Logic and Proofs

Dit-Yan Yeung

Department of Computer Science and Engineering
Hong Kong University of Science and Technology

COMP 2711: Discrete Mathematical Tools for Computer Science

Contents

1. Propositional Logic
   - Propositions
   - Compound Propositions
   - Precedence of Logical Operators
   - More Examples
   - Propositional Equivalences
2. Predicate Logic
   - Predicates
   - Quantifiers
   - Quantifiers with Restricted Domains
   - Logical Equivalences involving Quantifiers
   - More Examples
   - Nested Quantifiers
3. Rules of Inference
   - Rules of Inference for Propositional Logic
   - Rules of Inference for Predicate Logic
4. Basic Proof Techniques
   - Some Terminology
   - Direct Proof
   - Proof by Contraposition
   - Proof by Contradiction
5. More Proof Techniques
   - Exhaustive Proof
   - Existence Proof
   - Uniqueness Proof
   - Further Remarks

Propositional Logic

Logic is the basis of all mathematical reasoning.

The rules of logic give precise meaning to mathematical statements.

Proposition

Definition

A **proposition** is a declarative statement (i.e., a sentence that declares a fact) that is either true or false, but not both.

Remark

Propositions are the basic building blocks of logic. The area of logic that deals with propositions is called **propositional logic** or **propositional calculus**.

Definition

The **truth value** of a proposition is true, denoted by T, if it is a true proposition and false, denoted by F, if it is a false proposition.

Example

Example 1

Each of the following declarative statements is a proposition:

(a) Hong Kong is a city in China.

(b) COMP 2711 or COMP 2711H is an elective course for the COMP program.

(c) $2 + 2 = 2^2$

(d) $1 + 1 = 3$

Propositions (a) and (c) are true but (b) and (d) are false.

Example

Example 2

Each of the following is not a proposition:

(a) No parking

(b) Who has an iPad?

(c) $y = \log(x + 1)$

(d) $x^2 - 3x + 1 = 0$

Logical Operator and Truth Table

Logical operators or **logical connectives** can be used to turn existing propositions into new propositions.

The definition of a logical operator can be given in the form of a **truth table** by enumerating all possible truth values of the proposition(s) involved.

Negation

Definition

Let p be a proposition. The **negation** of p, denoted by $\neg p$ or $\overline{p}$ and read as "not p", is the statement "it is not the case that p". The truth value of $\neg p$ is the opposite of the truth value of p.

Example 3

The truth table for the negation operator is shown below:

p	$\neg p$
T	F
F	T

The truth table has a row for each of the two possible truth values of the proposition p and the corresponding truth value of $\neg p$.

Conjunction

Definition

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. Its truth table is shown below:

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

Disjunction

Definition

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. Its truth table is shown below:

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

Exclusive Or

Definition

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. Its truth table is shown below:

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

Conditional Statement

Definition

Let p and q be propositions. The **conditional statement** $p \rightarrow q$ is the proposition "if p, then q". The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \rightarrow q$, p is called the **hypothesis** (or **antecedent** or **premise**) and q is called the **conclusion** (or **consequence**). Its truth table is shown below:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Conditional Statement (cont'd)

Remark

Equivalent ways of expressing $p \rightarrow q$:

- if p, then q
- q if p
- p implies q
- p only if q (which says that "p cannot be true when q is not true")
- q follows from p
- p is a sufficient condition for q
- q is a necessary condition for p
- q unless $\neg p$

Example

Example 4

Consider the following statement that a professor makes:

> "If you get 100% on the final exam, then you will get an A."

If a student manages to get 100% on the final exam, then she would expect to receive an A. If the student does not get 100%, she may or may not receive an A depending on other factors. However, if she does get 100% but the professor does not give her an A, she will feel cheated.

Principle (Principle of the excluded middle)

A statement is true exactly when it is not false.

Converse, Contrapositive, and Inverse

Definition

The **converse** of $p \rightarrow q$ is $q \rightarrow p$. The **contrapositive** of $p \rightarrow q$ is $\neg q \rightarrow \neg p$. The **inverse** of $p \rightarrow q$ is $\neg p \rightarrow \neg q$. The contrapositive always has the same truth value as $p \rightarrow q$, so we say that the two propositions are **equivalent**. The converse and the inverse are also equivalent.

