

# Mathematical Foundations of Computer Science

## Lecture Outline

Jan 16, 2023

---

### Introduction to Logic

A *proposition* is a statement that is either true or false. For example, “ $2 + 2 = 4$ ” and “Donald Knuth is a faculty at Rutgers-Camden” are propositions, whereas “What time is it?”,  $x^2 < x + 40$  are not propositions.

We can construct compound propositions from simpler propositions by using some of the following connectives. Let  $p$  and  $q$  be arbitrary propositions.

**Negation:**  $\bar{p}$  (read as “not  $p$ ”) is the proposition that is true when  $p$  is false and vice-versa.

**Conjunction:**  $p \wedge q$  (read as “ $p$  and  $q$ ”) is the proposition that is true when both  $p$  and  $q$  are true.

**Disjunction:**  $p \vee q$  (read as “ $p$  or  $q$ ”) is the proposition that is true when at least one of  $p$  or  $q$  is true.

**Exclusive Or:**  $p \oplus q$  (read as “ $p$  exclusive-or  $q$ ”) is the proposition that is true when exactly one of  $p$  and  $q$  is true and false otherwise.

**Implication:**  $p \rightarrow q$  (read as “ $p$  implies  $q$ ”) is the proposition that is false when  $p$  is true and  $q$  is false and is true otherwise.

The implication  $q \rightarrow p$  is called the *converse* of the implication  $p \rightarrow q$ . The implication  $\neg p \rightarrow \neg q$  is called the *inverse* of  $p \rightarrow q$ . The implication  $\neg q \rightarrow \neg p$  is the *contrapositive* of  $p \rightarrow q$ .  $p$  *only if*  $q$  means “if not  $q$  then not  $p$ ”, or equivalently if  $p$  then  $q$ .

**Biconditional:**  $p \leftrightarrow q$  (read as “ $p$  if, and only if,  $q$ ”) is the proposition that is true if  $p$  and  $q$  have the same truth values and is false otherwise. “If and only if” is often abbreviated as *iff*.

The following truth table makes the above definitions precise.

$p$	$q$	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
T	T	F	T	T	F	T	T	T
T	F	F	F	T	T	F	T	F
F	T	T	F	T	T	T	F	F
F	F	T	F	F	F	T	T	T

**Necessary and Sufficient Conditions:** For propositions  $p$  and  $q$ ,

$p$  is a *sufficient* condition for  $q$  means that  $p \rightarrow q$ .

$p$  is a *necessary* condition for  $q$  means that  $\neg p \rightarrow \neg q$ , or equivalently  $q \rightarrow p$ .

Why is  $p \wedge q$  not the correct answer?

Thus  $p$  is a necessary and sufficient condition for  $q$  means “ $p$  iff  $q$ ”.

## Logical Equivalence

Two compound propositions are logically equivalent if they always have the same truth value. Two statement  $p$  and  $q$  can be proved to be logically equivalent either with the aid of truth tables or using a sequence of previously derived logically equivalent statements.

**Example.** Show that  $p \rightarrow q \equiv \neg p \vee q \equiv \neg q \rightarrow \neg p$ .

**Solution.** The truth table below proves the above equivalence.

$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \vee q$	$\neg q \rightarrow \neg p$
T	T	F	F	T	T	T
T	F	F	T	F	F	F
F	T	T	F	T	T	T
F	F	T	T	T	T	T

**Example.** Show that  $p \equiv \neg p \rightarrow C$  and  $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow C$ .

$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$p \wedge \neg q$	$C$	$\neg p \rightarrow C$	$(p \wedge \neg q) \rightarrow C$
T	T	F	F	T	F	F	T	T
T	F	F	T	F	T	F	T	F
F	T	T	F	T	F	F	F	T
F	F	T	T	T	F	F	F	T

The above equivalence forms the basis of proofs by contradiction.

---

## The logic of Quantified Statements

Consider the statement  $x < 15$ . We can denote such a statement by  $P(x)$ , where  $P$  denotes the predicate “is less than 15” and  $x$  is the variable. This statement  $P(x)$  becomes a proposition when  $x$  is assigned a value. In the above example,  $P(8)$  is true while  $P(18)$  is false.

