MC4010 - Discrete Mathematics

The Foundations: Logic and Proofs

T. Mayooran

Department of Inter Disciplinary Studies, Faculty of Engineering, University of Jaffna

2023-09-11

All contents of these slides are agglomerated from recommended reference textbook of this course and the previous year's lecture slides (Which were prepared by Dr P. Kathirgamanathan).

Slides are prepared through RMarkdown Beamer presentation option and executed via RStudio.

Introduction

- The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments.
- Besides the importance of logic in understanding mathematical reasoning, logic has numerous applications to computer science.
- These rules are used in the design of computer circuits, the construction of computer programs, the verification of the correctness of programs, and in many other ways. Furthermore, software systems have been developed for constructing some, but not all, types of proofs automatically.

Proposition

Our discussion begins with an introduction to the basic building blocks of logic—propositions. A proposition is a declarative sentence (that is, a sentence that declares a fact) that is either true or false, but not both.

Examples: All the following declarative sentences are propositions.

1. Colombo is the capital of the Sri Lanka.
2. Toronto is the capital of Canada.
3. $1 + 1 = 2$.
4. $2 + 2 = 3$.

   Propositions 1 and 3 are true, whereas 2 and 4 are false.

Proposition

Example: Consider the following sentences.

1. What time is it?
2. Read this carefully.
3. $x + 1 = 2$.
4. $x + y = z$.

Sentences 1 and 2 are not propositions because they are not declarative sentences. Sentences 3 and 4 are not propositions because they are neither true nor false.

Note that each of sentences 3 and 4 can be turned into a proposition if we assign values to the variables.

- We use letters to denote propositional variables (or statement variables), that is, variables that represent propositions, just as letters are used to denote numerical variables.
- The conventional letters used for propositional variables are $p, q, r, s, \ldots$.
- The truth value of a proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition.
- The area of logic that deals with propositions is called the propositional calculus or propositional logic. It was first developed systematically by the Greek philosopher Aristotle more than 2300 years ago.
- Many mathematical statements are constructed by combining one or more propositions. New propositions, called compound propositions, are formed from existing propositions using logical operators.

Definition: 1 (negation)

Let p be a proposition. The negation of p, denoted by $\neg p$ (also denoted by $\bar{p}$), is the statement "It is not the case that p."The proposition $\neg p$ is read "not p." The truth value of the negation of p, $\neg p$, is the opposite of the truth value of p.

Example: Find the negation of the proposition "Michael's PC runs Linux" and express this in simple English.

Solution: The negation is "It is not the case that Michael's PC runs Linux." This negation can be more simply expressed as "Michael's PC does not run Linux."

p	$\neg p$
T	F
F	T

Table 1: Truth table for the negation of a proposition p

Table 1 displays the truth table for the negation of a proposition p. This table has a row for each of the two possible truth values of a proposition p. Each row shows the truth value of $\neg p$ corresponding to the truth value of p for this row.

Definition: 2 (conjunction)

Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, is the proposition "p and q." The conjunction $p \wedge q$ is true when both p and q are true and is false otherwise.

Table 2 displays the truth table of $p \wedge q$. This table has a row for each of the four possible combinations of truth values of p and q. The four rows correspond to the pairs of truth values TT, TF, FT, and FF, where the first truth value in the pair is the truth value of p and the second truth value is the truth value of q.

Example: Find the conjunction of the propositions p and q where p is the proposition "Rebecca's PC has more than 16 GB free hard disk space" and q is the proposition "The processor in Rebecca's PC runs faster than 1 GHz."

Solution: The conjunction of these propositions, $p \wedge q$, is the proposition "Rebecca's PC has more than 16 GB free hard disk space, and the processor in Rebecca's PC runs faster than 1 GHz." This conjunction can be expressed more simply as "Rebecca's PC has more than 16 GB free hard disk space, and its processor runs faster than 1 GHz." For this conjunction to be true, both conditions given must be true. It is false, when one or both of these conditions are false.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 2: The Truth Table for the Conjunction of Two Propositions.

Definition: 3 (disjunction)

Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, is the proposition "p or q." The disjunction $p \vee q$ is false when both p and q are false and is true otherwise.

Example: What is the disjunction of the propositions p and q where p and q are the same propositions as in the previous Example?

