CS201 Discrete Math for Computer Science[1]

Qi Wang
Department of Computer Science and Engineering
Southern University of Science and Technology
Fall 2019

“All you need is a cool head, a large sheet of paper and fairly decent handwriting”

— **Anonymity**

Preface

It is the aim of these lecture notes to provide the learning materials of the one-semester course of discrete mathematics for computer science. The notes cover the main parts that the students will learn along the whole course in one semester, and will try to get the students prepared for some further courses in computer science, electronic engineering, etc.

More precisely, the notes cover logic, sets and functions, counting techniques, complexity, elementary number theory, algebraic structures, cryptography and coding, relation, graph theory. Students are strongly encouraged to do all the exercises when using these notes. This is extremely helpful for the understanding of the contents in this book.

These lecture notes will be subsequently updated to incorporate feedback and corrections from students.

Any suggestion is welcome via email: wangqi@sustech.edu.cn

Qi. Wang
December 2019

Contents

Chapter 1

Mathematical Logic and Proof

> "... mathematical logic is and must be the basis for software design.
> ... mathematical analysis of designs and specifications have become
> *central activities* in computer science research ..."
>
> — **Edsger W. Dijkstra**

Logic a basis of all mathematical reasoning, which specifies syntax of mathematical statements, the meaning of statements, and the rules of logical inference. Moreover, logic is essential to computer science: at the hardware level, the design of "logic circuits" to implement instructions is dramatically simplified by the use of symbolic logic (as you will learn in CS207 Digital Logic); at the software level, as quoted above, logic is the basis in the design of programs. A good understanding of the concepts of logic is also a prerequisite to studying a number of central areas of computer science, including databases, compilers, artificial intelligence and complexity theory, etc.

In this chapter, besides the concepts of logic, we will also learn what makes up a *correct* mathematical argument, i.e., a *proof*. Mathematical proofs are important in computer science, in terms that they are important to, for example, verify the correctness of computer programs, and show the security of a system. More surprisingly, automated reasoning systems are used to construct computer-aided proofs automatically. In the later part of this chapter, we will learn several proof methods to construct valid mathematical proofs. These methods will be utilized from time to time in this course.

1.1 Propositional logic

A ***proposition*** is a *declarative* statement that is either true or false. Typically, we use lowercase letters, such as $p, q, r, \ldots$, to represent propositions. The ***truth value*** of a proposition is true, denoted by T, if it is a true statement, and false, denote by F, if it is a false statement. Some examples of propositions are the following.

Example 1.1.1 *(1) SUSTech is located in Shenzhen.*

(2) $1 + 1 = 2$.

(3) $2 + 2 = 3$.

Since they are all "declarative" and "either true or false", they are indeed propositions, and their truth values are T, T, and F, respectively. We have also examples of non-propositions.

Example 1.1.2 *(1) No parking.*

(2) What time is it?

(3) $x + 2 = 5$.

(4) She is very talented.

The first two are not "declarative", and the last two do not have a truth value since it depends on "x" and "she", respectively. What about the following?

Example 1.1.3 *(1)* $x \cdot 0 = 0$.

(2) $x \cdot 0 = 1$.

These two are NOT propositions, even if they are declarative and are always true or false. The reason is that they both contain variables: whether a statement is a proposition or not is a *structural* property. What about the following?

Example 1.1.4 *(1) There are infinitely many twin prime numbers.*

(2) There are other life forms on other planets in the universe.

These two are both propositions, even if we do not know their truth values for now. Anyhow, they are declarative, and are either true or false.