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

Biconditional Statement

Definition

Let p and q be propositions. The **biconditional statement** or **bi-implications** $p \leftrightarrow q$ 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 value and is false otherwise. Its truth table is shown below:

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

Biconditional Statement (cont'd)

Remark

Equivalent ways of expressing $p \leftrightarrow q$:

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

Remark

The proposition $p \leftrightarrow q$ has exactly the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$.

Precedence of Logical Operators

Multiple logical operators can be used to construct compound propositions. The general rule of precedence is as follows:

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Parentheses can be used either for clarity or to change the precedence.

Example

Example 5

Construct the truth table of the compound proposition

$$p \vee \neg q \rightarrow p \wedge q,$$

which may be written more clearly as $(p \vee \neg q) \rightarrow (p \wedge q)$.

Example

Example 6

Express the system specification "the automated reply cannot be sent when the file system is full" using logical operators.

Example

Definition

Multiple system specifications are **consistent** if there exists an assignment of truth values to the propositions to make all specifications true. When there is no way to satisfy all the specifications, the specifications are said to be **inconsistent**.

Example 7

Determine whether the following system specifications are consistent:

- "the diagnostic message is stored in the buffer or it is retransmitted"
- "the diagnostic message is not stored in the buffer"
- "if the diagnostic message is stored in the buffer, then it is retransmitted"

Examples

Example 8

Do the system specifications in the previous example remain consistent if the specification "the diagnostic message is not retransmitted" is added?

Example 9

Find the bitwise AND ($\wedge$), bitwise OR ($\vee$), and bitwise XOR ($\oplus$) of the bit strings 01 1011 0110 and 11 0001 1101.

Remark

Computer **bit operations** correspond to the logical operators. In particular, the bit operations AND, OR, and XOR correspond to the operators $\wedge$, $\vee$, and $\oplus$, respectively. The bits 1 and 0 correspond to the truth values true and false, respectively.

Tautology and Contradiction

Definition

A **tautology** is a compound proposition that is always true, no matter what the truth values of the propositions that occur in it. A **contradiction** is a compound proposition that is always false. A **contingency** is a compound proposition that is neither a tautology nor a contradiction.

Example 10

$p \vee \neg p$ is a tautology, $p \wedge \neg p$ is a contradiction, and $p \to \neg p$ is a contingency, as illustrated in the following truth table.

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

Logical Equivalence

Definition

The compound propositions p and q are called **logically equivalent** if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ (or $p \Leftrightarrow q$) denotes that p and q are logically equivalent.

Remark

The symbol $\equiv$ is *not* a logical operator and $p \equiv q$ is *not* a compound proposition but rather is the statement that $p \leftrightarrow q$ is a tautology.

Example 11

Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Example 12

Show that $p \to q$ and $\neg p \vee q$ are logically equivalent.

Propositional Equivalences

The following table summarizes the major propositional equivalences:

Equivalence	Name
$p \wedge \mathrm{T} \equiv p$ $p \vee \mathrm{F} \equiv p$	Identity laws
$p \vee \mathrm{T} \equiv \mathrm{T}$ $p \wedge \mathrm{F} \equiv \mathrm{F}$	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

Propositional Equivalences (cont'd)

Equivalence	Name
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	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
$p \vee \neg p \equiv \mathrm{T}$ $p \wedge \neg p \equiv \mathrm{F}$	Negation laws

Propositional Equivalences (cont'd)

Equivalence	Name
$p \to q \equiv \neg p \vee q$ $p \to q \equiv \neg q \to \neg p$ $p \vee q \equiv \neg p \to q$ $p \wedge q \equiv \neg(p \to \neg q)$ $\neg(p \to q) \equiv p \wedge \neg q$ $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$ $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$ $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$ $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$	Involving conditional statements
$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$ $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$	Involving biconditional statements

Examples

Example 13

Use De Morgan's laws to express the negations of "Alice will send a secret message or Bob will send a secret message" and "today is Friday and today is a holiday".

Example 14

Show that $\neg(p \to q)$ and $p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences.

Examples

Example 15

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.

Example 16

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology by developing a series of logical equivalences.

Predicate Logic

Suppose we know that "every COMP student is required to take either COMP 2711 or COMP 2711H".

No rules of propositional logic allow us to conclude the truth of the statement "Chan Tai Man, a COMP student, is required to take either COMP 2711 or COMP 2711H".

In this section, we will study **predicate logic** which is more powerful than propositional logic.