Solution: The disjunction of p and q, $p \vee q$, is the proposition "Rebecca's PC has at least 16 GB free hard disk space, or the processor in Rebecca's PC runs faster than 1 GHz." This proposition is true when Rebecca's PC has at least 16 GB free hard disk space, when the PC's processor runs faster than 1 GHz, and when both conditions are true.

It is false when both of these conditions are false, that is, when Rebecca's PC has less than 16 GB free hard disk space and the processor in her PC runs at 1 GHz or slower.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 3: The Truth Table for the Disjunction of Two Propositions.

Definition: 4 (exclusive or)

Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

The truth table for the exclusive or of two propositions is displayed in Table 4.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Table 4: The Truth Table for the Exclusive Or of Two Propositions.

Conditional Statements

Definition: 5 (conditional statement) Let p and q be propositions. The conditional statement $p \to q$ is the proposition "if p, then q." The conditional statement $p \to q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \to q, p$ is called the hypothesis (or antecedent or premise) and q is called the conclusion (or consequence).

The statement $p \to q$ is called a conditional statement because $p \to q$ asserts that q is true on the condition that p holds. A conditional statement is also called an implication.

The truth table for the conditional statement $p \to q$ is shown in Table 5. Note that the statement $p \to q$ is true when both p and q are true and when p is false (no matter what truth value q has).

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 5: The Truth Table for the Conditional Statement $p \to q$.

A useful way to understand the truth value of a conditional statement is to think of an obligation or a contract.

For example, the pledge many politicians make when running for office is " If I am elected, then I will lower taxes."

If the politician is elected, voters would expect this politician to lower taxes. Furthermore, if the politician is not elected, then voters will not have any expectation that this person will lower taxes, although the person may have sufficient influence to cause those in power to lower taxes.

It is only when the politician is elected but does not lower taxes that voters can say that the politician has broken the campaign pledge. This last scenario corresponds to the case when p is true but q is false in $p \to q$.

Example: Let p be the statement "Maria learns discrete mathematics" and q the statement "Maria will find a good job." Express the statement $p \to q$ as a statement in English.

Solution: From the definition of conditional statements, we see that when p is the statement "Maria learns discrete mathematics" and q is the statement "Maria will find a good job," $p \to q$ represents the statement

"If Maria learns discrete mathematics, then she will find a good job."

There are many other ways to express this conditional statement in English. Among the most natural of these are:

- "Maria will find a good job when she learns discrete mathematics."
- "For Maria to get a good job, it is sufficient for her to learn discrete mathematics."
- "Maria will find a good job unless she does not learn discrete mathematics."

Definition: 6 (biconditional statement) Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition "p if and only if q." The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called bi-implications.

The truth table for $p \leftrightarrow q$ is shown in Table 6. Note that the statement $p \leftrightarrow q$ is true when both the conditional statements $p \rightarrow q$ and $q \rightarrow p$ are true and is false otherwise. That is why we use the words "if and only if" to express this logical connective and why it is symbolically written by combining the symbols$\rightarrow$and$\leftarrow$. There are some other common ways to express $p \leftrightarrow q$:

- "p is necessary and sufficient for q"
- "if p then q, and conversely"
- "p iff q."

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Table 6: The Truth Table for the biconditional Statement $p \leftrightarrow q$.

The last way of expressing the biconditional statement $p \leftrightarrow q$ uses the abbreviation "iff" for "if and only if." Note that $p \leftrightarrow q$ has exactly the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$.

Compound Propositions

We have now introduced four important logical connectives—conjunctions, disjunctions, conditional statements, and biconditional statements—as well as negations.

We can use these connectives to build up complicated compound propositions involving any number of propositional variables.We can use truth tables to determine the truth values of these compound propositions

We use a separate column to find the truth value of each compound expression that occurs in the compound proposition as it is built up.

The truth values of the compound proposition for each combination of truth values of the propositional variables in it is found in the final column of the table.

The precedence levels of the logical operators, $\neg, \wedge, \vee, \rightarrow$, and $\leftrightarrow$.

Example

Construct the truth table of the compound proposition $(p \vee \neg q) \to (p \wedge q)$.

Example

Consider the following propositions:

p : Mathematicians are generous.

q : Spiders hate algebra.

Write the compound propositions symbolized by:

1. $p \vee \neg q$
2. $\neg(q \wedge p)$
3. $\neg p \rightarrow q$
4. $\neg p \leftrightarrow \neg q$

Solutions

1. Mathematicians are generous or spiders don't hate algebra (or both)
2. It is not the case that spiders hate algebra and mathematicians are generous.
3. If mathematicians are not generous then spiders hate algebra.
4. Mathematicians are not generous if and only if spiders don't hate algebra.

