p \wedge r}$	$\boldsymbol{(p \wedge q) \vee (p \wedge r)}$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	T	F	F
F	F	F	F	F	F

- Equivalence of two propositions (a first look): Note that the column of $p \wedge (q \vee r)$ and the column of $(p \wedge q) \vee (p \wedge r)$ are identical, thus indicating that those two propositions are equivalent, meaning that they have the same truth values for the same combinations of truth-values of the simple propositions that make them up.

  In fact, that's one basic way to show that two different propositions are equivalent:
    - Build a truth table for each proposition, and then observe if the two columns of the two propositions are identical (make sure that the combinations of the truth-values are listed in the same order in both tables).

  Note that to save time and space, the two tables can be combined into a single table, as follows:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{q \vee r}$	$\boldsymbol{p \wedge q}$	$\boldsymbol{p \wedge r}$	$\boldsymbol{p \wedge (q \vee r)}$	$\boldsymbol{(p \wedge q) \vee (p \wedge r)}$
T	T	T	T	T	T	T	T
T	T	F	T	T	F	T	T
T	F	T	T	F	T	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

- Another example: Showing equivalence of $\neg(p \wedge q)$ and $\neg p \vee \neg q$:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{p \wedge q}$	$\boldsymbol{\neg p}$	$\boldsymbol{\neg q}$	$\boldsymbol{\neg(p \wedge q)}$	$\boldsymbol{\neg p \vee \neg q}$
T	T	T	T	F	F	F	F
T	T	F	T	F	F	F	F
T	F	T	F	F	T	T	T
T	F	F	F	F	T	T	T
F	T	T	F	T	F	T	T
F	T	F	F	T	F	T	T
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

  Looking at the two rightmost columns, we find them to be identical, thereby proving that $\neg(p \wedge q)$ and $\neg p \vee \neg q$ are logically equivalent.

<u>**Predicates**</u>:

- Predicates generalize propositions to include "quantification", that is, the phrases "for every" and "there exists", and thereby increase the expressive and reasoning power of logic.
- *Universal quantifier*: It is the phrase "for every" (or "for all"), and it is denoted $\forall$.
- *Existential quantifier*: It is the phrase "there exists" or "there is" (at least), and is denoted $\exists$.

- Example: Consider the English sentence "every rational number is a fraction of two integers", which is equivalent to the more detailed sentence "for every rational number *x*, there exists an integer *m* and there exists an integer *n* such that $x = \frac{m}{n}$". That sentence can be written more formally (and more succinctly) as: $(\forall x \in \boldsymbol{Q})(\exists m \in \boldsymbol{Z})(\exists n \in \boldsymbol{Z})(x = \frac{m}{n})$. An alternative form is: $\forall x \in \boldsymbol{Q}, \exists m \in \boldsymbol{Z}, \exists n \in \boldsymbol{Z}, x = \frac{m}{n}$.
- *Predicate*: A predicate is a proposition that involves one or more quantifier.
- Examples of predicates:
  - Some natural numbers are prime numbers: $(\exists n \in \boldsymbol{N})(n \text{ is prime})$.   Note: that is true
  - Every natural number is prime: $(\forall n \in \boldsymbol{N})(n \text{ is prime})$.   Note: that is false
  - Between every two distinct real numbers there is at least one rational number:
    $$(\forall x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})(\exists z \in \boldsymbol{Q})(x = y \ \vee\ x < z < y \ \vee\ y < z < x).$$
    Or equivalently:
    $$(\forall x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})(x < y \ \Rightarrow\ (\exists z \in \boldsymbol{Q})(x < z < y)).$$
  - For every integer *n*, *n*(*n*+1) is even: $(\forall n \in \boldsymbol{Z})(n(n+1) \text{ is even})$. Note that sometimes a predicate is written semi-formally such as: $(\forall \text{ integer } n)(n(n+1) \text{ is even})$, or: $\forall \text{ integer } n, n(n+1) \text{ is even}$.
  - All humans are mortal: $(\forall \text{ human } x)(x \text{ is mortal})$, or: $\forall \text{ human } x, x \text{ is mortal}$.
- General form of predicates: From the above examples, we can see that each predicate is for the form:
  - $(\exists x \in A)(P(x))$
    Notes: P(*x*) is a proposition involving the variable *x*, and A is some defined set called the *domain* of *x*. Such a predicate is called an *existential statement/predicate*, and it is True if there is at least one element *x* in the set A that would make the sentence P(*x*) True.