Predicate

Definition

Informally, a **predicate** is a statement that may be true or false depending on the choice of values of its variables. Each choice of values produces a proposition. More formally, a statement involving n variables $x_1, x_2, \ldots, x_n$, denoted by $P(x_1, x_2, \ldots, x_n)$, is the value of the **propositional function** P at the n-tuple $(x_1, x_2, \ldots, x_n)$ and P is called an ***n*-place predicate** or ***n*-ary predicate**.

Remark

Boolean functions are commonly found in many programming languages. They are essentially predicates.

Examples

Example 17

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

Example 18

Let $A(x)$ denote the statement "HKUST student x is required to take either COMP 2711 or COMP 2711H". Suppose Alice is a COMP student and Bob is a CHEM student. What are the truth values of $A(\text{Alice})$ and $A(\text{Bob})$?

Example 19

Let $Q(x, y)$ denote the statement "$x = y + 3$". What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Universal Quantification

When the variables in a propositional function are assigned values, the resulting proposition has a certain truth value. However, sometimes we may want to say that a predicate is true over a set of values.

Definition

The **universal quantification** of $P(x)$ is the statement "for all elements x in the domain such that $P(x)$". 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 $\forall x\, P(x)$.

Domain

Remark

The **domain** or **universe** is the set of all possible values of a variable. The domain must always be specified when a universal quantifier is used; without it, the universal quantification of a statement is not well defined. Generally, an implicit assumption is made that the domain is nonempty or else $\forall x\, P(x)$ is true for any propositional function $P(x)$ because there are no elements x in the domain for which $P(x)$ is false.

Examples

Example 20

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?

Example 21

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?

Examples

Example 22

Let $P(x)$ be the statement "$x^2 > 0$". What is the truth value of the quantification $\forall x\, P(x)$, where the domain consists of all integers?

Example 23

What is the truth value of $\forall x\, (x^2 \geq x)$ if the domain consists of all real numbers? What is the truth value of it if the domain consists of all integers?

Existential Quantification

Definition

The **existential quantification** of $P(x)$ is the statement "there exists an element x in the domain such that $P(x)$". The notation $\exists x\, P(x)$ denotes the existential quantification of $P(x)$. Here $\exists$ is called the **existential quantifier**.

Remark

Note that $\exists x$ means "there exists at least one x in the domain" but not "there exists one and only one x in the domain" or "there exists a unique x in the domain". If we really want to refer to the latter meaning, we should use the **uniqueness quantifier** which is denoted by $\exists!$. Thus the quantification $\exists! x\, P(x)$ means "there exists a unique x such that $P(x)$ is true".

Universal and Existential Quantifiers

Universal and Existential Quantifiers		
Statement	When is it true?	When is it false?
$\forall x\, P(x)$	$P(x)$ is true for every x.	There exists an x for which $P(x)$ is false.
$\exists x\, P(x)$	There exists an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Examples

Example 24

Let $P(x)$ be 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 25

Let $Q(x)$ be 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?

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.

Example 26

$\forall x\, P(x) \vee Q(x)$ is the disjunction of $\forall x\, P(x)$ and $Q(x)$, i.e., it means $(\forall x\, P(x)) \vee Q(x)$ rather than $\forall x\, (P(x) \vee Q(x))$.

Example

Example 27

What does each of the following statements mean, assuming that the domain in each case consists of all real numbers?

(a) $\forall x < 0\, (x^2 > 0)$

(b) $\forall y \neq 0\, (y^3 \neq 0)$

(c) $\exists z > 0\, (z^2 = 2)$

Quantifier with Restricted Domain

Remark

The restriction of a universal quantification is the same as the universal quantification of a conditional statement. On the other hand, the restriction of an existential quantification is the same as the existential quantification of a conjunction.

Theorem 2.1

Let U_1 be a domain and U_2 be another domain, with $U_1 \subseteq U_2$. Suppose that $Q(x)$ is a statement such that $U_1 = \{x \mid Q(x) \text{ is true}\}$. Then, if $P(x)$ is a statement about U_2, it may also be interpreted as a statement about U_1, and

(a) $\forall x \in U_1 \, (P(x))$ is equivalent to $\forall x \in U_2 \, (Q(x) \rightarrow P(x))$

(b) $\exists x \in U_1 \, (P(x))$ is equivalent to $\exists x \in U_2 \, (Q(x) \wedge P(x))$.