Example

Let p be the proposition "Today is Monday" and q be "I will go to London". Write the following propositions symbolically.

1. If today is Monday then I won't go to London.
2. Today is Monday or I will go to London, but not both.
3. I will go to London and today is not Monday.
4. If and only if today is not Monday then I will go to London.

Solutions

1. $p \rightarrow \neg q$
2. $p \oplus q$
3. $q \wedge \neg p$
4. $\neg p \leftrightarrow q$

Exercise

Construct truth tables for the following compound propositions.

1. $\neg p \vee q$
2. $\neg p \wedge \neg q$
3. $\neg q \rightarrow p$
4. $\neg p \leftrightarrow \neg q$
5. $(p \vee q) \rightarrow (p \wedge q)$
6. $(p \rightarrow q) \oplus \neg q$
7. $\neg p \leftrightarrow (p \wedge q)$

Logic and Bit Operations

Computers represent information using bits.A bit is a symbol with two possible values, namely, 0 (zero) and 1 (one). This meaning of the word bit comes from binary digit, because zeros and ones are the digits used in binary representations of numbers.

The well-known statistician John Tukey introduced this terminology in 1946.A bit can be used to represent a truth value, because there are two truth values, namely, true and false. As is customarily done, we will use a 1 bit to represent true and a 0 bit to represent false. That is, 1 represents T (true), 0 represents F (false).

variable is called a Boolean variable if its value is either true or false. Consequently, a Boolean variable can be represented using a bit.

Truth Value	*Bit*
T	1
F	0

Computer bit operations correspond to the logical connectives. By replacing true by a one and false by a zero in the truth tables for the operators $\wedge$, $\vee$, and $\oplus$ the tables shown in Figure 1 for the corresponding bit operations are obtained.

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Figure 1: Truth table for the Bit Operators OR, AND, and XOR.

Definition: 7 (bit string)

A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

Example: 101010011 is a bit string of length nine.

Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit strings 01 1011 0110 and 11 0001 1101. (Here, and throughout this Section, bit strings will be split into blocks of four bits to make them easier to read.)

Solution: The bitwise *OR*, bitwise *AND*, and bitwise *XOR* of these strings are obtained the *OR*, *AND*, and *XOR* of the corresponding bits, respectively. This gives us

01 1011 0110	
11 0001 1101	
11 1011 1111	bitwise *OR*
01 0001 0100	bitwise *AND*
10 1010 1011	bitwise *XOR*

Practice problems:

Problem 1 Let p, q, and r be the propositions

$$p \text{ :You get an A on the final exam.}$$

$$q \text{ :You do every exercise in this book.}$$

$$r \text{ :You get an A in this class.}$$

Write these propositions using p, q, and r and logical connectives (including negations).

a) You get an A in this class, but you do not do every exercise in this book.

b) You get an A on the final, you do every exercise in this book, and you get an A in this class.

c) To get an A in this class, it is necessary for you to get an A on the final.

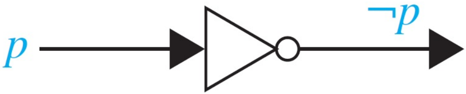
d) You get an A on the final, but you don't do every exercise in this book; nevertheless, you get an A in this class.

e) Getting an A on the final and doing every exercise in this book is sufficient for getting an A in this class.

f) You will get an A in this class if and only if you either do every exercise in this book or you get an A on the final.

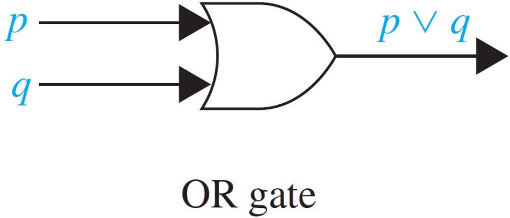
Logic Circuits

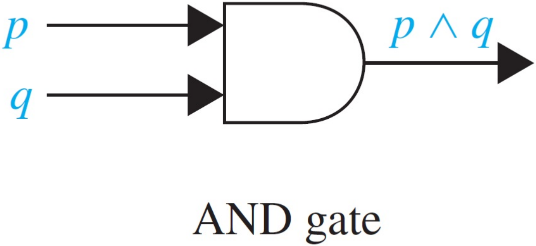
- Propositional logic can be applied to the design of computer hardware. This was first observed in 1938 by Claude Shannon in his MIT master's thesis.
- A logic circuit (or digital circuit) receives input signals $p_1, p_2, \ldots, p_n$, each a bit [either 0 (off) or 1 (on)], and produces output signals $s_1, s_2, \ldots, s_n$, each a bit. In this section we will restrict our attention to logic circuits with a single output signal; in general, digital circuits may have multiple outputs.