  - $(\forall x \in A)(P(x))$, or simply: $\forall x \in A, P(x)$
    Notes: Such a predicate is called a *universal statement/predicate*. It is true if P(*x*) is true for every element *x* in the domain A.

  - $(\forall x \in A)(\exists y \in B)(P(x,y))$

    Note: P(x,y) is a proposition involving variables x and y. It is true if for every element x in A, we can find at least element y in B (where y depends on x), such that P(x,y) is true.

  - Generally, a predicate is of the form$(Q_1 x_1 \in A_1)(Q_2 x_2 \in A_2) \dots (Q_n x_n \in A_n)(P(x_1, x_2, \dots, x_2))$ where each Q_i is $\forall$ or $\exists$, and $P(x_1, x_2, \dots, x_2)$ is a simple/compound proposition involving the variables $x_1, x_2, \dots, x_2$, and can be an implication or an equivalence.

Logical Rules of Reasoning:

At the foundation of formal reasoning and proving lie basic rules of logical equivalence and logical implications. The following tables summarize those rules. Note that all of those rules can be proved using truth tables.

Logical Equivalences

Definition: Two propositions/predicates p and q are said to be *equivalent* (denoted $p \Leftrightarrow q$) if whenever p is true, q is true, and vice versa. (Sometimes people use $\equiv$ or iff or even $=$, when they mean $\Leftrightarrow$)

Let p, q, and r be three arbitrary propositions/predicates. The following logical equivalences hold:

1. Commutative laws:	$p \wedge q \Leftrightarrow q \wedge p$	$p \vee q \Leftrightarrow q \vee p$
2. Associative laws:	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
3. Distributive laws:	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
4. Identity laws:	$p \wedge T \Leftrightarrow p$	$p \vee F \Leftrightarrow p$
5. Complementation laws:	$p \vee \neg p \Leftrightarrow T$	$p \wedge \neg p \Leftrightarrow F$
6. Double negative laws:	$\neg(\neg(p) \Leftrightarrow p$	
7. Idempotent laws:	$p \wedge p \Leftrightarrow p$	$p \vee p \Leftrightarrow p$
8. Universal bound laws:	$p \vee T \Leftrightarrow T$	$p \wedge F \Leftrightarrow F$
9. De Morgan's laws:	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$
10. Absorption laws:	$p \vee (p \wedge q) \Leftrightarrow p$	$p \wedge (p \vee q) \Leftrightarrow p$
11. Negations of T and F:	$\neg T \Leftrightarrow F$	$\neg F \Leftrightarrow T$

Definitions:

- A *conditional implication*, denoted $p \rightarrow q$, is by definition $\neg p \vee q$. That is, $p \rightarrow q \stackrel{\text{def}}{=} \neg p \vee q$.
- A *tautology* is a proposition/predicate that is always true. For example, $p \vee \neg p$ is a tautology.
- *Logical implication*: If $p \rightarrow q$ is a tautology, we say that p *logically implies* q, or simply p implies q, and denote it $p \Rightarrow q$. In other terms, $p \Rightarrow q$ if (whenever p is true, q must be true).

