1. The Foundations (Logic)

1.1, 1.2 Propositional Logic (Chapter numbers are from the 7th edition of your textbook)

Motivation: Basis of all mathematical reasoning and numerous applications in computer science

- artificial intelligence
- computer programming and algorithm development
- design of computer circuits
- etc

By the end of these lectures, you will be able

- **to translate daily language to precise logical expressions**

"You cannot ride the roller coaster if you are less than 1.70m tall unless you are older than 18 years."

"Everyone has exactly one best friend."

- **to verify your reasoning and conclusions**

"If you are older than 18 years, then you can have a driving license." $\equiv$??

"If you can have a driving license, then you are older than 18 years," or

"If you cannot have a driving license, then you are not older than 18 years."

Proposition: A statement that is either *true* or *false*, but not both.

e.g.

- Snow is white
- Rain is wet
- $1 + 1 = 2$
- $2 + 3 = 7$

} Propositions

- What time is it?
- Consider reading the material.
- $x + 1 = 2$
- $x + y = z$

} Not Propositions

✵ Use letters to denote propositions:

p, q, r, s, …

Truth values: true T, false F

Compound Propositions

Many mathematical statements are constructed by combining propositions. Compound propositions are formed by using logical operators such as:

- negation (NOT) ¬
- conjunction (AND) ∧
- disjunction (OR) ∨
- exclusive or (XOR) ⊕
- implication (IF) →
- biconditional (IFF) ↔

:

Compound Propositions

Many mathematical statements are constructed by combining propositions. Compound propositions are formed by using logical operators such as:

- negation (NOT) $\neg$
- conjunction (AND) $\wedge$
- disjunction (OR) $\vee$
- exclusive or (XOR) $\oplus$
- implication (IF) $\rightarrow$
- biconditional (IFF) $\leftrightarrow$

Truth tables:

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

Definition:*Negation (NOT)*

Negation of p is $\neg p$ (not p)

e.g.

Proposition p: Today is Tuesday.

Negation of p: Today is **not** Tuesday

Truth table:

p	$\neg p$
T	F
F	T

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

Definition: Conjunction (AND)

The proposition “ p and q ”

denoted by $p \wedge q$

is T when both p and q are true,

is F otherwise.

The proposition $p \wedge q$ is called the conjunction of p and q.

Definition: Disjunction (OR)

The proposition “p or q”

denoted by $p \vee q$

is F when p and q are both false

is T otherwise

The proposition $p \vee q$ is called disjunction of p and q.

Definition: Exclusive Or (XOR)

The exclusive or of p and q, $p \oplus q$, is T when exactly one of p and q is true and is F otherwise.

e.g.

p: “Snow is white”

q: “Snow is cold”

$p \oplus q \equiv$??

$p \wedge q \equiv$??

$p \vee q \equiv$??

Truth table:

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

Definition: *Implication (IF)*

The implication $p \rightarrow q$ is F when p is T and q is F
is T otherwise.

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

e.g. "If today is Tuesday, then 2 + 2 = 10" (True)

"If today is Tuesday, then we have a quizze" (?)

$p \rightarrow q$
p: premise (hypothesis)
q: conclusion (consequence)

“If you are blonde, then you have blue eyes”

Blonde and blue eyes	⇒ true
Blonde and brown eyes	⇒ false
Not blonde and blue eyes	⇒ true
Not blonde and brown eyes	⇒ true

Common ways of expressing implication:

- if p then q
- p implies q
- p is sufficient for q
- q whenever p
- q is necessary for p
- q follows from p

$p \to q$

Converse: $q \to p$

Contrapositive: $\neg q \to \neg p$

“If you are older than 18 years, then you can have a driving license”

Converse: “If you can have a driving license, then you are older than 18 years”

Contrapositive: “If you cannot have a driving license, then you are not older than 18 years”

Definition: *Biconditional (IFF)*

The biconditional p ↔ q is T when p and q have same truth value and is F otherwise.

P	q	p ↔ q
T	T	T
T	F	F
F	T	F
F	F	T

p ↔ q is T if both p → q is T and q → p is T.

“p if and only if q”
“p is necessary and sufficient for q”
“if p then q, and conversely”

p ↔ q is logically equivalent to say that p → q ∧ q → p.

Translation from English to logical expression

Example:

"You cannot ride the roller coaster if you are less than 1.70m tall unless you are older than 18 years."

q: "You can ride the roller coaster"

r: "You are less than 1.70m tall"

s: "You are older than 18 years"

Let's try….

Translation from English to logical expression

Example:

"You cannot ride the roller coaster if you are less than 1.70m tall unless you are older than 18 years."

q: "You can ride the roller coaster"

r: "You are less than 1.70m tall"

s: "You are older than 18 years"

$$(r \land \neg s) \rightarrow \neg q$$

e.g.[*]

p: “It is below freezing”
q: “It is snowing”

- “It is below freezing but not snowing.”

- “It’s below freezing or it’s snowing; but it’s not snowing if it’s below freezing.”

[*] exempli gratia

e.g.

p: “It is below freezing”

q: “It is snowing”

- “It is below freezing but not snowing.”
  $p \wedge \neg q$

- “It’s below freezing or it’s snowing; but it’s not snowing if it’s below freezing.”
  $(p \vee q) \wedge (p \rightarrow \neg q)$

and ≈ but

Logic and bit operations:

A **bit** has two possible values, 0 or 1.

Binary digit ⇒ bit (John Tukey, 1946)

In most programming languages, a variable is a Boolean variable if its value is either T or F, or equivalently 0 or 1.