Inverter

Basic logic gates.





Complicated digital circuits can be constructed from three basic circuits, called gates, shown in the above Figures. The inverter, or NOT gate, takes an input bit p, and produces as output $\neg p$. The OR gate takes two input signals p and q, each a bit, and produces as output the signal $p \vee q$. Finally, the AND gate takes two input signals p and q, each a bit, and produces as output the signal $p \wedge q$.

Example: Determine the output for the combinatorial circuit in Figure 2.

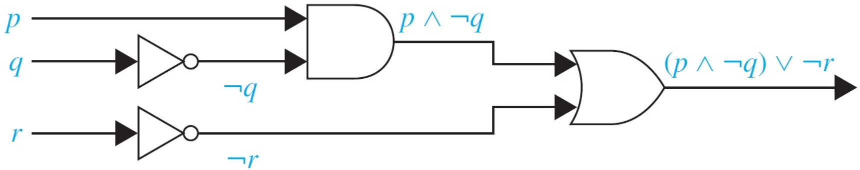


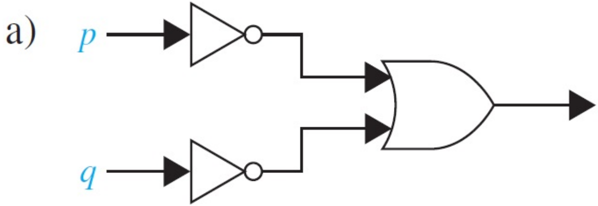
Figure 2: A combinatorial circuit.

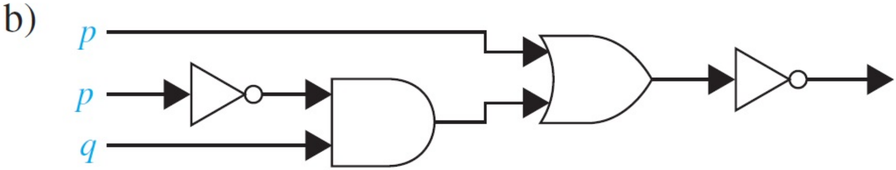
Practice problem:

1. Build a digital circuit that produces the output $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$ when given input bits p, q, and r.
2. Construct a combinatorial circuit using inverters, OR gates, and AND gates that produces the output $(p \wedge \neg r) \vee (\neg q \wedge r)$ from input bits p, q, and r.

Practice problem:

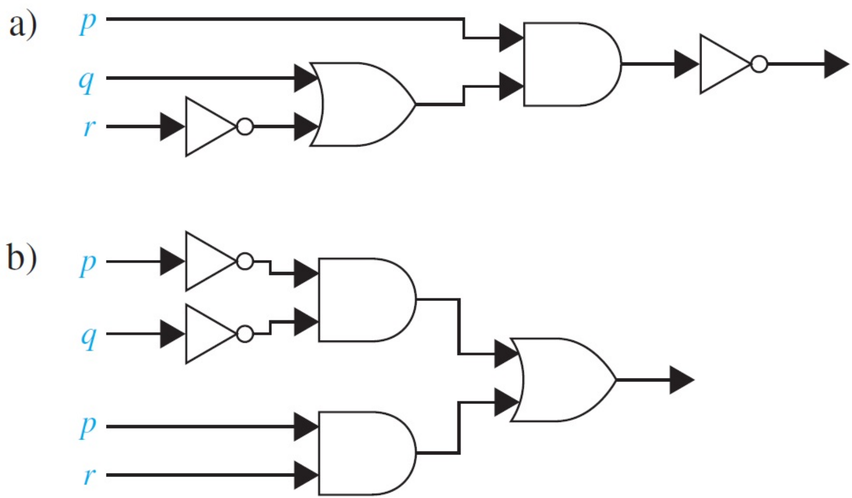
Find the output of each of these combinatorial circuits.





Practice problem:

Find the output of each of these combinatorial circuits.



