What is discrete mathematics?

Discrete mathematics is devoted to the study of **discrete** or distinct unconnected objects.

Classical mathematics deals with functions on real numbers.
Real numbers form a continuous line.
Some calculus techniques apply only to continuous functions.

Dealing with discrete objects requires techniques different from classical mathematics.

Motivation to study discrete mathematics

Computers typically work with discrete information. Examples:

bits
integers
letters
employee records
passwords

This is why a course in Discrete mathematics is standard in Computer Science or Software Engineering programmes.

Applications of discrete mathematics

The techniques of discrete mathematics help us solve many kinds of problems. For example:

- What is the shortest route to go from point A to point B given a map marked with all distances between points?
- How many different ways are there of choosing a valid password in a system?
- What is the most efficient way to multiply a given sequence of matrices?
- How should you schedule a given collection of tasks on a set of computers, so that all tasks finish as soon as possible?

Applications of discrete mathematics

Discrete mathematics provides the foundations for many fields:

1. Computer security and cryptography.
2. Automata theory: the theory behind compilers.
3. Algorithms and data structures.
4. Database theory.
5. Routing and other problems in computer networks.
6. Scheduling theory.

Logic

Logic deals with the methods of reasoning. The rules of logic give precise meaning to mathematical statements.

It deals with objects having two values.

true .... **T** **1**
false .... **F** **0**

We call these values **truth values**.

Proposition or Statement
A declarative sentence which is either true or false but not both. (We say its **truth value** is either **T** or **F**.)

Examples of propositions

Montreal is a city in Canada ..... truth value is T.

Concordia is located near a metro station .... truth value is T.

$7 < 4$ ... truth value is F.

Examples of things that are **not** propositions

Don't do that! .... not a declarative sentence.

What is the time? ... not a declarative sentence.

$x < 4$ ... truth value depends on x.

Compound propositions

Propositions obtained from other propositions using **logical operators** or **connectives**.

We give names to propositions, such as p, q, r, ...

Examples:

p: It is raining today.

q: Montreal is the capital of Canada.

r: $2 + 3 = 5$.

Propositions can be combined using logical connectives, such as **negation, or, and**, etc.

Logical operators

negation of *p*

It is not the case that p
$\neg p$

If the proposition p is true then the negation of p is false.
If the proposition p is false then the negation of p is true.

Example:
p: It is raining today.

$\neg p$: It is not the case that it is raining today.
or
It is not raining today.

Truth tables

We use a **truth table** to show the truth values of compound propositions in terms of the component parts.

p	$\neg$ p
T	F
F	T

The truth table of negation.

Disjunction

$p \vee q$ (p or q)
is true only if at least one of p, q is true
(also known as *inclusive or*).

Example: *q:* Montreal is the capital of Canada.

r: $2+3=5$.

$q \vee r$: Montreal is the capital of Canada or $2+3=5$.

---

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

Conjunction

$p \wedge q$ (p and q)
is true only if both p, q are true.

Example: p: It is raining.

q: It is dark outside.

$p \wedge q$: It is raining and it is dark outside.

---

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

Exclusive or

$p \oplus q$ (p exclusive or q)
is true only if exactly one of p, q is true and the other is false.

Example: *p:* I will have soup.

q: I will have salad.

$p \oplus q$: I will have soup or salad but not both.

---

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

Classroom exercise:

Conditional

$p \rightarrow q$ (if p then q)
is false only when p is true and q is false.

p is called the **hypothesis** or **antecedent**
and q is called the **conclusion** or **consequence**.

Example: $p \rightarrow q$: If today is Monday, then I have to go to school.

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

Biconditional

$p \leftrightarrow q$ (p if and only if q)
is true only if p, q have the same truth values.

Example:

$q \leftrightarrow r$: I go to school if and only if the weather is good.

---

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

The conditional $p \rightarrow q$ can be expressed in English in many ways:

if p then q

p implies q

p only if q

p is sufficient for q

q is necessary for p

q if p

q whenever p

Classroom exercise:

Propositional Equivalences

Definitions

A **tautology**
is a compound proposition that is **true**
for all truth values of the propositions in it.
Example: $p \vee \neg p$

A **contradiction**
is a compound proposition that is **false**
for all truth values of the propositions in it.
Example: $p \wedge \neg p$

A **contingency**
is a proposition which is neither a tautology nor a contradiction.
Example: $p \vee q$

Logical equivalence

Two compound propositions p, q are **logically equivalent** if they have the same truth table.

$$p \equiv q$$

Definition
Two compound propositions p, q are
logically equivalent if $p \longleftrightarrow q$ is a tautology.