Another way to convert the statement  $P(x)$  into a proposition is through *quantification*. The two types of quantification that we will study are *universal quantification* and *existential quantification*. Using universal quantifier  $\forall$  (“for all”) alongside  $P(x)$  means that the statement  $P(x)$  is true for all elements in the domain of  $x$ . Thus the proposition  $\forall x \in D, P(x)$  is true when  $P(x)$  is true for all  $x \in D$  and is false if there is an element

$x' \in D$  for which  $P(x')$  is false. Using existential quantifier  $\exists$  (“there exists”) alongside  $P(x)$  means that there exists an element in the domain of  $x$  for which  $P(x)$  is true. Thus the proposition  $\exists x \in D, P(x)$  is true if there is an  $x' \in D$  for which  $P(x')$  is true and is false if  $P(x)$  is false for all  $x \in D$ .

Examples of propositions using quantifiers are as follows.

1.  $\forall x \in \mathbb{Z}, x^3 + 1$  is composite.
2.  $\forall x \in \mathbb{Z}, x$  is even  $\rightarrow x + 1$  is odd.
3.  $\exists x \in \mathbb{N}, x^2 \neq x$ .
4.  $\exists x \in \mathbb{Z}, 2|x$  and  $2 \nmid x + 1$ .
5.  $\forall x \in \mathbb{Z} \exists y \in \mathbb{Z}, x + y = 0$ .
6.  $\exists x \in \mathbb{Z} \forall y \in \mathbb{Z}, x > y$ .

Sometimes it helps (in proofs) to consider the negation of a proposition. Verify the following equivalence.

$$\begin{aligned}\neg(\forall x \in D, P(x)) &\equiv \exists x \in D, \neg P(x) \\ \neg(\exists x \in D, P(x)) &\equiv \forall x \in D, \neg P(x)\end{aligned}$$

## Proofs

We will illustrate some proof techniques by proving some properties about numbers. Before we do that let's go through some basic definitions given below.

An integer  $n$  is *even* iff  $n = 2k$  for some integer  $k$ . An integer is *odd* iff  $n = 2k + 1$  for some integer  $k$ . Symbolically,

$$\begin{aligned}n \text{ is even} &\leftrightarrow \exists \text{ an integer } k \text{ s.t. } n = 2k \\ n \text{ is odd} &\leftrightarrow \exists \text{ an integer } k \text{ s.t. } n = 2k + 1\end{aligned}$$

An integer  $n$  is *prime* iff  $n > 1$  and for all positive integers  $r$  and  $s$ , if  $n = r \cdot s$ , then  $r = 1$  or  $s = 1$ . Otherwise  $n$  is *composite*.

Given any real number  $x$ , the *floor of*  $x$ , denoted by  $\lfloor x \rfloor$ , is defined as follows

$$\lfloor x \rfloor = n \leftrightarrow n \leq x < n + 1, \text{ where } n \text{ is an integer}$$

Given any real number  $x$ , the *ceiling of*  $x$ , denoted by  $\lceil x \rceil$ , is defined as follows

$$\lceil x \rceil = n \leftrightarrow n - 1 < x \leq n, \text{ where } n \text{ is an integer}$$

A real number is *rational* iff it can be expressed as a ratio of two integers with a non-zero denominator. A real number that is not rational is *irrational*. More formally,

$$r \text{ is rational} \leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = a/b \text{ and } b \neq 0.$$


---

**Example.** Prove the following: If the sum of two integers is even then so is their difference.

**Solution.** Let  $m$  and  $n$  be particular but arbitrarily chosen integers such that  $m + n$  is even. By definition of even, we have  $m + n = 2k$ , for some integer  $k$ . Then

$$m = 2k - n$$

Now  $m - n$  can be written as follows.

$$\begin{aligned} m - n &= 2k - n - n \\ &= 2(k - n) \end{aligned}$$

Since  $k$  and  $n$  are integers,  $k - n$  is an integer,  $2(k - n)$  is even and hence  $m - n$  is even.

---

**Example.** Prove that, for all integers  $n$ , if  $n$  is odd then  $n^2 + n + 1$  is odd.

**Solution.** Since  $n$  is odd  $n = 2k + 1$  for some integer  $k$ . Then,

$$\begin{aligned} n^2 + n + 1 &= (2k + 1)^2 + 2k + 1 + 1 \\ &= 4k^2 + 4k + 1 + 2k + 2 \\ &= 4k^2 + 6k + 2 + 1 \\ &= 2(2k^2 + 3k + 1) + 1 \end{aligned}$$

Since  $k$  is an integer,  $p = 2k^2 + 3k + 1$  is an integer and  $n^2 + n + 1$  is odd, since  $n^2 + n + 1 = 2p + 1$  where  $p$  is an integer.