Propositional Equivalences

Definition: 8 (tautology and contradiction) A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. A compound proposition that is neither a tautology nor a contradiction is called a contingency.

Example: We can construct examples of tautologies and contradictions using just one propositional variable. Consider the truth tables of $p \vee \neg p$ and $p \wedge \neg p$, shown in below Table. Because $p \vee \neg p$ is always true, it is a tautology. Because $p \wedge \neg p$ is always false, it is a contradiction.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

Logical Equivalences

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

Definition: 9 The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent.

Remark: The symbol $\equiv$ is not a logical connective, and $p \equiv q$ is not a compound proposition but rather is the statement that $p \leftrightarrow q$ is a tautology. The symbol $\Longleftrightarrow$ is sometimes used instead of $\equiv$ to denote logical equivalence.

De Morgan's Laws.

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Exercise

1. Show that $\neg(p \wedge q)$ and $\neg p \vee \neg q$ are logically equivalent.
2. Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.
3. Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.
4. Show that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent. This is the distributive law of disjunction over conjunction.

Some important equivalences.

Below table contains some important equivalences. In these equivalences, T denotes the compound proposition that is always true and F denotes the compound proposition that is always false.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws

Some important equivalences.

$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

Some important equivalences.

$$p \to q \equiv \neg p \lor q$$

$$p \to q \equiv \neg q \to \neg p$$

$$p \lor q \equiv \neg p \to q$$

$$p \land q \equiv \neg(p \to \neg q)$$

$$\neg(p \to q) \equiv p \land \neg q$$

$$(p \to q) \land (p \to r) \equiv p \to (q \land r)$$

$$(p \to r) \land (q \to r) \equiv (p \lor q) \to r$$

$$(p \to q) \lor (p \to r) \equiv p \to (q \lor r)$$

$$(p \to r) \lor (q \to r) \equiv (p \land q) \to r$$

Some important equivalences.

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$

$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$

$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

Practice problems:

1. Proof all equivalences which are provided in the tables given in the previous slides (42,43,44,45).
2. Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences.
3. Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Predicates and Quantifiers

Predicates

Statements involving variables, such as

$$"x > 3," \quad "x = y + 3," \quad "x + y = z,"$$

and "computer x is under attack by an intruder," and "computer x is functioning properly," are often found in mathematical assertions, in computer programs, and in system specifications. These statements are neither true nor false when the values of the variables are not specified.

The statement "x is greater than 3" has two parts. The first part, the variable x, is the subject of the statement. The second part—the predicate, "is greater than 3"—refers to a property that the subject of the statement can have.We can denote the statement "x is greater than 3" by $P(x)$, where P denotes the predicate "is greater than 3" and x is the variable.

The statement $P(x)$ is also said to be the value of the propositional function P at x. Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value.

Example:

Let $P(x)$ denote the statement "$x > 3$." What are the truth values of $P(4)$ and $P(2)$?

Solution:

We obtain the statement $P(4)$ by setting $x = 4$ in the statement "$x > 3$." Hence, $P(4)$, which is the statement "$4 > 3$," is true. However, $P(2)$, which is the statement "$2 > 3$," is false.

Quantifiers

When the variables in a propositional function are assigned values, the resulting statement becomes a proposition with a certain truth value. However, there is another important way, called quantification, to create a proposition from a propositional function.

Definition (universal quantification)

The universal quantification of $P(x)$ is the statement "$P(x)$ for all values of x in the domain." The notation $\forall x\ P(x)$ denotes the universal quantification of $P(x)$. Here $\forall$ is called the universal quantifier. We read $\forall x\ P(x)$ as "for all x $P(x)$" or "for every x $P(x)$." An element for which $P(x)$ is false is called a counterexample of $\forall x\ P(x)$.

Example Let $P(x)$ be the statement "$x + 1 > x$." What is the truth value of the quantification $\forall x\ P(x)$, where the domain consists of all real numbers?

Solution: Because $P(x)$ is true for all real numbers x, the quantification $\forall x\ P(x)$ is true.

Besides "for all" and "for every," universal quantification can be expressed in many other ways, including "all of," "for each," "given any," "for arbitrary," "for each," and "for any."

Example: Let $Q(x)$ be the statement "$x < 2$." What is the truth value of the quantification $\forall x\ Q(x)$, where the domain consists of all real numbers?