Example 1: Is the proposition $p \longrightarrow q$ logically equivalent to the proposition $\neg p \vee q$?

p	q	¬ p	a ¬ p ∨ q	b p ⟶ q	a ↔ b
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Thus,

$$p \longrightarrow q \equiv \neg p \vee q$$

Example 2: Are the compound propositions $(p \rightarrow q) \wedge (q \rightarrow p)$ and $p \leftrightarrow q$
logically equivalent?

p	q	a $p \rightarrow q$	b $q \rightarrow p$	$a \wedge b$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Conclusion:

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

Example 3: Show that
$(p \wedge q) \vee (\neg p \wedge \neg q) \equiv p \leftrightarrow q$.

p	q	a $\neg$ p	b $\neg$ q	c p $\wedge$ q	d a $\wedge$ b	c $\vee$ d	p $\leftrightarrow$ q
T	T	F	F	T	F	T	T
T	F	F	T	F	F	F	F
F	T	T	F	F	F	F	F
F	F	T	T	F	T	T	T

Conclusion:

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

Example 4: Using truth tables, determine whether the following proposition is a tautology, contradiction or a contingency.

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

			A	B	C	D	
p	q	r	p $\to$ q	p $\to$ r	A $\to$ r	A $\land$ B	C $\leftrightarrow$ D
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	F
T	F	F	F	F	T	F	F
F	T	T	T	T	T	T	T
F	T	F	T	T	F	T	F
F	F	T	T	T	T	T	T
F	F	F	T	T	F	T	F

Since the last column contains both T's and F's, it is a contingency.

Example 5:

$$((\neg(q \rightarrow p)) \wedge \neg r) \stackrel{?}{\equiv} (\neg p \vee (\neg q \vee r))$$

			A	B	C	D	H	G	I	J
p	q	r	q $\rightarrow$ p	$\neg$ r	$\neg$ A	C $\wedge$ B	$\neg$ p	$\neg$ q	$\neg$ q $\vee$ r	H $\vee$ I
T	T	T	T	F	F	F	F	F	T	T
T	T	F	T	T	F	F	F	F	F	F
T	F	T	T	F	F	F	F	T	T	T
T	F	F	T	T	F	F	F	T	T	T
F	T	T	F	F	T	F	F	F	T	T
F	T	F	F	T	T	T	T	F	F	T
F	F	T	T	F	F	F	T	T	T	T
F	F	F	T	T	F	F	T	T	T	T

No!

Basic logical equivalences

equivalence	law
$p \wedge T \equiv p$	Identity
$p \vee F \equiv p$	
$p \vee T \equiv T$	Domination
$p \wedge F \equiv F$	
$p \vee p \equiv p$	Idempotent
$p \wedge p \equiv p$	
$\neg(\neg p) \equiv p$	Double negation
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive
$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$	de Morgan

Other useful equivalences

$$\text{Negation laws}: \begin{cases} (\neg p) \vee p \equiv T \\ (\neg p) \wedge p \equiv F \end{cases}$$

$$\text{Absorption laws}: \begin{cases} p \wedge (p \vee q) \equiv p \\ p \vee (p \wedge q) \equiv p \end{cases}$$

A proof of the last equivalence:

$p \vee (p \wedge q)$

$\equiv (p \wedge T) \vee (p \wedge q)$ identity law

$\equiv p \wedge (T \vee q)$ distributive law

$\equiv p \wedge T$ domination law

$\equiv p$ identity

Use brackets to avoid ambiguity!

Classroom exercise:

Contrapositive, converse and inverse

Consider the proposition $p \rightarrow q$.

$q \rightarrow p$ is called the **converse of** $p \rightarrow q$

$\neg q \rightarrow \neg p$ is called the **contrapositive of** $p \rightarrow q$

$\neg p \rightarrow \neg q$ is called the **inverse of** $p \rightarrow q$

Example: If you are a Computer Science student, you can take COMP 232.

Contrapositive: If you cannot take COMP 232, you are not a Computer Science student.

Converse: If you can take COMP 232, you are a Computer Science student.

Inverse: If you are not a Computer Science student, you cannot take COMP 232.