1.1.1 Logical connectives

Propositions by themselves are atomic and elementary. We can build more complex propositions by various **logical connectives**. The new propositions are called **compound propositions** or **propositional functions**, and the propositions that form a propositional function are called the ***propositional variables***. Here we introduce six logical connectives, namely, *negation, conjunction, disjunction, exclusive or, implication*, and *biconditional.*

The ***negation*** of a proposition p, denoted by $\neg p$, is the proposition "*not* p", or equivalently "it is not the case that p". The truth table of $\neg p$ is as below. Note that a **truth table** displays the relationships between the truth values of propositions, whose rows contain *all* possible values of elementary propositions.

p	$\neg p$
T	F
F	T

Example 1.1.5 *Consider the proposition p: SUSTech is located in Shenzhen, whose truth value is T. Then the negation of p is ¬p: SUSTech is* not *located in Shenzhen, or equivalently, It is* not the case *that SUSTech is located in Shenzhen.*

Some other negation examples include "$5 + 2 \neq 8$", "10 is not a prime number.", "It is not the case that class begins at 8am", etc.

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 proposition is defined to be true only when both p and q are true and is false otherwise. The **disjunction** of p and q, denoted by $p \vee q$, is the proposition p *or* q. Note that here the 'or' is used in an inclusive way. The proposition is false only when both p and q are false, otherwise it is true. Now we give the truth tables of both $p \wedge q$ and $p \vee q$.

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

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 of the exclusive or is displayed below.

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

Example 1.1.6 *(1) Construct a truth table for $(p \oplus q) \oplus r$.*

(2) Construct a truth table for $p \oplus p$.

Solution.

(1)

p	q	r	$p \oplus q$	$(p \oplus q) \oplus r$
T	T	T	F	T
T	T	F	F	F
T	F	T	T	F
T	F	F	T	T
F	T	T	T	F
F	T	F	T	T
F	F	T	F	T
F	F	F	F	F

(2)

p	$p \oplus p$
T	F
F	F

□

Now we talk about the most important logical connective for proofs: implication. An **implication** represents an "if …then …" claim, denoted by $p \to q$ or $p \Rightarrow q$ for two propositions p and q. In this case, p is called the **hypothesis**, and q is called the **conclusion**. In English, $p \to q$ is usually rendered in various ways: "If p, then q", "p implies q", "p is *sufficient* for q", "q is *necessary* for p", "q follows from p", "q unless $\neg p$", "p only if q". The implication $p \to q$ is true provided that (a) p is false (in which case all bets are off), or (b) q is true. In other words, $p \to q$ is false only when p is true and q is false. The truth table of $p \to q$ is the following.

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

The **converse** of $p \to q$ is the proposition $q \to p$. The **inverse** of $p \to q$ is the proposition $\neg p \to \neg q$. The **contrapositive** of $p \to q$ is the proposition $\neg q \to \neg p$.

The **biconditional** proposition of p and q, denoted by $p \leftrightarrow q$, is the propositional function that is true when both p and q have the same truth values and false if p and q have opposite truth values. The compound proposition $p \leftrightarrow q$ also reads: "p if and only if q", or "p is necessary and sufficient for q", or "if p then q, and conversely". The truth table of $p \leftrightarrow q$ is the following.

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

1.1.2 Logical equivalence

Two propositions are **logically equivalent** if they have exactly the same truth values under all circumstances. We write $p \equiv q$. A compound proposition that is *always true* for all possible truth values is called a **tautology**, and that is *always false* for all possible truth values is called a **contradiction**. A compound proposition that is neither a tautology nor a contradiction is called a **contingency**. Easy examples of a tautology and a contradiction are provided by $p \vee \neg p$ and $p \wedge \neg p$, as shown by the following truth table.

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

To motivate our study on logical equivalence, we look at the following example. There are two pieces of codes taken from different version of *Mergesort*. Do they do the same thing?

(1) if $((i+j \le p+q)\ \&\&\ (i \le p)\ \&\&\ ((j > q)\ \vert\vert\ (\mathit{List}1[i] \le \mathit{List}2[j])))$	(1) if $(((i+j \le p+q)\ \&\&\ (i \le p)\ \&\&\ (j > q))\ \vert\vert\ ((i+j \le p+q)\ \&\&\ (i \le p)\ \&\&\ (\mathit{List}1[i] \le \mathit{List}2[j])))$
(2) $\quad \mathit{List}3[k] = \mathit{List}1[i]$	(2) $\quad \mathit{List}3[k] = \mathit{List}1[i]$
(3) $\quad i = i+1$	(3) $\quad i = i+1$
(4) else	(4) else
(5) $\quad \mathit{List}3[k] = \mathit{List}2[j]$	(5) $\quad \mathit{List}3[k] = \mathit{List}2[j]$
(6) $\quad j = j+1$	(6) $\quad j = j+1$
(7) $k = k+1$	(7) $k = k+1$