Solution: $Q(x)$ is not true for every real number x, because, for instance, $Q(3)$ is false. That is, $x = 3$ is a counterexample for the statement $\forall x\ Q(x)$. Thus $\forall x\ Q(x)$ is false.

Example: What is the truth value of $\forall x\ P(x)$, where $P(x)$ is the statement "$x^2 < 10$" and the domain consists of the positive integers not exceeding 4?

Example: What does the statement $\forall x\ N(x)$ mean if $N(x)$ is "Computer x is connected to the network" and the domain consists of all computers on campus?

Solution: The statement $\forall x\ N(x)$ means that for every computer x on campus, that computer x is connected to the network. This statement can be expressed in English as "Every computer on campus is connected to the network."

Example:

Symbolize the proposition 'Every day I go jogging'.

Solution:

Define the following

$D(x)$: x is a day

$J(x)$: x is when I go jogging

Then 'Every day I go jogging' can be paraphrased 'For every x, if x is a day, then x is when I go jogging'. We can express this proposition symbolically by:

$$\forall x[D(x) \to J(x)]$$

Definition (existential quantifier)

The existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$." We use the notation $\exists\ x\ P(x)$ for the existential quantification of P(x). Here $\exists$ is called the existential quantifier.

Besides the phrase "there exists,"we can also express existential quantification in many other ways, such as by using the words "for some," "for at least one," or "there is." The existential quantification $\exists\ x\ P(x)$ is read as

"There is an x such that $P(x)$,"

"There is at least one x such that $P(x)$,"

or

"For some $xP(x)$."

Example: Let $P(x)$ denote the statement "$x > 3$." What is the truth value of the quantification $\exists\ x\ P(x)$, where the domain consists of all real numbers?

Example: Let $Q(x)$ denote the statement "$x = x + 1$." What is the truth value of the quantification $\exists\ x\ Q(x)$, where the domain consists of all real numbers?

Statement	*When True?*	*When False?*
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Example: Symbolize 'Some people think of no one but themselves'

Solution:

Define $P(x)$: x is a person

$N(x)$: x thinks of no one but himself.

Then 'Some people think of no one but themselves' can be written:

$$\exists x[P(x) \wedge N(x)]$$

Exercise: Symbolize the proposition 'Some of the children didn't apologize'.

Exercise: Symbolize the proposition 'Nobody likes cheats'.

Methods of Proofs

Proving mathematical theorems can be difficult. To construct proofs we need all available ammunition, including a powerful battery of different proof methods. These methods provide the overall approach and strategy of proofs. Understanding these methods is a key component of learning how to read and construct mathematical proofs.

One we have chosen a proof method, we use axioms, definitions of terms, previously proved results, and rules of inference to complete the proof.

In this section, we are going to discuss two important methods of proof such as (1) Direct Proofs and (2) Proofs by Contradiction.

To prove a theorem of the form $\forall x(P(x) \to Q(x))$, our goal is to show that $P(c) \to Q(c)$ is true, where c is an arbitrary element of the domain, and then apply universal generalization.

Direct Proofs

A direct proof of a conditional statement $p \to q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.

A direct proof shows that a conditional statement $p \to q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs.

In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Definition:

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$. (Note that every integer is either even or odd, and no integer is both even and odd.)

Definition:

The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called irrational.

Example: Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution: Note that this theorem states $\forall n P((n) \rightarrow Q(n))$, where $P(n)$ is "n is an odd integer" and $Q(n)$ is "n^2 is odd." As we have said, we will follow the usual convention in mathematical proofs by showing that $P(n)$ implies $Q(n)$, and not explicitly using universal instantiation.

To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that n is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer.

We want to show that n^2 is also odd. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2. When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

By the definition of an odd integer, we can conclude that n^2 is an odd integer (it is one more than twice an integer). Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer.

Practice Problems

1. Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square. (An integer a is a perfect square if there is an integer b such that $a = b^2$.) (To see answers click here)
2. Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number r and every real number s, if r and s are rational numbers, then $r + s$ is rational.) (To see answers click here)

Proofs by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r. Proofs of this type are called proofs by contradiction.

The proof by contradiction does not prove a result directly, it is another type of indirect proof.

Exercises:

1. Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction. (To see answers click here)
2. Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd." (To see answers click here)

Don't hesitate to contact us if you have any questions about this course's teaching contents.

Also don't forget to check out the course page and Microsoft Team folder,

- course page https://mayooran1987.github.io/MC4010/
- Microsoft Team folder link