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
- development and verification of computer programs and algorithms
- design of computer circuits
- etc

By the end of this lecture, 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
- $1 + 1 = 2$
- $2 + 3 = 7$

- What time is it?
- Consider reading the material.

**Propositions**

- $x + 1 = 2$
- $x + y = z$

**Not Propositions**

- Use letters to denote propositions:
  - $p, q, r, s, \ldots$

  **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) \( \neg \)
- conjunction (AND) \( \land \)
- disjunction (OR) \( \lor \)
- exclusive or (XOR) \( \oplus \)
- implication (IF) \( \rightarrow \)
- biconditional (IFF) \( \leftrightarrow \)
Definition 1: Negation (NOT).

Let p be a proposition.

“It is not the case that p” is another proposition, called the negation of p. denoted as \( \neg p \) (not p)

e.g.

Proposition p: Today is Tuesday.
Negation of p: Today is not Tuesday

Truth table:

<table>
<thead>
<tr>
<th>p</th>
<th>( \neg p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>
**Definition 2: Conjunction (AND).**
Let p and q be propositions. The proposition “p and q” denoted by $p \land q$ is T when both p and q are true, is F otherwise.

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

**Definition 3: Disjunction (OR).**
Let p and q be propositions.

The proposition “p or q” denoted by $p \lor q$ is F when p and q are both false, is T otherwise.

The proposition $p \lor q$ is called the *disjunction* of p and q.
Definition 4: Exclusive Or (XOR).

Let p and q be propositions.

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.

- p: “Snow is white”
- q: “Snow is cold”

\[ p \oplus q = ?? \]
\[ p \land q = ?? \]
\[ p \lor q = ?? \]

Truth table:

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>p \land q</th>
<th>p \lor q</th>
<th>p \oplus q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Definition 5: Implication (IF).

Let p and q be propositions.

The implication \( p \rightarrow q \) is the proposition that is F when p is T and q is F is T otherwise.

\[
\begin{array}{|c|c|c|}
\hline
p & q & p \rightarrow q \\
\hline
T & T & T \\
T & F & F \\
F & T & T \\
F & F & T \\
\hline
\end{array}
\]

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
- q only if p
- p is sufficient for q
- q whenever p
- q is necessary for p
- q whenever p
- q follows from p
p → q

Converse: q → p

Contrapositive: ¬q → ¬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 6: Biconditional (IFF).**

Let p and q be propositions.

The biconditional \( p \iff q \) is the proposition that is T when p and q have same truth value and is F otherwise.

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>( p \iff q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

\( p \iff q \) is T if both \( p \rightarrow q \) is T and \( q \rightarrow p \) is T.

“\( p \text{ if and only if } q \)”

“\( p \) is necessary and sufficient for \( q \)”

“if \( p \) then \( q \), and conversely”

\( p \iff q \) is logically equivalent to say that \( p \rightarrow q \land q \rightarrow p \).
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.”
e.g.:

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

- “It is below freezing but not snowing.”
  \[p \land \neg q\]

- “It’s below freezing or it’s snowing; but it’s not snowing if it’s below freezing.”
  \[(p \lor q) \land (p \rightarrow \neg q)\]

and \(\approx\) but
**Logic and bit operations:**

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

Binary digit $\Rightarrow$ 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 $\iff$ Logical operations

$T \rightarrow 1, \quad F \rightarrow 0$

Bitwise OR, AND, XOR

\[
\begin{array}{c c}
1010 & 1110 \\
1100 & 0101 \\
1110 & 1111 & \text{bitwise OR} \\
1000 & 0100 & \text{bitwise AND} \\
0110 & 1011 & \text{bitwise XOR}
\end{array}
\]
1.3 Propositional Equivalences:

**Definition: Logical equivalence.**
The propositions (compound or not) r and s are logically equivalent if r and s have the same truth values, or more formally r ↔ s is a tautology.

Notation: \( r \equiv s \)

e.g.
Show that \( \neg(p \lor q) \equiv \neg p \land \neg q \) (De Morgan’s law)

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>p\lor q</th>
<th>\neg(p\lor q)</th>
<th>\neg p</th>
<th>\neg q</th>
<th>\neg p \land \neg q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
**Logical Equivalences**

\[
\begin{align*}
& \quad p \land T \equiv p \\
& \quad p \lor F \equiv p \quad \text{Identity laws}
\end{align*}
\]

\[
\begin{align*}
& \quad p \lor T \equiv T \\
& \quad p \land F \equiv F \quad \text{Domination laws}
\end{align*}
\]

\[
\begin{align*}
& \quad p \lor p \equiv p \\
& \quad p \land p \equiv p \quad \text{Idempotent laws}
\end{align*}
\]

\[
\begin{align*}
& \quad \neg(\neg p) \equiv p \quad \text{Double Negation law}
\end{align*}
\]