The proposition $p \rightarrow q$ is logically equivalent to its contrapositive $\neg q \rightarrow \neg p$.

$p \rightarrow q$
$\equiv \neg p \vee q$ (Example 1 above)
$\equiv q \vee \neg p$ (commutative law)
$\equiv \neg(\neg q) \vee \neg p$ (double negation law)
$\equiv \neg q \rightarrow \neg p$ (Example 1 above)

However, neither the inverse nor the converse of $p \rightarrow q$ is logically equivalent to it.

Everyone should know:

the definition of a

proposition, tautology, contradiction, contingency,

all **logical operations**,

basic **logical equivalences**,

how to **construct** a **truth table**,

how to **use** logical equivalences.

Predicates and Quantifiers

Statements involving variables, like

$x^2 \geq x + 2$

"The American city is polluted."

are not propositions, since their truth values depend on the values of the variable involved.

For what value of x?

Which city?

Nevertheless, we sometimes wish to make general statements:

"All American cities are polluted."

"Some cats do not chase mice."

For this, we need to introduce new terminology.

Predicates

Consider a statement involving an integer variable:

$x^2 \geq x + 2$

Here x is the **variable**
and $x^2 \geq x + 2$, the **predicate**, is a property of x.

We denote $x^2 \geq x + 2$ by $P(x)$.

P is called a **propositional function**,
its value depends on the value assigned to x.

$P(x) \equiv x^2 > x + 2.$

Assigning a specific value to x in $P(x)$ yields a proposition.

$P(0) \equiv 0 \geq 0 + 2$ false

$P(5) \equiv 25 \geq 5 + 2$ true

$P(-10) \equiv 100 \geq -10 + 2$ true

Quantifiers

Another way to make a proposition out of a propositional function is to use statements about *how general the validity of a propositional function is*.

This method is called **quantification.**

For the predicate $P(x)$, the **universe of discourse** specifies all possible values of x.

We study **universal quantification**

and **existential quantification**.

Universal quantification of $P(x)$

$\forall x \, P(x)$

Read $\forall x$ as **For All** x.

True when $P(x)$ is true for all values of x in the univ. of discourse.

Example 1: When the universe of discourse is integers
$\forall x \ (x^2 \geq x + 2)$
is a false proposition since $0^2 \geq 0 + 2$ is false.

Example 2: Let $Q(x)$ be the predicate $x^2 \geq x$.
$Q(x)$ is true for all integers.
Therefore, $\forall x \ (x^2 \geq x)$ is a true proposition.

Existential quantification of $P(x)$

$\exists x\, P(x)$

$\exists$ should be read **There Exists**.

It is true when there exists a value of x in the universe of discourse such that $P(x)$ is true.

Example 1: $\exists x\ (x^2 \geq x + 2)$
is a true proposition since it is true when $x = 4$

Example 2: $\exists x\ (x^2 \geq x)$
is a true proposition, since it is true when $x = 0$.

Classroom exercise:

Universal conditional statements

Statements of the form $\forall x\ P(x) \rightarrow Q(x)$

Example: If a number is an integer, it is a rational number.

$\forall x$ if $x \in Z$ then $x \in Q$.

$\forall x\ \ x \in Z \rightarrow x \in Q$

Alternatively, every integer is a rational number.

$\forall x \in Z,\ \ Rational(x)$.

Implicit quantification

Sometimes, the quantifier is not explicitly present, but instead is implicit.

The notation $P(x) \Longrightarrow Q(x)$ is equivalent to $\forall x \; P(x) \rightarrow Q(x)$. It means $P(x)$ logically implies $Q(x)$.

Example: $x \in Z \Longrightarrow x \in Q \equiv \forall x \; x \in Z \rightarrow x \in Q$.

The notation $P(x) \Longleftrightarrow Q(x)$ is equivalent to $\forall x \; P(x) \leftrightarrow Q(x)$. It means $P(x)$ is logically equivalent to $Q(x)$.

Example: x is even $\Longleftrightarrow x^2$ is even $\equiv$
$\forall x \quad x$ is even $\leftrightarrow x^2$ is even.

Negations of quantifications

Suppose the universe of discourse is all Canadians, and let $P(x)$ be the predicate x *is a good driver.*

Then the statement:
All Canadians are good drivers.

can be written as: $\forall x \; P(x)$.

The negation of this statement is:
It is not the case that all Canadians are good drivers.
There are Canadians who are not good drivers.