Bit operations ⇔ Logical operations

T → 1, F → 0

Bitwise OR, AND, XOR

$$\begin{array}{lll}
1010 & 1110 & \\
1100 & 0101 & \\
\hline
1110 & 1111 & \text{bitwise OR} \\
1000 & 0100 & \text{bitwise AND} \\
0110 & 1011 & \text{bitwise XOR}
\end{array}$$

1.3 Propositional Equivalences:

Definition: Logical equivalence

The propositions r and s are logically equivalent if r and s have the same truth values.

Notation: $r \equiv s$

1.3 Propositional Equivalences

Definition: Logical equivalence

The propositions r and s are logically equivalent if r and s have the same truth values.

Notation: $r \equiv s$

e.g.

Show that $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (De Morgan's law)

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Logical Equivalences

$$\left.\begin{array}{l} p \wedge T \equiv p \\ p \vee F \equiv p \end{array}\right\} \qquad \text{Identity laws}$$

$$\left.\begin{array}{l} p \vee T \equiv T \\ p \wedge F \equiv F \end{array}\right\} \qquad \text{Domination laws}$$

$$\left.\begin{array}{l} p \vee p \equiv p \\ p \wedge p \equiv p \end{array}\right\} \qquad \text{Idempotent laws}$$

$$\neg(\neg p) \equiv p \qquad \text{Double Negation law}$$

$$\left.\begin{array}{l} p \vee q \equiv q \vee p \\ p \wedge q \equiv q \wedge p \end{array}\right\} \qquad \text{Commutative laws}$$

$$\left.\begin{aligned}(p \vee q) \vee r &\equiv p \vee (q \vee r)\\(p \wedge q) \wedge r &\equiv p \wedge (q \wedge r)\end{aligned}\right\} \quad \text{Associate laws}$$

$$\left.\begin{aligned}p \vee (q \wedge r) &\equiv (p \vee q) \wedge (p \vee r)\\p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r)\end{aligned}\right\} \quad \text{Distributive laws}$$

$$\left.\begin{aligned}\neg(p \wedge q) &\equiv \neg p \vee \neg q\\\neg(p \vee q) &\equiv \neg p \wedge \neg q\end{aligned}\right\} \quad \text{De Morgan's laws}$$

Some additional useful logical equivalences:

$p \vee \neg p \equiv T$

$p \wedge \neg p \equiv F$

$(p \rightarrow q) \equiv (\neg p \vee q)$

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

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

You can show all these logical equivalences using truth tables.

Definition:

Tautology: A compound proposition that is always true

Contradiction: A compound proposition that is always false

Contingency: Neither tautology nor contradiction

e.g.	$p \vee \neg p$	$p \wedge \neg p$
	tautology	contradiction

e.g.

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

e.g.

Show that $(p \land q) \to (p \lor q)$ is a tautology.

$$\begin{aligned}
(p \land q) \to (p \lor q) &\equiv \neg(p \land q) \lor (p \lor q) \\
&\equiv (\neg p \lor \neg q) \lor (p \lor q) && \text{De Morgan} \\
&\equiv (\neg p \lor p) \lor (\neg q \lor q) && \text{Assoc \& Comm} \\
&\equiv T \lor T \\
&\equiv T
\end{aligned}$$

e.g.

Show that $\neg(p \rightarrow q) \equiv p \wedge \neg q$

e.g.

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

You can show these logical equivalences using truth tables or using known equivalences.

Consistency of Propositions

Consider the following propositions for a system specification:

“Whenever the system software is being upgraded, users cannot access the file system”
“If users can access the file system, then they can save new files.”
“If users cannot save new files, then the system software is not being upgraded.”

Are they consistent?

Consistency of Propositions

Consider the following propositions for a system specification:

“Whenever the system software is being upgraded, users cannot access the file system”
“If users can access the file system, then they can save new files.”
“If users cannot save new files, then the system software is not being upgraded.”

Are they consistent?

The best way is to construct a truth table with
$p \to \neg q$, $q \to r$, $\neg r \to \neg p$
(but what are p, q, r ?)

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

Consistency of Propositions

Consider the following propositions for a system specification:

“Whenever the system software is being upgraded, users cannot access the file system”
“If users can access the file system, then they can save new files.”
“If users cannot save new files, then the system software is not being upgraded.”

Are they consistent?

The best way is to construct a truth table with

$p \rightarrow \neg q$, $q \rightarrow r$, $\neg r \rightarrow \neg p$
(but what are p, q, r ?)

If we can find a truth value assignment such that all propositions are T, then they are **consistent**, otherwise **inconsistent**.

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

1.4 Predicates and Quantifiers:

Statement: $\overbrace{x}^{\text{Subject}}\ \overbrace{\text{is greater than 3}}^{\text{Predicate}}$

This is a **propositional function.**

We can express it in another form:

$P(x)$: $x > 3$

Then what are the truth values of $P(4)$ and $P(2)$?

Definition 1: **Universal Quantification of** *P(x)*

is the proposition "*P(x)* is T for all values of *x* in the **universe of discourse (*domain*)**."

Notation: $\forall x\ P(x)$

"for all *x* *P(x)*"

"for every *x* *P(x)*"

$\forall$: Universal quantifier

e.g.

"Every student in this class has studied calculus."

Definition 1: **Universal Quantification of** *P(x)*

is the proposition "*P(x)* is T for all values of *x* in the **universe of discourse (*domain*)**."

Notation: $\forall x \; P(x)$

"for all *x* *P(x)*"

"for every *x* *P(x)*"

$\forall$: Universal quantifier

e.g.

"Every student in this class has studied calculus."

Express this as a universal quantification.

Let *P(x)* denote "*x* has studied calculus"

Then $\forall x \; P(x)$, where universe of discourse is all the students in the class.