For simplicity, let's rewrite the atomic propositions: $s-(i+j \le p+q)$, $t-(i \le p)$, $u-(j > q)$, and $v-(\mathit{List}1[i] \le \mathit{List}2[j])$. Then it suffices to answer whether the following two are equivalent or not.

$$(1)\ s \wedge t \wedge (u \vee v) \qquad (1')\ (s \wedge t \wedge u) \vee (s \wedge t \wedge v)$$

We further set $w-(s \wedge t)$, then we consider the following two compound propositions.

$$(1)\ w \wedge (u \vee v) \qquad (1')\ (w \wedge u) \vee (w \wedge v)$$

By comparing the truth tables of the two compound propositions (left as an exercise), we conclude that the two propositions $w \wedge (u \vee v)$ and $(w \wedge u) \vee (w \wedge v)$ are logically equivalent. Alternatively, two propositions p and q are **logically equivalent** if $p \leftrightarrow q$ is a tautology. Equivalent statements are important for logical reasoning since they can be substituted and can help us make a logical argument and further infer new propositions.

Example 1.1.7 *(1) Show that* $\neg(p \vee q) \equiv \neg p \wedge \neg q$

(2) Show that $\neg(p \wedge q) \equiv \neg p \vee \neg q$

(3) Show that $\neg(\neg p) \equiv p$

Note that the first two in Example 1.1.7 are referred to as **De Morgan's laws**, and the third one is called **Double negation law**.

Example 1.1.8 *(1) Show that $p \wedge q \equiv q \wedge p$ and $p \vee q \equiv q \vee p$ (**Commutative laws**)*

*(2) Show that $(p \vee q) \vee r \equiv p \vee (q \vee r)$ and $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ (**Associative laws**)*

*(3) Show that $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ and $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$ (**Distributive laws**)*

Example 1.1.9 *Show that $p \to q \equiv \neg q \to \neg p$.*

Solution. We use De Morgan's laws as follows.

$$\begin{array}{rcll} p \to q & \equiv & \neg p \vee q & \text{Useful law} \\ & \equiv & q \vee \neg p & \text{Commutative law} \\ & \equiv & \neg\neg q \vee \neg p & \text{Double Negation law} \\ & \equiv & \neg q \to \neg p. & \text{Useful law} \end{array}$$

□

1.1.3 Rules of inference for propositional logic

The main concern of logic is how the truth of some propositions is connected with the truth of another. An ***argument*** is a set of two or more propositions related to each other in such a way that all but one of them (the **premises**) are supposed to provide support for the remaining one (the **conclusion**). The transition from premises to conclusion is the so-called ***inference*** upon which the argument relies.

Suppose that the premises of an argument are all true. Then the conclusion may be either true or false. When the conclusion is true, then the argument is said to be ***valid***, otherwise, the argument is called ***invalid***. To check an argument for validity one proceeds as follows.

(i) Identify the premises and the conclusion of the argument.

(ii) Construct a truth table including the premises and the conclusion.

(iii) Find rows in which all premises are true.

(iv) In each row of Step (iii), if the conclusion is true then the argument is valid; otherwise the argument is invalid.

Example 1.1.10 *Show that the argument*

$$\begin{array}{rl} & p \to q \\ & q \to p \\ \therefore & p \vee q \end{array}$$

Solution. We construct the truth table as follows.

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

From the last row we see that the premises are true but the conclusion is false. The argument is then invalid. □

Example 1.1.11 (Modus Ponens) *Show that the argument*

$$\begin{array}{ll} & p \to q \\ & p \\ \therefore & q \end{array}$$

is valid.

Solution. The truth table is as follows.