Logical Equivalence

Definition

Statements involving predicates and quantifiers are **logically equivalent** if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain is used for the variables in these propositional functions. We use the notation $S \equiv T$ to indicate that two statements S and T involving predicates and quantifiers are logically equivalent.

Example 28

Show that $\forall x \, (P(x) \wedge Q(x))$ and $\forall x \, P(x) \wedge \forall x \, Q(x)$ are logically equivalent, where the same domain is used throughout.

Logical Equivalence (cont'd)

Remark

This logical equivalence shows that we can distribute a universal quantifier over a conjunction. Furthermore, we can also distribute an existential quantifier over a disjunction:

$$\exists x \, (P(x) \vee Q(x)) \equiv \exists x \, P(x) \vee \exists x \, Q(x).$$

However, we cannot distribute a universal quantifier over a disjunction, nor can we distribute an existential quantifier over a conjunction:

$$\begin{aligned} \forall x \, (P(x) \vee Q(x)) &\not\equiv \forall x \, P(x) \vee \forall x \, Q(x) \\ \exists x \, (P(x) \wedge Q(x)) &\not\equiv \exists x \, P(x) \wedge \exists x \, Q(x). \end{aligned}$$

Examples

Example 29

Express the following statement as a universal quantification: "every student in the class has sought the approval of the instructor to take the course". Then express the negation of the statement using an existential quantifier.

Example 30

Express the following statement as an existential quantification: "there is a student in the class who has sought the approval of the instructor to take the course". Then express the negation of the statement using a universal quantifier.

De Morgan's Laws for Quantifiers

De Morgan's Laws for Quantifiers			
Negation	Equivalent statement	When is it true?	When is it false?
$\neg\forall x\, P(x)$	$\exists x\, \neg P(x)$	There exists an x for which $P(x)$ is false.	$P(x)$ is true for every x.
$\neg\exists x\, Q(x)$	$\forall x\, \neg Q(x)$	$Q(x)$ is false for every x.	There exists an x for which $Q(x)$ is true.

De Morgan's Laws for Quantifiers (cont'd)

Remark

When the domain of a predicate $P(x)$ consists of n elements, where n is a positive integer, the rules for negating quantified statements are exactly the same as De Morgan's laws discussed before. When the domain has n elements $x_1, x_2, \ldots, x_n$, it follows that $\neg\forall x\, P(x)$ is the same as $\neg\big(P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)\big)$, which is equivalent to $\neg P(x_1) \vee \neg P(x_2) \vee \cdots \vee \neg P(x_n)$ by De Morgan's laws, and this is the same as $\exists x\, \neg P(x)$. Similarly, $\neg\exists x\, P(x)$ is the same as $\neg\big(P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)\big)$, which by De Morgan's laws is equivalent to $\neg P(x_1) \wedge \neg P(x_2) \wedge \cdots \wedge \neg P(x_n)$, and this is the same as $\forall x\, \neg P(x)$.

Examples

Example 31

What is the negation of the statement $\forall x\, (x^2 > x)$?

Example 32

What is the negation of the statement $\exists x\, (x^2 = 2)$?

Example 33

Show that $\neg\forall x\, \big(P(x) \rightarrow Q(x)\big)$ and $\exists x\, \big(P(x) \wedge \neg Q(x)\big)$ are logically equivalent.

Examples

Example 34

Express the statement "every student in this class has studied mathematics in secondary school" using predicates and quantifiers.

Example 35

Express the statement "some student in this class has learned C++ programming" using predicates and quantifiers.

Example 36

Express the statement "every student in this class has learned either C++ or Python" using predicates and quantifiers.

Example 37

Express the statement "every mail message larger than one megabyte will be compressed" using predicates and quantifiers.

Examples

Example 38

Consider the following statements. The first two are premises and the third is the conclusion. The entire set is called an argument.

- "All lions are fierce"
- "Some lions do not drink coffee"
- "Some fierce creatures do not drink coffee"

Let $P(x)$, $Q(x)$, and $R(x)$ be the statements "x is a lion", "x is fierce", and "x drinks coffee", respectively. Assuming that the domain consists of all creatures, express the statements in the argument using quantifiers and $P(x)$, $Q(x)$, and $R(x)$.

Remark

In the next section, we will discuss the issue of determining whether the conclusion is a valid consequence of the premises. In this example, it is.