DOMAIN (universe of discourse) MUST BE SPECIFIED!!

OR

$\forall x\ (S(x) \rightarrow P(x))$

where

S(x) denotes "*x* is in the class"

Universe of discourse is the set of all students.

e.g.

What is the truth value of $\forall x\ P(x)$, where

$P(x)$: "$x^2 < 10$"

Universe of discourse: $x \in \{1,2,3,4\}$

$$\forall x\ P(x) \equiv P(1) \wedge P(2) \wedge P(3) \wedge P(4)$$

$$\equiv \mathrm{F}$$

Definition 2: **The Existential Quantification of** *P(x)*

is the proposition "there exists an element *x* in the universe of discourse (domain) such that *P(x)* is true."

Notation:

$\exists x\ P(x)$

"there exists an *x* s.t. *P(x)*"

"there is at least one *x* s.t. *P(x)*"

$\exists$: Existential quantifier

e.g.

$$P(x): \quad x = x + 1, \quad x \in \mathrm{R}$$

$$\exists x\, P(x) \equiv ?$$

e.g.

$$P(x): \quad x^2 > 10, \quad x \in \{1, 2, 3, 4\}$$

$$\begin{aligned} \exists x\, P(x) &\equiv P(1) \vee P(2) \vee P(3) \vee P(4) \\ &\equiv \mathrm{T} \end{aligned}$$

1.5 Nested Quantifiers:

Translating Sentences into Logical Expression

e.g.

"Everyone has at least one best friend."

Let *B (x,y)*: "*y* is the best friend of *x*"

Universe of discourse for both *x* and *y* is the set of all students in this class.

1.5 Nested Quantifiers:

Translating Sentences into Logical Expression

e.g.

“Everyone has at least one best friend.”

Let $B\ (x,y)$: “y is the best friend of x”

Universe of discourse for both x and y is the set of all students in this class.

$\forall x\ \exists y \quad B(x, y)$

How about “Everyone has exactly one best friend.”?

Universe of discourse is all the students in this class.

Let *B(x,y):* “*y* is the best friend of *x*”

How about “Everyone has exactly one best friend.”?

Universe of discourse is all the students in this class.

Let $B(x,y)$: “y is the best friend of x”

“For every person x, there is a person y such that y is the best friend of x and if z is a person other than y, then z is not the best friend of x.”

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

How about “Everyone has exactly one best friend.”?

Universe of discourse is all the students in this class.

Let *B(x,y):* “*y* is the best friend of *x*”

“For every person *x*, there is a person *y* such that *y* is the best friend of *x* and if *z* is a person other than *y*, then *z* is not the best friend of *x*.”

$$\forall x\, \exists y \;\; (\, B(x, y) \wedge (\, \forall z \;\; (z \neq y) \rightarrow \neg B(x, z)\,)\,) \equiv$$

$$\forall x\, \exists y\, \forall z \;\; B(x, y) \wedge (\, (z \neq y) \rightarrow \neg B(x, z)\,)$$

Replacing quantifiers:

$$Q(x) \rightarrow \forall y\, P(x,y) \equiv \forall y\, (\, Q(x) \rightarrow P(x,y)\,)$$

e.g.

Consider

$P(x,y)$: "Student x solves question y"

$Q(x)$: "Student x passes the exam"

Replacing quantifiers:

$$Q(x) \rightarrow \forall y\, P(x,y) \equiv \forall y\, (\, Q(x) \rightarrow P(x,y)\,)$$

e.g.

Consider

$P(x,y)$: “Student x solves question y”

$Q(x)$: “Student x passes the exam”

So we can also write

$$\forall x\, (Q(x) \rightarrow \forall y\, P(x,y)\,) \equiv \forall x\, \forall y\, (\, Q(x) \rightarrow P(x,y)\,)$$

Remark: Be careful when replacing quantifiers!

Example: We **cannot** write

$\forall x \ (\forall y \, P(x,y) \rightarrow Q(x)) \equiv \forall x \, \forall y \, (\, P(x,y) \rightarrow Q(x) \,)$ **(this is wrong!)**

since

$\forall y \, (\, P(x,y) \rightarrow Q(x) \,)$ is **not** logically equivalent to $(\forall y \, P(x,y) \,) \rightarrow Q(x)$

Remark: Be careful when replacing quantifiers!

Example: We **cannot** write

$\forall x\ (\forall y\ P(x,y) \rightarrow Q(x)) \equiv \forall x\ \forall y\ (\ P(x,y) \rightarrow Q(x)\ )$ **(this is wrong!)**

since

$\forall y\ (\ P(x,y) \rightarrow Q(x)\ )$ is **not** logically equivalent to $(\forall y\ P(x,y)\ ) \rightarrow Q(x)$

e.g.

Consider

$P(x,y)$: "Student x solves question y"

$Q(x)$: "Student x passes the exam"

The Order of Quantifiers

The order of quantifiers is **important !!!** unless all quantifiers are universal or existential.

e.g.

$\forall x \, \exists y \, P(x,y)$ is **not** equivalent to $\exists y \, \forall x \, P(x,y)$.

Let $P(x,y)$ be the statement " $x + y = 0$ ".

$\forall x \, \exists y \, P(x,y)$: " For every real number x there is a real number y such that $x+y=0$."

$\exists y \, \forall x \, P(x,y)$: " There is a real number y such that for every real number x, $x+y=0$."

Negation of Quantified Statements:

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

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

Negation of Quantified Statements:

$$\neg(\forall x\, P(x)) \quad \equiv \quad \exists x\ \neg P(x) \quad \equiv \quad \exists x \quad P(x) \text{ is false}$$

$$\neg(\exists x\, P(x)) \quad \equiv \quad \forall x\ \neg P(x) \quad \equiv \quad \forall x \quad P(x) \text{ is false}$$

e.g.