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

The first row shows that the argument is valid. □

Example 1.1.12 (Modus Tollens) *Show that the argument*

$$\begin{array}{ll} & p \to q \\ & \neg q \\ \therefore & \neg p \end{array}$$

is valid.

Solution. The truth table is as follows.

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

The last row shows that the argument is valid. □

Example 1.1.13 (Disjunctive Addition) *Show that the argument*

$$\begin{array}{rl} & p \\ \therefore & p \vee q \end{array}$$

is valid.

Solution. The truth table is as follows.

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

The first and second rows show that the argument is valid. □

Example 1.1.14 (Conjunctive Addition) *Show that the argument*

$$\begin{array}{rl} & p,\ q \\ \therefore & p \wedge q \end{array}$$

is valid.

Example 1.1.15 (Conjunctive Simplification) *Show that the argument*

$$\begin{array}{rl} & p \wedge q \\ \therefore & p \end{array}$$

is valid.

Example 1.1.16 (Disjunctive Syllogism) *Show that the argument*

$$\begin{array}{rl} & p \vee q \\ & \neg q \\ \therefore & p \end{array}$$

is valid.

Example 1.1.17 (Hypothetical Syllogism) *Show that the argument*

$$\begin{array}{rl} & p \to q \\ & q \to r \\ \therefore & p \to r \end{array}$$

is valid.

Example 1.1.18 (Rule of Contradiction) *Show that if c is a contradiction then the following argument is valid for any p.*

$$\begin{array}{ll} & \neg p \to c \\ \therefore & p \end{array}$$

1.2 Predicate logic

Using only propositional logic, we are able to express an argument like:

- 3 is an integer.
- If 3 is an integer, then 3^2 is no smaller than 0.
- Therefore, 3^2 is no smaller than 0.

This is an application of the inference rule called **modus ponens**, which says that from p and $p \to q$, we can deduce q. The first two statements are premises (meaning we are given them as true without proof), and the last is the conclusion of the argument. But what if we encounter other integers? In fact, what we would like is a general way to express the property that the square of any integer is no smaller than 0. With just propositional logic, we *cannot* write this fact down.

1.2.1 Variables and quantifiers

A ***predicate*** is an expression involving one or more variables defined on some domain, called the ***domain of discourse*** or ***universe***. Substitution of a particular value for the variables produces a proposition which is either true or false. For instance, "$P(n)$: n is prime" is a predicate on the natural numbers. Observe that $P(1)$ is false, $P(2)$ is true. In the expression $P(x)$, x is called a ***variable***. As the variable x varies, the truth value of $P(x)$ varies as well. The set of true values of a predicate $P(x)$ is called the **truth set** and will be denoted by T_P.

Example 1.2.1 *Let $Q(x, y) : x = y + 3$ with domain the collection of natural numbers. What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?*

Solution. By substitution in the expression of Q we find: $Q(1, 2)$ is false since $1 = x \neq y + 3 = 5$. On the contrary, $Q(3, 0)$ is true since $x = 3 = 0 + 3 = y + 3$. □

Besides substitutions of the variable(s), another way to generate propositions is by **quantifiers**. For example, $\forall x \in D\ P(x)$ is a proposition which is true if $P(x)$ is true for all values of x in the domain D of P. For example, if k is an nonnegative integer, then the predicate $P(k) :\ 2k$ is even is true for all $k \in \mathbb{N}$. We write

$$\forall k \in \mathbb{N},\ 2k \text{ is even.}$$

The symbol $\forall$ is called the **universal quantifier**. The proposition $\forall x \in D\ P(x)$ is false if $P(x)$ is false for at least one value of x. In this case x is called a ***counterexample***.