Nested Quantifiers

Example 39

Assume that the domain for the variables x and y consists of all real numbers. The statement

$$\forall x \forall y \, (x + y = y + x)$$

says that $x + y = y + x$ for all real numbers x and y, which is the commutative law for addition of real numbers. Likewise, the statement

$$\forall x \exists y \, (x + y = 0)$$

says that for every real number x there is a real number y such that $x + y = 0$, which states that every real number has an additive inverse.

Nested Quantifiers (cont'd)

Example 40

Similarly, the statement

$$\forall x \forall y \forall z \, \big(x + (y + z) = (x + y) + z\big)$$

is the associative law for addition of real numbers.

Remark

Everything within the scope of a quantifier can be thought of as a propositional function. For example, $\forall x \exists y \, (x + y = 0)$ is the same thing as $\forall x \, P(x)$, where $P(x)$ is $\exists y \, Q(x, y)$ with $Q(x, y)$ denoting $x + y = 0$.

Examples

Example 41

Translate into English the statement

$$\forall x \forall y \, \big((x > 0) \land (y < 0) \rightarrow (xy < 0)\big),$$

where the domain for both variables consists of all real numbers.

Example 42

Let $Q(x, y)$ denote "$x + y = 0$". What are the truth values of the quantifications $\exists y \forall x \, Q(x, y)$ and $\forall x \exists y \, Q(x, y)$, where the domain for all variables consists of all real numbers?

Remark

This example illustrates that the order in which quantifiers appear makes a difference. The statements $\exists y \forall x \, Q(x, y)$ and $\forall x \exists y \, Q(x, y)$ are not logically equivalent.

Quantifications of Two Variables

The following table summarizes the meanings of the different possible quantifications involving two variables.

Quantifications of Two Variables		
Statement	When is it true?	When is it false?
$\forall x \forall y\, P(x,y)$ $\forall y \forall x\, P(x,y)$	$P(x,y)$ is true for every pair x, y.	There is a pair x, y for which $P(x,y)$ is false.
$\forall x \exists y\, P(x,y)$	For every x there is a y for which $P(x,y)$ is true.	There is an x such that $P(x,y)$ is false for every y.
$\exists x \forall y\, P(x,y)$	There is an x such that $P(x,y)$ is true for every y.	For every x there is a y for which $P(x,y)$ is false.
$\exists x \exists y\, P(x,y)$ $\exists y \exists x\, P(x,y)$	There is a pair x, y for which $P(x,y)$ is true.	$P(x,y)$ is false for every pair x, y.

Examples

Example 43

Let $Q(x,y,z)$ be the statement "$x + y = z$". What are the truth values of the statements $\forall x \forall y \exists z\, Q(x,y,z)$ and $\exists z \forall x \forall y\, Q(x,y,z)$, where the domain of the variables consists of all real numbers?

Example 44

Translate the statement "the sum of two positive integers is always positive" into a logical expression.

Example 45

Translate the statement "every real number except zero has a multiplicative inverse".

Examples

Example 46

Translate the statement

$$\forall x\, \big(C(x) \vee \exists y\, (C(y) \wedge F(x,y))\big)$$

into English, where $C(x)$ is "x has a computer", $F(x,y)$ is "x and y are friends", and the domain for both x and y consists of all students in the school.

Example 47

Translate the statement

$$\exists x \forall y \forall z\, \big((F(x,y) \wedge F(x,z) \wedge (y \neq z)) \rightarrow \neg F(y,z)\big)$$

into English, where $F(a,b)$ means a and b are friends and the domain for x, y, and z consists of all students in the school.

Examples

Example 48

Express the statement "if a person is female and is a parent, then this person is someone's mother" as a logical expression involving predicates, quantifiers with a domain consisting of all people, and logical connectives.

Example 49

Express the statement "everyone has exactly one best friend" as a logical expression involving predicates, quantifiers with a domain consisting of all people, and logical connectives.

Examples

Example 50

Use quantifiers to express the statement "there is a woman who has taken a flight on every airline in the world".

Example 51

Express the negation of the statement $\forall x \exists y\,(xy = 1)$ so that no negation precedes a quantifier.

Example 52

Use quantifiers to express the statement "there does not exist a woman who has taken a flight on every airline in the world" so that no negation precedes a quantifier.

Rules of Inference

Proofs in mathematics are valid arguments that establish the truth of mathematical statements.

- By an **argument**, we mean a sequence of statements that end with a conclusion.
- By **valid**, we mean that the conclusion, or final statement of the argument, must follow from the truth of the preceding statements, or **premises**, of the argument. That is, an argument is valid if and only if it is impossible for all the premises to be true and the conclusion to be false.