Logical Implications Rules:

1. Specialization:	$(p \wedge q) \Rightarrow p$	$(p \wedge q) \Rightarrow q$
2. Generalization:	$p \Rightarrow (p \vee q)$	$q \Rightarrow (p \vee q)$
3. Elimination:	$((p \vee q) \wedge \neg p) \Rightarrow q$	$((p \vee q) \wedge \neg q) \Rightarrow p$
4. Transitivity:	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$	$((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)) \Rightarrow (p \Leftrightarrow r)$
5. Contrapositive:	$(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$	
6. Modus Ponens:	$((p \Rightarrow q) \wedge p) \Rightarrow q$	
7. Modus Tollens:	$((p \Rightarrow q) \wedge \neg q) \Rightarrow \neg p$	
8. Contradiction rule:	$(\neg p \Rightarrow F) \Rightarrow p$	[to prove p, assume $\neg p$ and derive something false]
9. Division into cases:	$\big((p \Rightarrow r) \wedge (q \Rightarrow r)\big) \Rightarrow ((p \vee q) \Rightarrow r)$	
10. $(p \Rightarrow q) \Rightarrow ((r \wedge p) \Rightarrow (r \wedge q))$		$(p \Rightarrow q) \Rightarrow ((r \vee p) \Rightarrow (r \vee q))$
11. $\big((p \Rightarrow q) \wedge (p \Rightarrow r)\big) \Rightarrow \big(p \Rightarrow (q \wedge r)\big)$		$\big((p \Rightarrow q) \vee (p \Rightarrow r)\big) \Rightarrow \big(p \Rightarrow (q \vee r)\big)$
12. $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$		

How to prove an implication rule: to prove that $P \Rightarrow Q$ for some proposition P and some proposition Q, build the truth table for $P \rightarrow Q$ (that is, for $\neg P \vee Q$), and show that the column under $P \rightarrow Q$ is all T. Example: show that $((p \vee q) \wedge \neg p) \Rightarrow q$.

How to prove an equivalence rule/law: to prove an equivalence rule $P \Leftrightarrow Q$ for some proposition P and some proposition Q, build the truth table for P and Q, and show that the columns of P and Q are identical. This was illustrated earlier.

Rules of Predicate Logic:

1. $(\forall x \in \mathrm{A})(\mathrm{P}(x)) \Rightarrow (\exists x \in \mathrm{A})(\mathrm{P}(x))$
2. $\neg(\forall x \in \mathrm{A})(\mathrm{P}(x)) \Leftrightarrow (\exists x \in \mathrm{A})(\neg\mathrm{P}(x))$
3. $\neg(\exists x \in \mathrm{A})(\mathrm{P}(x)) \Leftrightarrow (\forall x \in \mathrm{A})(\neg\mathrm{P}(x))$
4. $\neg[(Q_1 x_1 \in A_1)(Q_2 x_2 \in A_2) \dots (Q_n x_n \in A_n)(P(x_1, x_2, \dots, x_2))] \Leftrightarrow$ $(Q'_1 x_1 \in A_1)(Q'_2 x_2 \in A_2) \dots (Q'_n x_n \in A_n)(\neg P(x_1, x_2, \dots, x_2))$, where each Q_i is $\forall$ or $\exists$, and where $\forall' = \exists$ and $\exists' = \forall$.

Converse, inverse, and contrapositive:

- The *converse* of $p \rightarrow q$ is $q \rightarrow p$. The *converse* of $p \Rightarrow q$ is $q \Rightarrow p$. Note that if $p \Rightarrow q$, it does not follow that its converse holds.
- The *inverse* of $p \rightarrow q$ is $\neg p \rightarrow \neg q$. The *inverse* of $p \Rightarrow q$ is $\neg p \Rightarrow \neg q$. Note that if $p \Rightarrow q$, it does not follow that its inverse holds.
- The *contrapositive* of $p \rightarrow q$ is $\neg q \rightarrow \neg p$. The *contrapositive* of $p \Rightarrow q$ is $\neg q \Rightarrow \neg p$. Note that if $p \Rightarrow q$, then its contrapositive must hold (the contrapositive rule).

Definition of a proof: A *proof* is a sequence of steps from given/known propositions (called *assumptions* or *premises* or *hypotheses*) to a final proposition (called *conclusion*), where every step is an implication.