“There exists a living person who is 150 years old.”

Write down as a logical expression using predicates and quantifiers and then negate:
Let *P(x)*: “*x* is 150 years old,” and the universe of discourse is set of living people.

Negation of Quantified Statements:

$\neg(\forall x\ P(x)) \equiv \exists x\ \neg P(x) \equiv \exists x\ \ P(x)$ is false

$\neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x) \equiv \forall x\ \ P(x)$ is false

e.g.

"There exists a living person who is 150 years old."

Write down as a logical expression using predicates and quantifiers and then negate:
Let *P(x)*: "*x* is 150 years old," and the universe of discourse is set of living people.

$\exists x\ P(x)$

“There exists a living person who is 150 years old.” $\exists x\, P(x)$

Negation of $\exists x\, P(x)$?

“There exists a living person who is 150 years old.” $\exists x\, P(x)$

Negation of $\exists x\, P(x)$?

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

“Every living person is not 150 years old,” or equivalently “no living person is 150 years old.”

In the previous example, what changes if the universe of discourse is modifed as "the set of all people"? Then we would need another propositional function, e.g., $R(x)$: "x is a living person".

"There exists a living person who is 150 years old" ≡ ?

In the previous example, what changes if the universe of discourse is modifed as “the set of all people”? Then we would need another propositional function, e.g., $R(x)$: “x is a living person”.

“There exists a living person who is 150 years old” ≡

$$\exists x\ P(x) \wedge R(x)$$

Negation: $\forall x\ \neg P(x) \vee \neg R(x) \equiv \forall x\ P(x) \rightarrow \neg R(x) \equiv \forall x\ R(x) \rightarrow \neg P(x)$ which means “For every person x, if x is living, x is not 150 years old,” or equivalently “no living person is 150 years old”, which is the same as before.

You can show the equivalences $\neg(\forall x\ P(x)) \equiv \exists x\ \neg P(x)$ and $\neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x)$ by using De Morgan’s rule.

You can show the equivalences $\neg(\forall x\, P(x)) \equiv \exists x\; \neg P(x)$ and $\neg(\exists x\, P(x)) \equiv \forall x\, \neg P(x)$ by using De Morgan's rule.

e.g.

$P(x)$: $x^2 > 10$, $x \in \{1, 2, 3, 4\}$

Negation of $\exists x\, P(x)$?

$$\begin{aligned} \neg\exists x\, P(x) &\equiv \neg(P(1) \vee P(2) \vee P(3) \vee P(4)) \\ &\equiv \neg P(1) \wedge \neg P(2) \wedge \neg P(3) \wedge \neg P(4) \quad \text{by De Morgan's rule} \\ &\equiv \forall x\, \neg P(x) \end{aligned}$$

e.g.

Show that $\neg\forall x\,\exists y\, P(x,y) \equiv \exists x \forall y\, \neg P(x,y)$

Hint: Negate successively two times.

e.g. Negate $\forall x \exists y \;\; xy = 1$

$\exists x \forall y \;\; xy \neq 1$

e.g. **Negate** “Some student in this class has solved every exercise in the book.”

“Some student in this class has not solved every exercise in the book.” **Not correct!!!**

Let S(*x,y*) be “student *x* has solved exercise *y*”, where the universe of discourse for *x* is the set of students in this class, and for y, the set of exercises in the book.

e.g. **Negate** “Some student in this class has solved every exercise in the book.”

“Some student in this class has not solved every exercise in the book.” **Not correct!!!**

Let $S(x,y)$ be “student x has solved exercise y”, where the universe of discourse for x is the set of students in this class, and for y, the set of exercises in the book.

$\neg\exists x\forall y\; S(x,y) \equiv \forall x\exists y\; \neg S(x,y)$

“For every student in this class there is an exercise that she or he has not solved.”

Equivalently “No student in this class has solved every exercise in the book.”

e.g. **Negate** "Some student in this class has solved every exercise in the book."

What if the universe of discourse for x is the set of all students, and for y, the set of exercises in the book?

$S(x,y)$: "Student x has solved exercise y"

$Q(x)$: "Student x is in this class"

$\neg\exists x\forall y\ Q(x) \wedge S(x,y) \equiv \forall x\exists y\ \neg Q(x) \vee \neg \mathrm{S}(x,y) \equiv \forall x\exists y\ Q(x) \rightarrow \neg \mathrm{S}(x,y)$

"For every student in this class there is an exercise that she or he has not solved."

Equivalently "No student in this class has solved every exercise in the book."

e.g. **Negate** “Everyone has exactly one best friend.”

Universe of discourse is the set of all students in the class (for both x and y).

Let $B(x,y)$: “y is the best friend of x”.

$$\forall x\ \exists y\ \forall z \quad B(x, y) \wedge ((z \neq y) \rightarrow \neg B(x, z))$$

Negation: “Everyone does not have exactly one best friend.” ? Not very informative!

e.g. **Negate** “Everyone has exactly one best friend.”

Universe of discourse is the set of all students in the class (for both x and y).