To deduce new statements from statements we already have, we use **rules of inference** which are templates for constructing valid arguments.

Rules of inference are our basic tools for establishing the truth of statements.

Argument and Argument Form

Definition

An **argument** in propositional logic is a sequence of propositions. All but the final proposition in the argument are called **premises** and the final proposition is called the **conclusion**. An argument is **valid** if the truth of all its premises implies that the conclusion is true.

Definition

An **argument form** in propositional logic is a sequence of compound propositions involving propositional variables. An argument form is **valid** if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Rules of Inference for Propositional Logic

Remark

An argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid when $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$ is a tautology. Using a truth table to show the validity of an argument form can be very tedious. This process can be simplified significantly by using rules of inference which are relatively simple argument forms serving as building blocks to construct more complicated valid argument forms.

Rules of Inference for Propositional Logic (cont'd)

Rules of Inference for Propositional Logic		
Rule of inference	Tautology	Name
p $p \to q$ $\therefore\ q$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore\ \neg p$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore\ p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore\ q$	$[(p \vee q) \wedge \neg p] \to q$	Disjunctive syllogism

Rules of Inference for Propositional Logic (cont'd)

Rules of Inference for Propositional Logic		
Rule of inference	Tautology	Name
p $\therefore\ p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore\ p$	$(p \wedge q) \to p$	Simplification
p q $\therefore\ p \wedge q$	$[(p) \wedge (q)] \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore\ q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \to (q \vee r)$	Resolution

Examples

Example 53

Show that the hypotheses

- "it is not sunny this afternoon and it is colder than yesterday"
- "we will go swimming only if it is sunny"
- "if we do not go swimming, then we will take a canoe trip"
- "if we take a canoe trip, then we will be home by sunset"

lead to the conclusion

- "we will be home by sunset".

Remark

We could have used a truth table to show that whenever each of the four hypotheses is true, the conclusion is also true. However, because we are working with five propositional variables p, q, r, s, and t, such a truth table would have $2^5 = 32$ rows.

Examples

Example 54

Show that the hypotheses

- "if you send me an email message, then I will finish writing the program"
- "if you do not send me an email message, then I will go to sleep early"
- "if I go to sleep early, then I will wake up feeling refreshed"

lead to the conclusion

- "if I do not finish writing the program, then I will wake up feeling refreshed".

Example 55

Show that the hypotheses "it is not snowing or Jasmine is skiing" and "it is snowing or Bart is playing hockey" imply that "Jasmine is skiing or Bart is playing hockey".

Example

Example 56

Show that the hypotheses $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $p \vee s$.

Remark

Resolution plays an important role in programming languages based on the rules of logic, such as Prolog (where resolution rules for quantified statements are applied). Furthermore, it can be used to build automatic theorem proving systems.

Examples

Example 57

Is the following argument valid?

- If you do every problem in the textbook, then you will learn discrete mathematics. You learned discrete mathematics.
- Therefore, you did every problem in the textbook.

Example 58

Is the following argument valid?

- If you do every problem in the textbook, then you will learn discrete mathematics. You did not do every problem in the textbook.
- Therefore, you did not learn discrete mathematics.

Rules of Inference for Predicate Logic

Rules of Inference for Predicate Logic

Rule of inference	Name
$\forall x\, P(x)$ $\therefore\ P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore\ \forall x\, P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore\ P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore\ \exists x\, P(x)$	Existential generalization

Examples

Example 59

Show that the premises “everyone in this discrete mathematics class has taken a course in computer science” and “Joseph is a student in this class” imply the conclusion “Joseph has taken a course in computer science”.

Example 60

Show that the premises “a student in this class has not read the textbook” and “everyone in this class passed the first unit test” imply the conclusion “someone who passed the first unit test has not read the textbook”.

Combining Rules of Inference for Propositions and Quantified Statements

Remark

In the two examples above, we used both universal instantiation (a rule of inference for quantified statements) and modus ponens (a rule of inference for propositions). Because they are used so often together, this combination of rules is sometimes called **universal modus ponens**. Another useful combination is called **universal modus tollens**.