\[
\begin{align*}
& \quad p \lor q \equiv q \lor p \\
& \quad p \land q \equiv q \land p \quad \text{Commutative laws}
\end{align*}
\]

\[
\begin{align*}
& \quad (p \lor q) \lor r \equiv p \lor (q \lor r) \\
& \quad (p \land q) \land r \equiv p \land (q \land r) \quad \text{Associate laws}
\end{align*}
\]
\[ p \lor (q \land r) \equiv (p \lor q) \land (p \lor r) \]
\[ p \land (q \lor r) \equiv (p \land q) \lor (p \land r) \]
\[ \neg(p \land q) \equiv \neg p \lor \neg q \]
\[ \neg(p \lor q) \equiv \neg p \land \neg q \]
\[ \text{Distributive laws} \]
\[ \neg \neg(p \land q) \equiv p \lor q \]
\[ \neg \neg(p \lor q) \equiv p \land q \]
\[ \text{De Morgan’s laws} \]

**Some additional useful logical equivalences:**
\[ p \lor \neg p \equiv T \]
\[ p \land \neg p \equiv F \]
\[ (p \rightarrow q) \equiv (\neg p \lor q) \]
\[ (p \leftrightarrow q) \equiv (p \rightarrow q) \land (q \rightarrow p) \]
\[ (p \rightarrow q) \equiv (\neg q \rightarrow \neg p) \]

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.* $p \lor \neg p$  
$p \land \neg p$

tautology contradiction
e.g.
Show that \((p \land q) \rightarrow (p \lor q)\) is a tautology.

\[
(p \land q) \rightarrow (p \lor q) \equiv \neg(p \land q) \lor (p \lor q) \\
\equiv (\neg p \lor \neg q) \lor (p \lor q) \quad \text{De Morgan} \\
\equiv (\neg p \lor p) \lor (\neg q \lor q) \quad \text{Assoc & Comm} \\
\equiv T \lor T \\
\equiv T
\]

e.g.
Show that \(\neg(p \rightarrow q) \equiv p \land \neg q\)

e.g.
Show that \(\neg(p \leftrightarrow q) \equiv (p \lor q) \land (\neg p \lor \neg q)\)
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.

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>r</th>
<th>( p \rightarrow \neg q )</th>
<th>( q \rightarrow r )</th>
<th>( \neg r \rightarrow \neg p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Consistent!
1.4 Predicates and Quantifiers:

Subject   Predicate

Statement: $x$ is greater than 3

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  

\emph{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: \( x \in \{1,2,3,4\} \)

\[
\forall x \ P(x) \equiv P(1) \land P(2) \land P(3) \land P(4) \\
\equiv F
\]
**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)”

\[ \exists :\text{ Existential quantifier} \]

e.g.

\[ P(x): \ x > 3 \qquad x \in \{ \ldots, -1, 0, 1, \ldots \} \]

\[ \exists x \ P(x) \equiv T \]
e.g.

\[ P(x): \quad x = x + 1, \quad x \in \mathbb{R} \]

\[ \exists x \ P(x) \equiv \mathsf{F} \]

e.g.

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

\[ \exists x \ P(x) \equiv P(1) \lor P(2) \lor P(3) \lor P(4) \]
\[ \equiv \mathsf{T} \]
1.5 Nested Quantifiers:

Translating Sentences into Logical Expression

*E.g.*

“Everyone has *exactly* 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.
“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 $x.”$

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

$$\forall x \exists y \ \forall z \ B(x, y) \land ( (z \neq y) \rightarrow \neg B(x, z) )$$
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:**

\[ \neg(\forall x \ P(x)) \equiv \exists x \ \neg P(x) \equiv \exists x \ P(x) \text{ is false} \]

\[ \neg(\exists x \ P(x)) \equiv \forall x \ \neg P(x) \equiv \forall x \ P(x) \text{ is false} \]

e.g.

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

**Negation:**

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.

\[ \exists x \ P(x) \]

Negation of \( \exists x \ P(x) \)?
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 modified 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” \( \equiv \)?
In the previous example, what changes if the universe of discourse is modified 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” \( \equiv \)
\[
\exists x \ P(x) \land R(x)
\]

Negation: \( \forall x \ \neg P(x) \lor \neg R(x) \equiv \forall x \ P(x) \rightarrow \neg R(x) \equiv \forall x \ R(x) \rightarrow \neg P(x) \) 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.

e.g.

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

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

$\neg \exists x \ P(x) \equiv \neg(P(1) \lor P(2) \lor P(3) \lor P(4))$

$\equiv \neg P(1) \land \neg P(2) \land \neg P(3) \land \neg P(4)$ by De Morgan’s rule

$\equiv \forall x \ \neg P(x)$
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 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 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 “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 $x$”.

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

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

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

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

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

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

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

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

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

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

“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):

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

“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 \( x \).”

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.”