Let $B\ (x,y)$: “y is the best friend of x”.

$$\forall x\ \exists y\ \forall z \quad B\ (x,\ y) \wedge ((z \neq y) \rightarrow \neg B\ (x,\ z))$$

Negation: “Everyone does not have exactly one best friend.” ? Not very informative!

$$\neg\forall x\ \exists y \forall z \quad B\ (x,\ y) \wedge ((z \neq y) \rightarrow \neg B\ (x,\ z)\ ) \equiv$$

$$\exists x\ \neg\exists y\ \forall z \quad B\ (x,\ y) \wedge ((z \neq y) \rightarrow \neg B\ (x,\ z)\ ) \equiv$$

$$\exists x \forall y\ \neg\forall z \quad B\ (x,\ y) \wedge ((z \neq y) \rightarrow \neg B\ (x,\ z)\ ) \equiv$$

$$\exists x \forall y\ \exists z \quad \neg(B\ (x,\ y) \wedge ((z \neq y) \rightarrow \neg B\ (x,\ z)\ )) \equiv$$

$$\exists x \forall y\ \exists z \quad \neg B\ (x,\ y)\ \vee\ \neg((z \neq y) \rightarrow \neg B\ (x,\ z)\ )) \equiv$$

$$\exists x \forall y\ \exists z \quad \neg B\ (x,\ y)\ \vee\ ((z \neq y) \wedge B\ (x,\ z)\ ))$$

“There is a person x such that, for every person y,

y is not the best friend of x,

OR there exists a person z other than y such that z is the best friend of x”.

An alternative way of expressing the above negation (easier to interpret):

$$\exists x \forall y \, \exists z \quad \neg B\,(x,\, y) \;\vee\; ((z \neq y) \wedge B\,(x,\, z)\,)) \equiv$$

$$\exists x \forall y \, \exists z \quad B\,(x,\, y) \;\rightarrow\; ((z \neq y) \wedge B\,(x,\, z)\,))$$

An alternative way of expressing the above negation (easier to interpret):

$$\exists x \forall y\, \exists z \quad \neg B(x, y) \lor ((z \neq y) \land B(x, z))) \equiv$$

$$\exists x \forall y\, \exists z \quad B(x, y) \rightarrow ((z \neq y) \land B(x, z)))$$

"There is a person *x* such that, for every person *y*,
if *y* is the best friend of *x*,
then there exists a person *z* other than *y* such that *z* is the best friend of *x*".

An alternative way of expressing the above negation (easier to interpret):

$$\exists x \forall y\, \exists z \quad \neg B\,(x, y) \;\vee\; ((z \neq y) \wedge B\,(x, z)\,)) \equiv$$

$$\exists x \forall y\, \exists z \quad B\,(x, y) \;\rightarrow\; ((z \neq y) \wedge B\,(x, z)\,))$$

“There is a person *x* such that, for every person *y*,

if *y* is the best friend of *x*,

then there exists a person *z* other than *y* such that *z* is the best friend of *x*”.

We could rephrase the same statement as:

“There is a person *x* such that, *x* has no best friend or *x* has more than one best friend.”
or “There is a person who has no best friend or has more than one best friend.”

e.g. **Negate** $\forall x\ ((\forall y\ P(x,y)) \rightarrow Q(x))$

Note that

$\forall x\ ((\forall y\ P(x,y)) \rightarrow Q(x))$ is **not** logically equivalent to $\forall x\ \forall y\ (P(x,y) \rightarrow Q(x))$

e.g. **Negate** $\forall x\ ((\forall y\, P(x,y)) \rightarrow Q(x))$

Note that

$\forall x\ ((\forall y\, P(x,y)) \rightarrow Q(x))$ is **not** logically equivalent to $\forall x\, \forall y\, (P(x,y) \rightarrow Q(x))$

$\neg\, \forall x\ ((\forall y\, P(x,y)) \rightarrow Q(x)) \equiv \exists x\, \neg\, ((\forall y\, P(x,y)) \rightarrow Q(x)) \equiv \exists x\, \neg\, (\neg\, (\forall y\, P(x,y)) \vee Q(x))$

$\equiv\ \exists x\ ((\forall y\ P(x,y)) \wedge \neg Q(x))$

1.6/1.8/1.9 Mathematical Reasoning & Methods of Proof

We will learn:

- Rules of reasoning; how to reason correctly
  - are used to draw conclusions from other assertions and tie the steps of a proof.

- Methods of proof; how to show whether a given (mathematical) statement is true or not

Basic rule of inference: (Modus ponens)

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

e.g.

“If it is sunny today, then we’ll play soccer. It is sunny today, so we’ll play soccer”.

Basic rule of inference: (Modus ponens)

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

e.g.

“If it is sunny today, then we’ll play soccer. It is sunny today, so we’ll play soccer”.

Another notation:

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Basic rule of inference: (Modus ponens)

$(p \land (p \rightarrow q)) \rightarrow q$: Tautology

e.g.

"If it is sunny today, then we'll play soccer. It is sunny today, so we'll play soccer".

p	q	$p \rightarrow q$	$(p \land (p \rightarrow q)) \rightarrow q$
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	T

e.g.

If it is sunny today, then we’ll play soccer. We’ll play soccer, so it is sunny today.

e.g.

If it is sunny today, then we’ll play soccer. We’ll play soccer, so it is sunny today.

$[(p \rightarrow q) \land q] \rightarrow p$

e.g.

If it is sunny today, then we'll play soccer. We'll play soccer, so it is sunny today.

$[(p \rightarrow q) \wedge q] \rightarrow p$ **NOT** a tautology

F when p is F and q is T

Therefore, this is **not** a correct way of reasoning.

e.g.

It is sunny now. Therefore, it's sunny or snowy now. Tautology.

$$\frac{p}{\therefore\ p \lor q}$$

Addition Rule

e.g.