Example 1.2.2 *Show that the proposition* $\forall x \in \mathbb{R}\ x > \frac{1}{x}$ *is false.*

Solution. A counterexample is $x = \frac{1}{2}$. Clearly, $\frac{1}{2} < 2 = \frac{1}{\frac{1}{2}}$. □

Example 1.2.3 *Write in the form* $\forall x \in D\ P(x)$ *the proposition "Every real number is either positive, negative or* 0*."*

Solution. $\forall x \in \mathbb{R}\ x > 0,\ x < 0,\ \text{or } x = 0.$ □

The notation $\exists x \in D\ P(x)$ is a proposition that is true if there is at least one value of $x \in D$ where $P(x)$ is true; otherwise it is false. The notation $\exists$ is called the **existential quantifier**.

Example 1.2.4 *Let* $P(x)$ *denote the statement "*$x > 3$*". What is the truth value of the proposition* $\exists x \in \mathbb{R}\ P(x)$*.*

Solution. Since $4 \in \mathbb{R}$ and $4 > 3$, the given proposition is true. □

Given a predicate in more than one variables we can quantify each (or some) of the variables. For example, the statement "For every real number x and y, it holds that $x^2 - y^2 = (x - y)(x + y)$" can be formalized as

$$\forall x, y \in \mathbb{R}\ x^2 - y^2 = (x - y)(x + y).$$

Somewhat more interestingly, the statement "There is no greatest integer" might be formulated as

$$\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z}\ m > n.$$

It is *crucial* to note that the meaning of a statement may change if the existential and universal quantifiers are exchanged. For example, $\exists m \in \mathbb{Z}\ \forall n \in \mathbb{Z}\ m > n$ means that "There is an integer strictly greater than all integers." This is not only contrary to the meaning of the original statement, but is patently wrong as it asserts in particular that there is an integer that is strictly greater than itself. Exchanging the order of two quantifiers of the same type (either universal or existential) does not change the truth value of a statement.

1.2.2 Negations

For propositions with quantifiers and variables, the following logical equivalences hold:

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

These are essentially the quantified version of De Morgan's laws: the first says that if you want to show that not all x such that $P(x)$, it is equivalent to finding some x such that not $P(x)$; The second says that to show that no x such that $P(x)$, you have to show that all x are such that not $P(x)$.

Example 1.2.5 *What is the negation of the proposition $\forall x\ P(x) \to Q(x)$?*

Solution. Since $P(x) \to Q(x) \equiv \neg P(x) \vee Q(x)$, we have $\neg(\forall x\ (P(x) \to Q(x))) \equiv \exists x\ (P(x) \wedge \neg Q(x))$. □

Example 1.2.6 *Write the negation of each of the following propositions.*

(1) $\forall x \in \mathbb{R}\ x > 3 \to x^2 > 9$.

(2) Every polynomial function is continuous.

(3) There exists a triangle with the property that the sum of angles is greater than $180°$.

Solution.

(1) $\exists x \in \mathbb{R}\ x > 3 \wedge x^2 \leq 9$.

(2) There exists a polynomial that is not continuous everywhere.

(3) For any triangle, the sum of the angles is less than or equal to $180°$.

□

Next we discuss predicates that contain multiple quantifiers. A typical example is the definition of a limit. We say that $L = \lim_{x\to a} f(x)$ if and only if $\forall \epsilon > 0$, $\exists$ a positive number δ such that if $|x - a| \leq \delta$ then $|f(x) - L| < \epsilon$.

Example 1.2.7 *Find the negation of the following propositions.*

(1) $\forall x \exists y\ P(x, y)$

(2) $\exists x \forall y\ P(x, y)$

Solution.

(1) $\exists x \forall y\ \neg P(x, y)$

(2) $\forall x \exists y\ \neg P(x, y)$

□

1.2.3 Arguments with quantified premises

In this section, we discuss three types of valid arguments that involve the universal quantifiers. The rule of **universal instantiation** is:

$$\begin{array}{lr} & \forall x \in D\ P(x) \\ & a \in D \\ \therefore & P(a) \end{array}$$

Example 1.2.8 *Use universal instantiation to fill in valid conclusion for the following argument. All positive integers are greater than or equal to* 1*.* 3 *is a positive integer. Therefore,* $3 \geq 1$*.*