$\exists x \; (\neg P(x))$

Negations of quantifications

The following equivalences hold:

$$\neg \forall\, x \;\; P(x) \Longleftrightarrow \exists\, x \;\; (\neg P(x))$$

$$\neg \exists\, x \;\; P(x) \Longleftrightarrow \forall\, x \;\; (\neg P(x))$$

Note that these statements are implicitly quantified over all predicates P.

Let the universe of discourse be all pigs
and $P(x)$ be the predicate x *can fly.*

Then the statement *“Some pigs can fly”* can be written as

$\exists x\, P(x)$

Some ... There are ... There is at least one.

The negation of this is:

It is not the case that some pigs can fly.
There are no pigs that can fly.
For every pig, it is not the case that it can fly.

$\forall\, x\ (\neg P(x))$.

Example: Let $P(x)$, $Q(x)$, and $R(x)$ be the statements "x is a professor," "x is ignorant," and "x is vain," respectively. Express the following using logical connectives and quantifiers. The universe of discourse for x is the set of all people.

1. No professors are ignorant.

   There is no one who is both a professor and ignorant.
   $\neg\exists x\, (P(x) \wedge Q(x)) \equiv \forall x\ (\neg P(x) \vee \neg Q(x))$

2. All ignorant people are vain.

   If someone is ignorant, then he/she is vain.
   $\forall x\ (Q(x) \rightarrow R(x))$

Classroom exercise:

Propositional functions of two variables

Example:
Let $R(x, y)$ be the predicate $x^2 \geq x + y$.

$R(1, 0) \equiv 1^2 \geq 1 + 0$ true
$R(5, 2) \equiv 5^2 \geq 5 + 2$ true
$R(0, 2) \equiv 0^2 \geq 0 + 2$ false

We need multiple quantifiers to turn a propositional function of many variables into a proposition.

When there are multiple quantifers, they must be considered from **left to right**:
$\forall x \, \exists y \;\; R(x, y)$
For every x there exists some y such that $R(x, y)$.

Classroom exercise:

Propositions:

$\forall y\,\forall x\;\; R(x,y)$
$\exists y\,\forall x\;\; R(x,y)$
$\forall y\,\exists x\;\; R(x,y)$
$\exists y\,\exists x\;\; R(x,y)$

$\forall x\,\forall y\;\; R(x,y)$
$\exists x\,\forall y\;\; R(x,y)$
$\forall x\,\exists y\;\; R(x,y)$
$\exists x\,\exists y\;\; R(x,y)$

Changing the **order** of the quantifiers may change the proposition.

Note that $\forall x\;\; R(x,y)$ or $\exists y\;\; R(x,y)$ are propositional functions of **one** variable.

In general,
$\forall x\,\exists y\;\; R(x,y) \not\Leftrightarrow \exists y \forall x\; R(x,y)$

<u>Example:</u> Universe of discourse is integers.
Consider the proposition
$\forall x\,\exists y\;\; (x < y)$

true, since it means:
For every integer x there exists an integer y greater than x.

Consider the proposition
$\exists y\,\forall x\,(x < y)$

false, since it means:
There is an integer y that is larger than any other integer.

Translation of sentences into logical expressions

Example 1: *Some applications can malfunction if they are not properly terminated.*

Some .... there are .... there exists

need to introduce names

universe of discourse: computer applications

variable X representing a computer application

$pt(X)$ ... X is properly terminated

$mf(X)$ .... X can malfunction

Some applications can malfunction if they are not properly terminated.

There exists an application X such that X can malfunction if X is not properly terminated.

There exists an application X such that if X is not properly terminated then X can malfunction.

$\exists X \; [(\neg pt(X)) \rightarrow mf(X)]$

Example 2: *Every student is assigned an id number.*

introduce names

For every student s there exists a number n such that n is the id of s.

s .... universe of discourse is students
n .... universe of discourse is integers
$id(n, s)$ .... n is the id of s

$\forall s \exists n \, id(n, s)$

What happens if $\forall$ and $\exists$ are reversed?

$\exists n \forall s \, id(n, s)$

There exists a number n such that for every student s, the number n is the id of s.

That is, all students have the same id number.

Example 3:

Every student is assigned a unique id number.

unique .... the id number of a student s cannot be the id number of any other student.

$\forall s \exists n \, [id(n, s) \wedge \forall t[s \neq t \rightarrow \neg id(n, t)]]$

universe of discourse for s, t is all students,
universe of discourse for n is integers.