Combining Rules of Inference for Propositions and Quantified Statements	
Rule of inference	Name
$\forall x\,(P(x) \rightarrow Q(x))$ $P(a)$, where a is a particular element in the domain $\therefore\ Q(a)$	Universal modus ponens
$\forall x\,(P(x) \rightarrow Q(x))$ $\neg Q(a)$, where a is a particular element in the domain $\therefore\ \neg P(a)$	Universal modus tollens

Example

Example 61

Assume that "for all positive integers n, if n is greater than 4, then n^2 is less than 2^n" is true. Use universal modus ponens to show that $100^2 < 2^{100}$.

Proof

A **proof** is a valid argument that establishes the truth of a mathematical statement.

A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proved theorems.

Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.

Some Terminology

Definition

A **theorem** is a statement that can be shown to be true.

Remark

In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important. Less important theorems are sometimes called **propositions**.

Definition

An **axiom** (or called **postulate**) is a statement that is assumed to be true.

Some Terminology (cont'd)

Definition

A less important theorem that is helpful in the proof of other theorems is called a **lemma**.

Definition

A **proof** is a valid argument that establishes the truth of a theorem. The statements used in a proof can include axioms, premises of the theorem, and previously proved theorems or lemmas.

Remark

Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually.

Some Terminology (cont'd)

Definition

A **corollary** is a theorem that can be established directly from a theorem that has been proved.

Definition

A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

Remark

When a proof of a conjecture is found, the conjecture becomes a theorem. However, many conjectures are eventually found to be false.

Direct Proof

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 axioms, definitions, previously proved theorems, and rules of inference, with the final step showing that q must also be true.

Example 62

Give a direct proof of the theorem "if n is an odd integer, then n^2 is odd". (An integer n is **odd** if there exists an integer k such that $n = 2k + 1$.)

Examples

Example 63

Give a direct proof that if m and n are both perfect squares, then mn is also a perfect square. (An integer a is a **perfect square** if there exists an integer b such that $a = b^2$.)

Example 64

Prove that the sum of two rational numbers is rational. (A 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**.)

Limitation of Direct Proofs

Remark

Direct proofs are useful but attempts at direct proofs sometimes lead to dead ends. There are other proof techniques. Proofs that are not direct proofs, i.e., that do not start with the hypothesis and end with the conclusion, are called **indirect proofs**. We will consider several types of indirect proofs.

Proof by Contraposition

A **proof by contraposition** makes use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive $\neg q \to \neg p$.

This means that the conditional statement $p \to q$ can be proved by showing that its contrapositive $\neg q \to \neg p$ is true.

To do so, we take $\neg q$ as a hypothesis, and using axioms, definitions, previously proved theorems, and rules of inference, we show that $\neg p$ must follow.

Remark

As a general guideline, we usually first try a direct proof. If this does not seem to go anywhere, we can try the same thing with a proof by contraposition.

Examples

Example 65

Prove that if n is an integer and $3n+2$ is odd, then n is odd.

Example 66

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Example 67

Prove that if n is an integer and n^2 is odd, then n is odd.

Proof by Contradiction

Suppose we want to prove that a statement p is true.

Furthermore, suppose we can find a proposition r such that $\neg p \to (r \wedge \neg r)$ is true.

Because $r \wedge \neg r$ is a contradiction which is false, but $\neg p \to (r \wedge \neg r)$ is true, we can conclude that $\neg p$ must be false and hence p is true.

This is called a **proof by contradiction**.

Examples

Example 68

Show that at least four of any 22 days must fall on the same day of the week.

Remark

This example is an application of the pigeonhole principle which will be covered later under the topic of combinatorics.

Example 69

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Proof by Contradiction for Conditional Statement

Remark

Proofs by contradiction can also be used to prove conditional statements. Suppose we want to prove that $p \rightarrow q$ is true. We first assume that the negation of the conclusion is true. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction. The validity of such proofs is based on the logical equivalence of $p \rightarrow q$ and $(p \wedge \neg q) \rightarrow \mathrm{F}$.

Proof by Contradiction for Conditional Statement (cont'd)

Remark

We can rewrite a proof by contraposition of a conditional statement $p \rightarrow q$ as a proof by contradiction. In a proof by contraposition, we assume that $\neg q$ is true and then show that $\neg p$ must also be true. To rewrite this proof by contraposition as a proof by contradiction, we suppose that both p and $\neg q$ are true. Then, we use the steps from the proof of $\neg q \rightarrow \neg p$ to show that $\neg p$ is true. This leads to the contradiction $p \wedge \neg p$, completing the proof.