Types of proofs: Let P and Q be two propositions/predicates, and suppose we wish to prove $P \Rightarrow Q$. There are several types of proof for $P \Rightarrow Q$:

- **Direct proof**: It is of the form $P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow P_n \Rightarrow Q$ where each implication is one of the rules of implication or a previously proved implication. This works because of transitivity of implication.
- **Indirect proof**:
  - **Proof by contradiction**: Assume $\neg Q$ is true, and derive (from P and $\neg Q$) a false statement through a sequence of implications. This works because of the contradiction rule.
  - **Contrapositive proof**: Prove that $\neg Q \Rightarrow \neg P$. This works because of the contrapositive rule.
- **Proof by a counterexample:** Suppose we wish to prove "$(\forall x \in \mathrm{A})(\mathrm{P}(x))$" is false. It is enough to prove that $\neg(\forall x \in \mathrm{A})(\mathrm{P}(x))$ is true, which is equivalent to proving that $(\exists x \in \mathrm{A})(\neg\mathrm{P}(x))$ is true. The latter means that we need (and it is sufficient) to find just one specific element x in A such that P(x) is false. The element x is called a counterexample. Thus, a proof of "$(\forall x \in \mathrm{A})(\mathrm{P}(x))$ is false" by a counterexample entails finding just one specific element x in A such that P(x) is false.
  - Exercise: Prove the following is not true: "$\forall$ positive integer $n, 4^n + 1$ is a prime number".

- **Proof of a declarative statement or a predicate**: Let Q be a declarative statement or a predicate, and suppose we are asked to prove Q to be true. Examples of Q: "11 is prime", "$\forall$set $A, |2^A| = 2^{|A|}$", etc.
  - Proof of$Q$ when $Q$is a declarative statement, not a predicate: use the definitions and properties of the terms in Q as your premises, and prove that those premises imply Q.
  - Proof of Q when Q is a universal predicate of the form $(\forall x \in \mathrm{A})(\mathrm{P}(x))$: Take *x* as an arbitrary element of A (don't take examples or specific elements of A), and use the definition/properties of the domain A as your premises, and prove that those premises imply Q.
  - Proof of Q when Q is an existential predicate of the form $(\exists x \in \mathrm{A})(\mathrm{P}(x))$: Find a specific element *x* in the domain A for which the proposition/predicate $\mathrm{P}(x)$ is true.
- **Proof by induction**: To be explained in a later lesson.

<u>Proof of equivalence</u>: Let P and Q be two propositions/predicates, and we wish to prove $P \Leftrightarrow Q$. There are two broad approaches:

- Direct approach: It is of the form $P \Leftrightarrow P_1 \Leftrightarrow P_2 \Leftrightarrow \cdots \Leftrightarrow P_n \Leftrightarrow Q$ where each equivalence is one of the equivalence laws or a previously proved equivalence.
- By two implications: Prove $P \Rightarrow Q$ and $Q \Rightarrow P$.

<u>Some fine points and additional notations</u>:

- If $P \Rightarrow Q$, we say:
  - Q is a *necessary condition* for P
  - P is a *sufficient condition* for Q
  - Q is true *if* P is true (or: if P, then Q).
  - P is true *only if* Q is true.

  Example: We know that: "an integer *n* is divisible by 6" ⇒ "*n* is divisible by 3". Clearly, divisibility by 3 is a necessary condition for divisibility by 6 (i.e., without being divisible by 3, an integer cannot be divisible by 6). Similarly, divisibility by 6 is a sufficient condition for divisibility by 3. Also, an integer is divisible by 6 only if it is divisible by 3.
- If and only if (iff)
  - We say "P is true *if and only if* Q is true" to mean the same thing as "P is equivalent to Q", i.e., $P \Leftrightarrow Q$.
- *Necessary and sufficient conditions*: When $P \Leftrightarrow Q$, we can say that Q is a necessary and sufficient condition for P. For example, divisibility by both 3 and 2 is a necessary and sufficient condition for divisibility by 6; that is because an integer is divisible by 6 if and only if it is divisible by both 3 and 2.
- Notation for *"therefore"*: $\therefore$
- *Paradox:* A paradox is a statement that contradicts itself (e.g., if it is true, then it is false, and if it is false, then it is true!). Examples:
  - "This statement is false"
  - "The next statement is true". "The previous statement is false".