Example 4: Assume the universe of discourse is students.

All comp. sci. students have a cs computer account.

comp_sci(s) .... s is a comp.sci. student.
cs_account(s) ... s has a cs computer account.

correct solution:

$\forall\, s\ [comp\_sci(s) \rightarrow cs\_account(s)]$

---

incorrect solution: $\forall\, s\ [\underbrace{comp\_sci(s) \wedge cs\_account(s)}_{\text{false when s is not a comp\_sci student.}}]$

Remember: the logical operation $\longrightarrow$ is used to **restrict** applicability of a property to a part of the universe of discourse when using $\forall$.

if p is valid *then* q is valid.

Example 5: Assume the universe of discourse is students.

Some computer science students like to dance.

$comp\_sci(s)$ ... s is a computer science student.

$dance(s)$ ... s likes to dance.

correct solution:

$\exists\, s\ [comp\_sci(s) \wedge dance(s)]$.

---

incorrect solution:

$\exists\, s\ [comp\_sci(s) \rightarrow dance(s)]$

Classroom exercise:

Quantifiers of the <u>same type</u> can be reversed without changing the truth value, i.e.,

$\forall x\, \forall y\; P(x,y) \equiv \forall y \forall x\; P(x,y)$
$\exists x\, \exists y\; P(x,y) \equiv \exists y \exists x\; P(x,y)$

Example:

$\forall x\, \forall y\ :\ x+y=y+x$ is equivalent to $\forall y\, \forall x\ :\ x+y=y+x$

$\exists x\, \exists y\ : 5x=3y$ is equivalent to $\exists y\, \exists x\ : 5x=3y$

Quantifiers and logical operations

$\neg(\exists x\, P(x)) \equiv \forall x\, (\neg P(x))$

$\neg(\forall x\, P(x)) \equiv \exists x\, (\neg P(x))$

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

Example: *There is a student in this class who is from Bangladesh or from Korea.*

is the same as

There is a student in this class who is from Bangladesh or there is a student in this class who is from Korea.

$\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$

However, in many cases

$\exists x\,(P(x) \wedge Q(x)) \not\equiv (\exists x\, P(x)) \wedge (\exists x\, Q(x))$

Example: *Some students speak Spanish and some students speak Italian*.

is **not** the same as

Some students speak Spanish and Italian.

Similarly,

$\forall x(P(x) \vee Q(x)) \not\equiv (\forall x P(x)) \vee (\forall x Q(x))$

Rewriting propositions

Example 1: *Every prime number greater than 2 is odd.*

Universe of discourse is integers.

For every number x, if x is prime and $x > 2$ then x is odd.

$\forall x\,[(prime(x) \wedge (x > 2)) \rightarrow odd(x)]$
$\equiv \forall x\,[\neg(prime(x) \wedge (x > 2)) \vee odd(x)]$
$\equiv \forall x\,[\neg(prime(x) \wedge (x > 2)) \vee \neg even(x)]$
$\equiv \forall x\,[\neg((prime(x) \wedge (x > 2)) \wedge even(x))]$
$\equiv \neg\exists x\,[(prime(x) \wedge (x > 2)) \wedge even(x)]$

$\equiv$ *It is not true that there exists a prime number that is greater than 2 and is even.*

Example 2: *Nobody is right all the time*

$\equiv$ *It is not true that there exists a person x such that x is right all the time.*

$\equiv$ *It is not true that there exists a person x such that at any time t, person x is right at time t.*

$right(x,t)$.... x is right at time t.

$\neg\exists\, x\, \forall\, t\ right(x,t)$
$\equiv \forall\, x\, \neg(\forall\, t\ right(x,t)$
$\equiv \forall\, x\, \exists\, t\ \neg\, right(x,t)$
$\equiv \forall\, x\, \exists\, t\ wrong(x,t)$

Every person is sometimes wrong.

Every student should know the definition of a:

universal quantifier,
existential quantifier.

and how to:

operate with logical operations and quantifiers.

translate a quantified expression into an English sentence.

translate an English sentence into a quantified expression.

Valid and Invalid Arguments

An argument is a sequence of statements.
Example:

p
q
r
$\therefore s$

Here p, q, and r are called premises and s is called the conclusion.

An argument is called **valid** if the truth of the conclusion follows necessarily (by logical form alone) from the truth of its premises.