It is windy and raining now. Therefore, it is windy now. Tautology.

$$\frac{p \land q}{\therefore\ p}$$

Simplification Rule

Rule of Inference	**Tautology**	**Name**
p $\therefore\ p \lor q$	$p \rightarrow (p \lor q)$	Addition
$p \land q$ $\therefore\ p$	$(p \land q\ ) \rightarrow p$	Simplification
p q $\therefore\ p \land q$	$((p) \land (q)) \rightarrow (p \land q)$	Conjunction
p $p \rightarrow q$ $\therefore\ q$	$[p \land (p \rightarrow q)] \rightarrow q$	**Modus Ponens**
$\neg q$ $p \rightarrow q$ $\therefore\ \neg p$	$[\neg q \land (p \rightarrow q)] \rightarrow \neg p$	**Modus Tollens**
$p \rightarrow q$ $q \rightarrow r$ $\therefore\ p \rightarrow r$	$[(p \rightarrow q) \land (q \rightarrow r)] \rightarrow (p \rightarrow r)$	**Hypothetical Syllogism**
$p \lor q$ $\neg p$ $\therefore\ q$	$[(p \lor q\ ) \land \neg p] \rightarrow q$	Disjunctive Syllogism

e.g. Show that hypotheses

“If you help me, then I will finish writing the program,” “If you do not help me, then I will go to sleep early,” and “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’ll wake up feeling refreshed.”

Let

p: “you help me”
q: “I’ll finish writing the program”
r: “I’ll go to sleep early”
s: “I’ll wake up feeling refreshed”

e.g. Show that hypotheses

“If you help me, then I will finish writing the program,” “If you do not help me, then I will go to sleep early,” and “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’ll wake up feeling refreshed.”

Let

p: “you help me”
q: “I’ll finish writing the program”
r: “I’ll go to sleep early”
s: “I’ll wake up feeling refreshed”

Step	Reason
1. $p \rightarrow q$	hypothesis
2. $\neg q \rightarrow \neg p$	contrapositive of step 1
3. $\neg p \rightarrow r$	hypothesis
4. $\neg q \rightarrow r$	hypothetical syllogism using steps 2, 3
5. $r \rightarrow s$	hypothesis
6. $\neg q \rightarrow s$	hypothesis syllogism using steps 4, 5

Rules of Inference for Quantified Statements

Universal instantiation:

$$\frac{\forall x\ P(x)}{\therefore\ P(c) \text{ if } c \in U}$$

U: universe of discourse

Universal generalization:

$$\frac{P(c) \text{ for an arbitrary } c \in U}{\therefore\ \forall x\ P(x)}$$

Existential instantiation:

If $\exists x\ P(x)$ is true then
we know one c exists
s.t. $P(c)$ is true.

$$\frac{\exists x\ P(x)}{\therefore\ P(c) \text{ for some element } c \in U}$$

Existential generalization:

If we know one c in U
s.t. $P(c)$ is true then
$\exists x\ P(x)$ is true

$$\frac{P(c) \text{ for some element } c \in U}{\therefore\ \exists x\ P(x)}$$

e.g.

i) “All lions are fierce”

ii) “Some lions do not drink coffee”

Does i) and ii) imply that “some fierce creatures do not drink coffee” ?

P(x): “x is a lion”

Q(x): “x is fierce”

R(x): “x drinks coffee”

Universe of discourse is the set of all creatures.

e.g.

i) “All lions are fierce”

ii) “Some lions do not drink coffee”

Does i) and ii) imply that “some fierce creatures do not drink coffee” ?

P(x): “x is a lion”

Q(x): “x is fierce”

R(x): “x drinks coffee”

Universe of discourse is the set of all creatures.

i) $\forall x\ (P(x) \rightarrow Q(x))$

ii) $\exists x\ (P(x) \wedge \neg R(x))$

i) $\wedge$ ii) $\Rightarrow ?\ \exists x\ (Q(x) \wedge \neg R(x))$

e.g.

i) “All lions are fierce”

ii) “Some lions do not drink coffee”

Does i) and ii) imply that “some fierce creatures do not drink coffee” ?

P(x): “x is a lion”

Q(x): “x is fierce”

R(x): “x drinks coffee”

Universe of discourse is the set of all creatures.

i) $\forall x\ (P(x) \rightarrow Q(x))$

ii) $\exists x\ (P(x) \wedge \neg R(x))$

i) $\wedge$ ii) $\Rightarrow?\ \exists x\ (Q(x) \wedge \neg R(x))$

(ii) implies that there is some x_1 such that $P(x_1) \wedge \neg R(x_1)$ by **Existential Instantiation**.

e.g.

i) “All lions are fierce”

ii) “Some lions do not drink coffee”

Does i) and ii) imply that “some fierce creatures do not drink coffee” ?

P(x): “x is a lion”

Q(x): “x is fierce”

R(x): “x drinks coffee”

Universe of discourse is the set of all creatures.

i) $\forall x\ (\mathrm{P}(x) \rightarrow \mathrm{Q}(x))$

ii) $\exists x\ (\mathrm{P}(x) \wedge \neg\mathrm{R}(x))$

i) $\wedge$ ii) $\Rightarrow$? $\exists x\ (\mathrm{Q}(x) \wedge \neg\mathrm{R}(x))$

(ii) implies that there is some x_1 such that $\mathrm{P}(x_1) \wedge \neg\mathrm{R}(x_1)$ by **Existential Instantiation**.

Hence by (i), $\mathrm{Q}(x_1)$ is true (using **Simplification** and **Modus Ponens** rules).

e.g.

i) “All lions are fierce”

ii) “Some lions do not drink coffee”

Does i) and ii) imply that “some fierce creatures do not drink coffee” ?

P(x): “x is a lion”

Q(x): “x is fierce”

R(x): “x drinks coffee”

Universe of discourse is the set of all creatures.

i) $\forall x\ (P(x) \rightarrow Q(x))$

ii) $\exists x\ (P(x) \land \neg R(x))$

i) $\land$ ii) $\Rightarrow$? $\exists x\ (Q(x) \land \neg R(x))$

(ii) implies that there is some x_1 such that $P(x_1) \land \neg R(x_1)$ by **Existential Instantiation**.