The rule of **universal modus ponens** is:

$$\begin{array}{lr} & \forall x \in D\ P(x) \to Q(x) \\ & P(a) \text{ for some } a \in D \\ \therefore & Q(a) \end{array}$$

Example 1.2.9 *Use the rule of the universal modus ponens to fill in valid conclusion for the following argument.*

$\forall n \in \mathbb{N}$*, if* $n = 2k$ *for some* $k \in \mathbb{N}$ *then* n *is even.* $0 = 2 \cdot 0$*. Therefore,* 0 *is even.*

The rule of **universal modus tollens** is:

$$\begin{array}{lr} & \forall x \in D\ P(x) \to Q(x) \\ & \neg Q(a) \text{ for some } a \in D \\ \therefore & \neg P(a) \end{array}$$

Example 1.2.10 *Use the rule of the universal modus tollens to fill in valid conclusion for the following argument.*

All healthy people eat an apple per day. Bob does not eat an apple a day. Therefore, Bob is not healthy.

The rule of **universal generalization** is:

$$\begin{array}{lr} & P(c) \text{ for an arbitrary } c \\ \therefore & \forall x P(x) \end{array}$$

The rule of **existential instantiation** is:

$$\begin{array}{lr} & \exists x P(x) \\ \therefore & P(c) \text{ for some } c \end{array}$$

The rule of **existential generalization** is:

$$\begin{array}{ll} & P(c) \text{ for some } c \\ \therefore & \qquad \exists x P(x) \end{array}$$

Example 1.2.11 *Given the two premises: “A student in this class has not read the book.” “Everyone in this class passed the first exam.” Show that these lead to a conclusion that “Someone who passed the first exam has not read the book.*

Proof. Let $C(x), B(x), P(x)$ denote x is in this class, x has read the book, and x passed the first exam, respectively. Then we are able to translate the two premises as $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \to P(x))$. The conclusion is $\exists x(P(x) \wedge \neg B(x))$. Then we have

Step	Reason
(1) $\exists x(C(x) \wedge \neg B(x))$	Premise
(2) $C(a) \wedge \neg B(a)$	E.I. from (1)
(3) $C(x)$	Simplification from (2)
(4) $\forall x(C(x) \to P(x))$	Premise
(5) $C(a) \to P(a)$	U.I. from (4)
(6) $P(a)$	M.P. from (3) and (5)
(7) $\neg B(a)$	Simplification from (2)
(8) $P(a) \wedge \neg B(a)$	Conj from (6) and (7)
(9) $\exists x(P(x) \wedge \neg B(x))$	E.G. from (8)

□

1.3 Mathematical proof

In this chapter we discuss some common methods of mathematical proofs together with some standard terminologies.

A **mathematical system** consists of axioms, definitions, and undefined terms. An **axiom** is a statement that is assumed to be true. A **definition** is used to create new concepts in terms of existing ones. A **theorem** is a proposition that has been proved to be true. A **lemma** is a theorem that is usually not interesting in its own right but is useful in proving another theorem. A **corollary** is a theorem that follows quickly from a theorem.

Example 1.3.1 *The Euclidean geometry furnishes an example of mathematical system:*

- *points and lines are examples of undefined terms.*
- *An example of a definition: Two angles are supplementary if the sum of their measures is* $180°$*.*
- *An example of an axiom: Given two distinct points, there is exactly one line that contains them.*
- *An example of a theorem: If two sides of a triangle are equal, then the angles opposite them are equal.*
- *An example of a corollary: If a triangle is equilateral, then it is equiangular.*

1.3.1 Direct proof

An argument that establishes the truth of a theorem is called a ***proof***. **Logic** is a powerful tool for the analysis of proofs. First we discuss for proving a theorem of the form "$\exists x$ such that $P(x)$." This theorem guarantees the existence of at least one x for which the predicate $P(x)$ is true. The proof of such a theorem is usually *constructive*: the proof is either by finding a particular x that makes $P(x)$ true or by exhibiting an algorithm for finding x.