When an argument is valid, and the premises are true, then the conclusion **must** be true.

A valid argument form

Consider the following argument:

If I drink coffee, I feel sick.
I am drinking coffee.
Therefore I feel sick.

This has the argument form:

$p \rightarrow q$

p

$\therefore q$

p	q	premise $p \rightarrow q$	premise p	conclusion q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	F

Note that when the premises are both true, the conclusion is also true. This is a valid argument form. It is called **modus ponens**.

An invalid argument form

The following argument form is invalid:

$p \to q$

$q \to p$

$\therefore p \vee q$

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

In the last row, both premises are true, but the conclusion is false.

Rules of inference

Valid argument forms that are commonly used.
They give a justification for obtaining a conclusion from facts that are known or can be assumed.

An inference rule

$$\frac{A}{\therefore\ B}$$

is the tautology $A \rightarrow B$. It should be read as

If A is true, then we conclude that B is true.

A is called the **hypothesis** or **premise**,
B is called the **conclusion**.

rule of inference	tautology	name
p $\therefore\ p \vee q$	$p \rightarrow (p \vee q)$	addition
$p \wedge q$ $\therefore\ p$	$(p \wedge q) \rightarrow p$	simplification
p q $\therefore\ p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	conjunction
p $p \rightarrow q$ $\therefore\ q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	modus ponens
$\neg q$ $p \rightarrow q$ $\therefore\ \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)]$ $\rightarrow (p \rightarrow r)$	hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore\ q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	disjunctive syllogism

Contradiction rule

$\neg p \rightarrow F$

$\therefore p$

Basis of the method of proof by contradiction.

p	¬ p	¬ p → F	(¬ p → F) → p
T	F	T	T
F	T	F	T

If an assumption leads to a contradiction, then the assumption must be false.

Exercise: Proof by cases rule

$$\begin{array}{l} p \vee q \\ p \rightarrow r \\ \underline{q \rightarrow r} \\ \therefore\ r \end{array}$$

Fallacies

The use of an incorrect inference may lead to an incorrect conclusion, called a **fallacy**.

Converse error:

$p \rightarrow q$ is true and q is true
Thus, p is true.

This is a false argument.

Example:
If the butler did it he has blood on his hands.
The butler has blood on his hands.
Therefore, the butler did it.

Inverse error:

$p \longrightarrow q$ is true and p is false
Thus, q is false.

This is a false argument.

Example:
If the butler is nervous, he did it.
The butler is calm.
Therefore, the butler didn't do it.

Fallacy of begging the question:

When a step of the proof is based on the truth of the statement being proved.

This is a false argument.

Example:

The number $\log_2 3$ is irrational if it is not the ratio of 2 integers. Therefore, since $\log_2 3$ cannot be written in the form a/b where a and b are integers, it is irrational.

We are given the following premises:

(1) If it does not rain or it is not foggy then the lifesaving demonstration will go on and a sailing race will be held.

(2) If the sailing race is held then a trophy is awarded.

(3) The trophy was not awarded

Show that using these premises, we can conclude that *it rained.*

p .... it rains
q .... it is foggy
r .... lifesaving demonstration will go on
s .... sailing race will be held.
t .... trophy is awarded

We know:
(1) If it does not rain or it is not foggy then the lifesaving demonstration will go on and a sailing race will be held.
$(\neg p \vee \neg q) \rightarrow (r \wedge s)$

(2) If the sailing race is held then a trophy is awarded.
$s \rightarrow t$

(3) The trophy was not awarded.
$\neg t$

Premises: $(\neg p \vee \neg q) \rightarrow (r \wedge s)$
$s \rightarrow t$
$\neg t$

1. $\neg t$
   $\underline{s \rightarrow t}$ modus tollens
   $\therefore\ \neg s$
2. $\underline{\ \neg s\ \ }$ addition
   $\therefore\ \neg s \vee \neg r \equiv \neg(r \wedge s)$
3. $\neg(r \wedge s)$
   $\underline{(\neg p \vee \neg q) \rightarrow (r \wedge s)}$ modus tollens
   $\therefore\ \neg(\neg p \vee \neg q) \equiv p \wedge q$
4. $\underline{(p \wedge q)}$ simplification
   $\therefore\ p$

p .... it rained.