Example 70

Give a proof by contradiction of the theorem "if $3n + 2$ is odd, then n is odd".

Proof by Contradiction for Conditional Statement (cont'd)

Remark

We can also rewrite a direct proof of a conditional statement $p \rightarrow q$ as a proof by contradiction. We assume that both p and $\neg q$ are true. From the direct proof, we can prove that q is true. Thus both q and $\neg q$ are true, leading to a contradiction. The validity of such proofs is based on the logical equivalence of $p \rightarrow q$ and $(p \wedge \neg q) \rightarrow \mathrm{F}$.

Proof by Contradiction for Biconditional Statement

Remark

To prove a theorem that is a biconditional statement of the form $p \leftrightarrow q$, we show that both $p \to q$ and $q \to p$ are true. The validity of this approach is based on the tautology

$$(p \leftrightarrow q) \leftrightarrow \big[(p \to q) \land (q \to p)\big].$$

Example 71

Prove the theorem "if n is a positive integer, then n is odd if and only if n^2 is odd".

Examples

Example 72

Show that these statements about the integer n are logically equivalent:

$$\begin{aligned} p_1 &: n \text{ is even} \\ p_2 &: n-1 \text{ is odd} \\ p_3 &: n^2 \text{ is even} \end{aligned}$$

Example 73

Show that the statement "every positive integer is the sum of the squares of two integers" is false.

Remark

To show that a statement of the form $\forall x\, P(x)$ is false, we need only find a counterexample, i.e., an example a for which $P(a)$ is false.

Proof by Cases

Sometimes it is difficult to prove a theorem using a single argument that holds for all possible cases. A useful approach is to consider different cases separately.

The validity of this approach is based on the tautology

$$\big[(p_1 \lor p_2 \lor \cdots \lor p_n) \to q\big] \leftrightarrow \big[(p_1 \to q) \land (p_2 \to q) \land \cdots (p_n \to q)\big].$$

This shows that the original conditional statement with a hypothesis made up of a disjunction of the propositions $p_1, p_2, \ldots, p_n$ can be proved by proving each of the n conditional statements $p_i \to q$, $i = 1, 2, \ldots, n$, individually.

This is known as a **proof by cases**.

Exhaustive Proof

Remark

Some theorems can be proved by examining a relatively small number of examples. A proof based on this approach is called an **exhaustive proof**, because it proceeds by exhausting all possibilities. It is a special type of proof by cases where each case involves checking a single example.

Example 74

Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Limitation of Exhaustive Proofs

Remark

People can carry out exhaustive proofs when it is necessary to check only a relatively small number of instances of a statement. Computers can handle a much larger number of instances of a statement. However, an exhaustive proof is not possible even for computers when it is impossible to list all instances to check.

Examples

Example 75

Prove that if n is an integer, then $n^2 \geq n$.

Example 76

Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers.

Example 77

Show that the equation $x^2 + 3y^2 = 8$ has no solutions in integers x and y.

Existence Proof

Definition

An **existence proof** is a proof of a proposition of the form $\exists x\, P(x)$, showing the existence of objects of a particular type.

Definition

A **constructive existence proof** of $\exists x\, P(x)$ is an existence proof which finds an element a such that $P(a)$ is true.

Existence Proof (cont’d)

Definition

A **nonconstructive existence proof** of $\exists x\, P(x)$ is an existence proof which does not find an element a such that $P(a)$ is true, but rather prove that $\exists x\, P(x)$ is true in some other way.

Remark

One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

Examples

Example 78

Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Example 79

Show that there exist irrational numbers x and y such that x^y is rational.

Uniqueness Proof

Definition

A **uniqueness proof** shows that an element with a particular property exists and that no other element has this property.

Two parts of a uniqueness proof:

Existence: Show that an element x with the desired property exists.

Uniqueness: Show that if $y \neq x$, then y does not have the desired property.

Uniqueness Proof (cont'd)

Remark

Showing that there is a unique element x such that $P(x)$ is true is equivalent to proving the statement $\exists x \left(P(x) \land \forall y \left(y \neq x \rightarrow \neg P(y)\right)\right)$.

Example 80

Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Further Remarks

Remark

Some other proof techniques will be discussed in later topics, including mathematical induction and combinatorial proofs.

Remark

We have not given a procedure that can be used for proving theorems in mathematics. In fact, it is a deep theorem of mathematical logic that such a procedure does not exist.