Example 1.3.2 *Show that there exists a positive integer whose square can be written as the sum of the squares of two positive integers.*

Proof. One example is $5^2 = 3^2 + 4^2$. □

By a *nonconstructive existence proof* we mean a method that involves either showing the existence of x using a proved theorem (or axioms) or the assumption that there is no such x leads to a contradiction. The disadvantage of nonconstructive method is that it may give virtually no clue about where or how to find x. Theorems are often of the form $\forall x \in D$ if $P(x)$ then $Q(x)$." We call $P(x)$ the **hypothesis** and $Q(x)$ the **conclusion**. We consider a proposition of the form $\forall x \in D\ P(x)$, which can be written as "$\forall x$, if $x \in D$ then $P(x)$. If D is a finite set, then one checks the truth value of $P(x)$ for each $x \in D$. This method is called the *method of exhaustion*.

Example 1.3.3 *Show that for each integer* $1 \leq n \leq 10$, $n^2 - n + 11$ *is a prime number.*

Proof. The given proposition can be written in the form "$\forall x in \mathbb{N}$, if $1 \leq n \leq 10$ then $P(n)$ is prime" where $P(n) = n^2 - n + 11$. Using the method of exhaustion we see that $P(1) = 11; P(2) = 13, P(3) = 17, P(4) = 23, P(5) = 31, P(6) = 41, P(7) = 53, P(8) = 67, P(9) = 83, P(10) = 101$. □

The most powerful technique for proving a universal proposition is one that works regardless of the size of the domain over which the proposition is quantified. It is called the *method of generalizing from the generic particular*. By a direct method of proof, we mean a method that consists of showing that if $P(x)$ is true for $x \in D$ then $Q(x)$ is also true.

Example 1.3.4 *For all* $m, n \in \mathbb{Z}$, *if* m, n *are both even, then so is* $m + n$.

Proof. Let m and n be two even integers. Then there exist integers k_1 and k_2 such that $n = 2k_1$ and $m = 2k_2$. We must show that $m + n$ is even, that is, an integer multiple of 2. Indeed, $m + n = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k$, where $k = k_1 + k_2 \in \mathbb{Z}$. Thus, by the definition of even, $m + n$ is even. □

Example 1.3.5 *If* $a, b \in \mathbb{Q}$, *then* $a + b \in \mathbb{Q}$.

Proof. Let a and b be two rational numbers. Then there exist integers $a_1, a_2, b_1 \neq 0$ and $b_2 \neq 0$ such that $a = \frac{a_1}{b_1}$ and $b = \frac{a_2}{b_2}$. By the property of addition of two fractions we have

$$a + b = \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

By letting $p = a_1 b_2 + a_2 b_1 \in \mathbb{Z}$ and $q = b_1 b_2 \in \mathbb{Z}^*$, we get $a + b = ı q$, which means that $a + b \in \mathbb{Q}$. □

Finally, to show a proposition of the form $\forall x \in D$, if $P(x)$ then $Q(x)$ is false, it suffices to find an element $x \in D$ where $P(x)$ is true but $Q(x)$ is false. Such an x is called a **counterexample**.

Example 1.3.6 *Disprove the proposition* $\forall a, b \in \mathbb{R}$, *if* $a < b$ *then* $a^2 < b^2$.

Proof. A counterexample is: let $a = -2$ and $b = -1$. Then $a < b$ but $a^2 > b^2$. □

1.3.2 Proof by contradiction and by contrapositive

Recall that in a direct proof one starts with the hypothesis of an implication $p \to q$ and then proves that the conclusion is true. Any other method of proof will be referred to as an ***indirect proof***. In this section, we study two methods of indirect proofs, namely, proof by contradiction and proof by contrapositive.

Proof by contradiction: We want to show that p is true. We assume it is not and therefore $\neg p$ is true and then derive a contradiction. By the rule of contradiction discussed in logic, p must be true.