Rules of Inference for Quantified Statements

rule of inference	name
$\dfrac{\forall x\, P(x)}{\therefore P(c) \text{ if } c \in U}$	Universal instantiation
$\dfrac{P(c) \text{ for arbitrary } c \in U}{\therefore \forall x\, P(x)}$	Universal generalization
$\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some } c \in U}$	Existential instantiation
$\dfrac{P(c) \text{ for some } c \in U}{\therefore \exists x\, P(x)}$	Existential generalization
$\forall x\, P(x) \rightarrow Q(x)$ $\underline{P(c) \text{ for specific } c \in U}$ $\therefore Q(c)$	Universal modus ponens
$\forall x\, P(x) \rightarrow Q(x)$ $\underline{\neg Q(c) \text{ for specific } c \in U}$ $\therefore \neg P(c)$	Universal modus tollens

Methods of Proofs

Methods that can be used to *verify* that a given proposition is true.

Proofs are used mostly in mathematics, but there is also a need for proofs in **software development**.

Examples of propositions from software development:

Software A works according to its specifications.

System B cannot stall.

The output values of computer control C are in an acceptable range.

Software segments in D communicate with each other correctly.

Examples of costly software problems:

- NASA probe sent to Mars. Cost: $130 000 000 U.S.
- Y2K problem. Billions were spent on it worldwide.
- Denver Airport baggage handling system. Cost: several tens of millions.
- US warship system shutdown. Several years ago, all computer systems on the ship crashed, including the propulsion and steering.

Lesson learned: Software developers must use methods that ensure software correctness.

Tools:

- Better software design techniques, discussed in software engineering courses.
- Proof techniques from mathematics.

Proof techniques

It would be very difficult to prove correctness for large and complex systems, but

- proof techniques can be used to prove correctness of small critical components,
- the reasoning used in proof techniques can be used to verify correctness of larger software systems informally.

Basic terminology

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

The statement
$(p \rightarrow q) \iff (\neg p \vee q)$

is a theorem, since we have shown that the truth tables for both expressions are the same.

The statement
There is life on the moon Europa of Jupiter

is not a theorem since we cannot show it to be true.

(This statement, or its negation might become a theorem eventually.)

A **proof** is a finite sequence of statements that show the correctness of a theorem.

A proof of statement s is a sequence of statements:

$s_1, s_2, s_3, \ldots, s_n, s$

where each s_i is one of:

- an axiom,
- a definition,
- an assumption of the theorem,
- a previously proven theorem,
- a statement derived using **rules of inference**

An **axiom** is a statement that is accepted as a basic true property.

Example of an axiom in geometry:
In the plane, there is exactly one straight line going through any two distinct points.

Example of an axiom in logic:
Any proposition is either true or false, but not both.

Methods of proofs can be divided into several basic types.

- **Direct proof**
- **Indirect proof**
- **Proof by contradiction**
- **Proof by cases**
- **Mathematical Induction**

Direct proof

We are to prove

$$p \Longrightarrow q$$

We need to prove that

When p is true then q is true.

Assume that p is true and derive from p a sequence of inferences that ends with q being true.

$$p \Longrightarrow q_1 \Longrightarrow q_2 \Longrightarrow q_3 \Longrightarrow \cdots \Longrightarrow q_n \Longrightarrow q$$

In each step we use a rule of inference, a known theorem, an axiom, etc.

Definition

m is even $\iff \exists\ i \in Z$ such that $m = 2i$

m is odd $\iff \exists\ i \in Z$ such that $m = 2i + 1$

Problem

Show that for every integer n, if n is even then n^2 is even.

$even(n) \Longrightarrow even(n^2)$

Proof: Suppose n is even.

$\Longrightarrow n = 2i$ for some integer i.

$\Longrightarrow n^2 = (2i)^2 = 2^2 \cdot i^2 = 2(2i^2)$.

$\Longrightarrow n^2 = 2j$, where $j = (2i^2)$.

$\Longrightarrow n^2$ is even, by definition, since j is an integer.