Hence by (i), $Q(x_1)$ is true (using **Simplification** and **Modus Ponens** rules).

$\neg R(x_1)$ is also true by using again **Simplification** rule.

e.g.

i) “All lions are fierce”

ii) “Some lions do not drink coffee”

Does i) and ii) imply that “some fierce creatures do not drink coffee” ?

P(x): “x is a lion”

Q(x): “x is fierce”

R(x): “x drinks coffee”

Universe of discourse is the set of all creatures.

i) $\forall x\ (P(x) \rightarrow Q(x))$

ii) $\exists x\ (P(x) \wedge \neg R(x))$

i) $\wedge$ ii) $\Rightarrow ?\ \exists x\ (Q(x) \wedge \neg R(x))$

(ii) implies that there is some x_1 such that $P(x_1) \wedge \neg R(x_1)$ by **Existential Instantiation**.

Hence by (i), $Q(x_1)$ is true (using **Simplification** and **Modus Ponens** rules).

$\neg R(x_1)$ is also true by using again **Simplification** rule.

Then $Q(x_1) \wedge \neg R(x_1)$ which implies that $\exists x\ (Q(x) \wedge \neg R(x))$ by **Existential Generalization**.

Fallacies: Types of **incorrect** reasoning:

Fallacy of affirming the conclusion:

e.g.
"If you have solved every problem in this book, then you know Discrete Math. You know Discrete Math. Therefore, you have solved every problem in this book."

$[(p \rightarrow q) \wedge q] \rightarrow p$ **NOT** a tautology
F when p is F and q is T

Fallacy of denying the hypothesis:

"If you are older than 18 years, then you can have a driving license. You are not older than 18 years, so you can't have a driving license."

$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ NOT a tautology
F when p is F and q is T

Begging the question fallacy: When one or more steps of a proof are based on the truth of the statement being proved (circular reasoning)

Methods of Proving Theorems

Theorem: A statement that can be shown to be true.
Proof: Arguments which show that a theorem is true.
Axioms: Underlying assumptions about a mathematical structure.
Definitions: Rules of the game!

Methods of Proving Theorems

Theorem: A statement that can be shown to be true.
Proof: Arguments which show that a theorem is true.
Axioms: Underlying assumptions about a mathematical structure.
Definitions: Rules of the game!

To prove a theorem, you usually start from premises (conditions), and using known theorems, axioms and definitions, you construct a sequence of steps that leads to the conclusion (forward reasoning).

Example - Fermat's Last Theorem:

The equation

$$x^n + y^n = z^n$$

has no solution in integers x, y, and z with $xyz \neq 0$, whenever n is an integer with $n > 2$.

Put forward in the 17th century, but formally proved only in 1990s.

Some further terminology:

Lemma: A simple theorem that is used in the proof of other theorems.

Corollary: A proposition that can be established directly from a theorem.

Conjecture: A statement whose truth-value is unknown. If a proof can be found, then it becomes a theorem.

Some further terminology:

Lemma: A simple theorem that is used in the proof of other theorems.

Corollary: A proposition that can be established directly from a theorem.

Conjecture: A statement whose truth-value is unknown. If a proof can be found, then it becomes a theorem.

Example: (Goldbach's conjecture)

"Every even positive integer greater than 4 is the sum of two primes".

Direct proof: (forward reasoning)
Many theorems are implications:

$$p \rightarrow q$$

To prove, we need to show that whenever p is T, q is also T.
This implies that the case p true and q false never occurs.

Direct proof: (forward reasoning)
Many theorems are implications:

$$p \rightarrow q$$

To prove, we need to show that whenever p is T, q is also T.
This implies that the case p true and q false never occurs.

e.g. p q

Prove that, $\forall n \in Z$, if n is odd, then n^2 is odd.

n is odd $\Rightarrow$ $\exists k \in Z$ such that $n = 2k + 1 \Rightarrow n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

$\therefore$ n^2 is odd.

Many theorems are actually quantifications:

e.g.

Prove that, $\forall n \in Z$, if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

$\forall n \in Z \;\; P(n) \rightarrow Q(n)$

Indirect proof: (backward reasoning)

$p \rightarrow q \equiv \neg q \rightarrow \neg p$ (contrapositive)

Indirect proof: (backward reasoning)

$$p \rightarrow q \equiv \neg q \rightarrow \neg p \text{ (contrapositive)}$$

e.g.

Prove that, $\forall n \in Z$, if $3n + 2$ is odd, then n is odd.

Let n be even. Then $\exists k \in Z$ s.t. $n = 2k \Rightarrow 3n + 2 = 6k + 2 = 2(3k + 1)$

$\therefore$ $3n + 2$ is even too.

Proof by contradiction:

e.g. Prove that $\sqrt{2}$ is irrational.

Proof by contradiction:

e.g. Prove that $\sqrt{2}$ is irrational.

Suppose that $\sqrt{2}$ is **not** irrational, that is,
suppose $\sqrt{2} = a/b$, where a and b have no common factors

Proof by contradiction:

e.g. Prove that $\sqrt{2}$ is irrational.