Example 1.3.7 *If n^2 is an even integer, then n must be even.*

Proof. Suppose to the contrary that n is not even, which means that n is odd. Then there is an integer k such that $n = 2k+1$. In this case, $n^2 = 2(2k^2+2k)+1$ is odd and this contradicts the assumption that n^2 is even. Hence, n must be even. □

Example 1.3.8 *The number $\sqrt{2}$ is irrational.*

Proof. Suppose not, then $\sqrt{2}$ is rational. Then there exist two integers m and n with no common divisors such that $\sqrt{2} = \frac{m}{n}$. Squaring both sides of this equality we find that $2n^2 = m^2$. Thus, m^2 is even. By Example 1.3.7, m is even. That is, $m = 2k$ for some integer k. Taking the square we find that $2n^2 = m^2 = 4k^2$, that is $n^2 = 2k^2$. This says that n^2 is even and again n is also even. But, this contradicts to our assumption that m and n have no common divisors. Hence, $\sqrt{2}$ must be irrational. □

Example 1.3.9 *There are infinitely many prime numbers.*

Proof. Suppose not, i.e., the set of prime numbers is finite. Then these prime numbers can be listed, say, $p_1, p_2, \ldots, p_n$. Now, consider the integer $N = p_1 p_2 \cdots p_n + 1$. Since for all $1 \le i \le n$, p_i does not divide N, we get that N is prime. However, N is not contained in the set of prime numbers. This leads to a contradiction. □

Proof by contrapositive: We already know that $p \to q \equiv \neg q \to \neg p$. So to prove $p \to q$, we instead prove $\neg q \to \neg p$.

Example 1.3.10 *If n is an integer such that n^2 is odd then n is also odd.*

Proof. Suppose that n is an integer that is even. Then there exists an integer k such that $n = 2k$. But then $n^2 = 2(2k^2)$ which is even. □

1.3.3 Proof by cases

The method of **proof by cases** is a direct method of proving the conditional proposition $p_1 \vee p_2 \vee \cdots \vee p_n \to q$. The method consists of proving the conditional propositions $p_1 \to q$, $p_2 \to q$, $\cdots$, $p_n \to q$.

Example 1.3.11 *Show that if n is a positive integer then $n^3 + n$ is even.*

Solution. We use the method of proof by cases.

Case 1. Suppose that n is even. Then there is $k \in \mathbb{N}$ such that $n = 2k$. In this case, $n^3 + n = 8k^3 + 2k = 2(4k^3 + k)$ which is even.

Case 2. Suppose that n is odd. Then there is a $k \in \mathbb{N}$ such that $n = 2k + 1$. So, $n^3 + n = 2(4k^3 + 6k^2 + 4k + 1)$ which is even. □

Example 1.3.12 *Use the proof by cases to prove the triangle inequality: $|x + y| \leq |x| + |y|$.*

Proof. Case 1. $x \geq 0$ and $y \geq 0$. Then $x+y \geq 0$ and so $|x+y| = x+y = |x|+|y|$.

Case 2. $x \geq 0$ and $y < 0$. Then $x+y < x+0 < |x| \leq |x|+|y|$. On the other hand, $-(x+y) = -x+(-y) \leq 0+(-y) = |y| \leq |x|+|y|$. Thus, if $|x+y| = x+y$ then $|x+y| < |x|+|y|$ and if $|x+y| = -(x+y)$ then $|x+y| \leq |x|+|y|$.

Case 3. The case $x < 0$ and $y \geq 0$ is similar to Case 2.

Case 4. Suppose $x < 0$ and $y < 0$. Then $x + y < 0$ and therefore $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$.

So in all four cases $|x + y| \leq |x| + |y|$. □

1.3.4 More methods of proofs

A **vacuous proof** is a proof of an implication $p \to q$ in which it is shown that p is false.

Example 1.3.13 *Let $P(n)$ denote "if $n > 1$ then $n^2 > n$". Show that $P(0)$.*

Proof. Since the premise $0 < 1$ is always false. Thus $P(0)$ is true. □

A **trivial proof** of an implication $p \to q$ is one in which q is shown to be true without any reference to p.

Example 1.3.14 *Show that if n is an even integer then n is divisible by 1.*

Proof. Since the proposition n is divisible by 1 is always true, the given implication is trivially true. □