Indirect proof

It can be used when we are to prove an implication.
We are to prove

$$p \Longrightarrow q$$

Do instead a direct proof of the contrapositive

$$\neg q \Longrightarrow \neg p$$

namely,

$$\neg q \Longrightarrow q_1 \Longrightarrow q_2 \Longrightarrow q_3 \Longrightarrow \cdots \Longrightarrow q_n \Longrightarrow \neg p$$

We use the fact that

$$p \Longrightarrow q \equiv \neg q \Longrightarrow \neg p$$

Problem: Show that for every integer n, if n^2 is an even integer than n is an even integer.
$even(n^2) \Longrightarrow even(n)$

Idea: Show instead that
$(\neg(n \text{ is even })) \Longrightarrow (\neg(n^2 \text{ is even}))$
$\Longleftrightarrow (n \text{ is odd }) \Longrightarrow (n^2 \text{ is odd}))$

Proof: Suppose n is odd.
$\Longrightarrow n = 2i + 1$ for some integer i.
$\Longrightarrow n^2 = (2i+1)^2 = 2(2i^2 + 2i) + 1$.
$\Longrightarrow n^2$ is odd, since $2i^2 + 2i$ is an integer. This proves the required statement, since
$odd(n) \Longrightarrow odd(n^2) \equiv even(n^2) \Longrightarrow even(n)$.

Important:

To prove that

$$p \iff q$$

we usually have to do **two** proofs:

Prove

$$p \implies q$$

and prove

$$q \implies p$$

Example: Prove that

$$n \text{ is even } \iff n^2 \text{ is even}$$

Proof: We show that

(i) $even(n) \Longrightarrow even(n^2)$

(ii) $even(n^2) \Longrightarrow even(n)$

Proof by contradiction

(also called reductio ad absurdum)
Uses the contradiction rule.

(a) We are to prove the correctness of a statement p.

To show that

$$p \text{ is true,}$$

it is sufficient to show that

$$\neg p \text{ implies a contradiction.}$$

Rational numbers : integers and fractions such as

$\ldots -2, -1, 0, 1, 2, 3, \ldots$ and $\ldots, \frac{2}{3}, \frac{5}{7}, \frac{7}{4}, \frac{15}{2}, \ldots$

A number is **irrational** if it cannot be expressed as an integer or a fraction $\frac{a}{b}$ where a and b are integers, and $b \neq 0$.

Problem: Show that $\sqrt{2}$ is an irrational number.

Proof: Assume that $\sqrt{2}$ is a rational number.
$\Longrightarrow \sqrt{2} = \frac{a}{b}$ where a and b are integers that **do not have a common factor.**
$\Longrightarrow 2 = \frac{a^2}{b^2}$
$\Longrightarrow 2b^2 = a^2$
$\Longrightarrow a^2$ is an even number.
$\Longrightarrow a$ is an even number.
$\Longrightarrow a = 2i$ for some integer i.
$\Longrightarrow 2b^2 = 2^2 i^2$
$\Longrightarrow b^2 = 2i^2$
$\Longrightarrow b^2$ is an even number.
$\Longrightarrow b$ is an even number.
$\Longrightarrow a$ and b are both even.
$\Longrightarrow a$ and b have a common factor,
a contradiction to our assumption.

Proof by contradiction

(b) We are to prove the correctness of a logical implication.

$$p \Longrightarrow q$$

Use the fact that $(p \wedge \neg q \rightarrow F) \equiv (p \rightarrow q)$

Assume that $p \wedge \neg q$ is true and derive from $p \wedge \neg q$ a sequence of inferences that ends with a contradiction.

$$p \wedge \neg q \Longrightarrow q_1 \Longrightarrow q_2 \Longrightarrow q_3 \Longrightarrow \cdots \Longrightarrow q_n \Longrightarrow F$$

Problem: Show that if $3n+2$ is odd, then n is odd.

Proof: Assume that $3n+2$ is odd and that n is even.

$\Longrightarrow n = 2k$ for some integer k

$\Longrightarrow 3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$

$\Longrightarrow 3n+2$ is even, since it is a multiple of 2.

This contradicts the assumption that $3n+2$ is odd, completing the proof.

Proof by cases

Uses the rule of inference of the same name.

Show the following:

$A_1 \vee A_2 \vee \ldots A_n$

$A_1 \rightarrow C$

$A_2 \rightarrow C$

...

$A_n \rightarrow C$

and conclude that C is true.

Example: Show that
$max(x, y) + min(x, y) = x + y$

Proof. We consider the following cases:

$x \geq y$: Then $max(x, y) = x$ and $min(x, y) = y$.
Thus $max(x, y) + min(x, y) = x + y$.

$x < y$: Then $max(x, y) = y$ and $min(x, y) = x$.
Thus $max(x, y) + min(x, y) = y + x = x + y$.

Since these are the only two possible cases, the equality holds.