Suppose that $\sqrt{2}$ is **not** irrational, that is,
suppose $\sqrt{2} = a/b$, where *a* and *b* have no common factors
$\Rightarrow 2 = a^2/\,b^2 \;\; \Rightarrow 2b^2 = a^2$
$\Rightarrow a^2$ is even $\Rightarrow a$ is even $\;\; \Rightarrow \exists c \in \mathrm{Z}$ s.t. $a = 2c$

$\therefore\; 2b^2 = 4c^2 \;\; \Rightarrow b^2 = 2c^2$
$\Rightarrow b^2$ is even $\Rightarrow$ b is even
$\therefore\; 2 \mid a \;\wedge\; 2 \mid b \;\Rightarrow\;$ *a* and *b* have common factors $\Rightarrow$ **contradiction!**
$\therefore\; \sqrt{2}$ is irrational.

Proof by contradiction:

e.g. Prove that $\sqrt{2}$ is irrational.

Suppose that $\sqrt{2}$ is not irrational, that is,
suppose $\sqrt{2} = a/b$, where *a* and *b* have no common factors
$\Rightarrow 2 = a^2/\, b^2 \quad \Rightarrow 2b^2 = a^2$
$\Rightarrow a^2$ is even $\Rightarrow a$ is even $\quad \Rightarrow \exists c \in \mathrm{Z}$ s.t. $a = 2c$

$\therefore\ 2b^2 = 4c^2 \quad \Rightarrow b^2 = 2c^2$
$\Rightarrow b^2$ is even $\Rightarrow$ b is even
$\therefore\ 2 \mid a \ \wedge\ 2 \mid b \ \Rightarrow$ *a* and *b* have common factors $\Rightarrow$ **contradiction!**
$\therefore\ \sqrt{2}$ is irrational.

Method: Suppose we want to prove p is true. We start assuming p is false and then proceed. If we end up with a contradiction, then we conclude that the assumption “p is false” is false, i.e., p is true.

Proof by cases:

$p \rightarrow q$ s.t. $p \equiv (p_1 \vee p_2 \vee \ldots \vee p_n)$

We can use the following logical equivalence:

$[\ (p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q\ ] \equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

Proof by cases:

$p \rightarrow q$ s.t. $p \equiv (p_1 \vee p_2 \vee \ldots \vee p_n)$

We can use the following logical equivalence:

$[\ (p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q\ ] \equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

e.g.

Prove that, $\forall n \in Z$, if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

Proof by cases:

$p \longrightarrow q$ s.t. $p \equiv (p_1 \vee p_2 \vee \ldots \vee p_n)$

We can use the following logical equivalence:

$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \equiv [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

e.g.

Prove that, $\forall n \in Z$, if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

q: $n^2 \equiv 1 \pmod 3$

p: n is not divisible by 3 $\Rightarrow$ p_1: $n \equiv 1 \pmod 3$, p_2 : $n \equiv 2 \pmod 3$ $\Rightarrow$ $p \equiv p_1 \vee p_2$

Proof by cases:

$p \rightarrow q$ s.t. $p \equiv (p_1 \vee p_2 \vee \ldots \vee p_n)$

We can use the following logical equivalence:

$[\,(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q\,] \;\equiv\; [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

e.g.

Prove that, $\forall n \in Z$, if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

q: $n^2 \equiv 1 \pmod 3$

p: n is not divisible by 3 $\Rightarrow$ p_1: $n \equiv 1 \pmod 3$, p_2 : $n \equiv 2 \pmod 3$ $\Rightarrow$ $p \equiv p_1 \vee p_2$

If p_1 is T:

$\exists k \in Z$ s.t. $n = 3k + 1 \Rightarrow n^2 = 9k^2 + 6k + 1 = 3\,(3k^2 + 2k) + 1$

$\Rightarrow n^2 \equiv 1 \pmod 3$

If p_2 is T:

$\exists k \in Z$ s.t. $n = 3k + 2 \Rightarrow n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$

$\Rightarrow n^2 \equiv 1 \pmod 3$

$\therefore (p_1 \rightarrow q) \wedge (p_2 \rightarrow q)$ is T $\Rightarrow$ $p \rightarrow q$ is T

e.g. (iff)

Prove that, $\forall n \in Z$, n is odd **if and only if** n^2 is odd.

p: n is odd, q: n^2 is odd $\Rightarrow$ Prove p $\leftrightarrow$ q

e.g. (iff)

Prove that, $\forall n \in Z$, n is odd **if and only if** n^2 is odd.

p: n is odd, q: n^2 is odd $\Rightarrow$ Prove $p \leftrightarrow q$

We have to show two things:

i) $p \rightarrow q$:
ii) $q \rightarrow p$:

e.g. (iff)

Prove that, $\forall n \in Z$, n is odd **if and only if** n^2 is odd.

p: n is odd, q: n^2 is odd $\Rightarrow$ Prove p $\leftrightarrow$ q

We have to show two things:

i) p $\rightarrow$ q: we already showed it.
ii) q $\rightarrow$ p: use indirect proof s.t. $\neg$p $\rightarrow$ $\neg$q

$\exists k \in Z$ s.t. $n = 2k \Rightarrow n^2 = 4k^2 = 2(2k^2)$ which is even.

Theorems and Quantifiers:

Constructive Existence proof:

Prove $\exists x$ P(x) : Find an a s.t. P(a) is true

Non-constructive existence proof:

$\exists x$ P(x) ? : Prove or disprove the existence of an a s.t. P(a) is true, without explicitly finding it.

Theorems and Quantifiers:

Constructive Existence proof:

Prove $\exists x$ P(x) : Find an a s.t. P(a) is true

Non-constructive existence proof:

$\exists x$ P(x) ? : Prove or disprove the existence of an a s.t. P(a) is true, without explicitly finding it.

Counter-example:

$\forall x$ P(x) ?

Find a for which P(a) is also false;
which means $\forall x$ P(x) is false.

e.g.

Show that 'all primes are odd' is false.

$x = 2$ even and prime

$\therefore$ it is false.