Chapter 1 The Foundations: Logic and Proofs

1.1 Propositional Logic

A **proposition** is a declarative sentence that is either true or false, but not both.

- **Negation** $\neg$ (NOT)
- **Conjunction operator** $\wedge$ (AND)
- **Disjunction operator** $\vee$ (OR)
- **Exclusive or operator** $\oplus$ (XOR)

  Exactly one of p and q is true for the XOR to be true.
- **Conditional operator** $\rightarrow$ (IF--THEN)

  The conditional statement is false only when p is true and q is false

  If p, then q
  p implies q
  If p, q
  q if p
  q when p
  q follows from p
  q whenever p
  p is a sufficient condition for q
  q is a necessary condition for p
  p only if q
  q unless $\neg$p
- **Biconditional operator** $\leftrightarrow$ (IF AND ONLY IF)

  Both p and q must have the same truth value for $p \leftrightarrow q$ to be true.

- Parentheses() get the highest precedence. Then $\neg$ $\wedge$ $\vee$ $\rightarrow$ $\leftrightarrow$
- **Bitwise Operations**

  01 1011 0110
  11 0001 1101
  11 1011 1111 bitwise OR
  01 0001 0100 bitwise AND
  10 1010 1011 bitwise XOR

1.2 Applications of Propositional Logic

Consistent System Specifications

A list of propositions is ***consistent*** if it is possible to assign truth values to the proposition variables so that each proposition is true.

1.3 Propositional Equivalences

Tautology : compound proposition that is always true
Contradiction : compound proposition that is always false.
Contingency: compound proposition that is neither a tautology nor a contradiction.

TABLE 6 Logical Equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

TABLE 7 Logical Equivalences Involving Conditional Statements.

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

TABLE 8 Logical Equivalences Involving Biconditional Statements.

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

- The proposition p *NOR* q is true when both p and q are false, and it is false otherwise. The operator $\downarrow$ is called Peirce arrow.

Propositional Satisfiability:

A compound proposition is ***satisfiable*** if there is an assignment of truth values to its variables that make it true. When no such assignments exist, the compound proposition is ***unsatisfiable***.

A compound proposition is unsatisfiable if and only if its negation is a tautology.

1.4 Predicates and Quantifiers

A **predicate** (propositional function) is a statement that contains variables. Once the values of the variables are specified, the function has a truth value.

Universal Quantification

A universal quantification of $P(x)$, denoted by $\forall\, x\, P(x)$, is the statement "$P(x)$ for all values of x in the domain(range of the possible values of the variable x).

For all
For every
All of
For each
Given any
For arbitrary
For any

Given the domain as $\{x_1, x_2, \cdots, x_n\}$,

$$\forall x P(x) \equiv P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

Existential Quantification

An existential quantification of $P(x)$, denoted by $\exists\, x\, P(x)$, is the statement "There exists an element x in the domain such that $P(x)$.

For some x P(x)
There is an x such that P(x)
There is at least one x such that P(x)

Given the domain as $\{x_1, x_2, \cdots, x_n\}$,

$$\exists x P(x) \equiv P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

Uniqueness quantifier: $\exists!$ or $\exists_1$

$\exists!\ P(x)$or $\exists_1 P(x)$: There exists a unique x such that $P(x)$ is true.

- The quantifiers $\exists$ and $\forall$ have higher precedence than all logical operators from propositional calculus.
- **All the variables in a propositional function must be quantified or set equal to a particular value to turn it into a proposition.**
- **Scope of a quantifier**: the part of a logical expression to which the quantifier is applied

$$\forall x(A(x) \wedge B(x)) \quad \equiv \quad \forall x A(x) \wedge \forall x B(x)$$
$$\exists x(A(x) \vee B(x)) \quad \equiv \quad \exists x A(x) \vee \exists x B(x)$$
$$\forall x(A(x) \vee B(x)) \quad \not\Leftrightarrow \quad \forall x A(x) \vee \forall x B(x)$$
$$\exists x(A(x) \wedge B(x)) \quad \not\Leftrightarrow \quad \exists x A(x) \wedge \exists x B(x)$$

De Morgan's laws for quantifiers

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

Translating from English into Logical Expressions

- **Tips**
  - All $S(x)$ are $O(x)$: $\forall x\ (S(x) \to O(x))$
  - No $S(x)$ are $O(x)$: $\forall x\ (S(x) \to \neg\ O(x))$
  - Some $S(x)$'s are $O(x)$: $\exists x\ (S(x) \wedge O(x))$
  - Some $S(x)$ are not $O(x)$: $\exists x\ (S(x) \wedge \neg\ O(x))$

1.5 Nested Quantifiers

Two quantifiers are nested if one is within the scope of the other.

- **The order of nested quantifiers matters if quantifiers are of different types**

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

$\exists x \forall y P(x, y)$ **is not the same as** $\forall y \exists x P(x, y)$

TABLE 1 Quantifications of Two Variables.

Statement	*When True?*	*When False?*
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Disjunctive (Conjunctive) Clauses

Disjunctions (conjunctions) with one or more literals (**Literal:** p or $\neg p$) as disjuncts (conjuncts) are called ***disjunctive (conjunctive) clauses.*** Disjunctive and conjunctive clauses are simply called clauses.

Conjunctive Normal Form (CNF)

A conjunction with one or more disjunctive clauses as its conjuncts is said to be in ***conjunctive normal form***.

$$(A_{11} \vee \ldots \vee A_{1n_1}) \wedge \ldots \wedge (A_{k1} \vee \ldots \vee A_{kn_K})$$

Disjunctive Normal Form (DNF)

A disjunction with one or more conjunctive clauses as its disjuncts is said to be in ***disjunctive normal form***.

$$(A_{11} \wedge \ldots \wedge A_{1n_1}) \vee \ldots \vee (A_{k1} \wedge \ldots \wedge A_{kn_K})$$

How to Obtain Normal Forms: Use logical Equivalences

1) $p \to q \Leftrightarrow \neg p \vee q$
2) $p \leftrightarrow q \Leftrightarrow (\neg p \vee q) \wedge (p \vee \neg q)$
3) $p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$
4) $\neg\neg p \Leftrightarrow p$

5) $\neg(p_1 \wedge \ldots \wedge p_n) \Leftrightarrow \neg p_1 \vee \ldots \vee \neg p_n$

6) $\neg(p_1 \vee \ldots \vee p_n) \Leftrightarrow \neg p_1 \wedge \ldots \wedge \neg p_n$

7) $p \wedge (q_1 \vee \ldots \vee q_n) \Leftrightarrow (p \wedge q_1) \vee \ldots \vee (p \wedge q_n)$

$(q_1 \vee \ldots \vee q_n) \wedge p \Leftrightarrow (p \wedge q_1) \vee \ldots \vee (p \wedge q_n)$

8) $p \vee (q_1 \wedge \ldots \wedge q_n) \Leftrightarrow (p \vee q_1) \wedge \ldots \wedge (p \vee q_n)$

$(q_1 \wedge \ldots \wedge q_n) \vee p \Leftrightarrow (p \vee q_1) \wedge \ldots \wedge (p \vee q_n)$

- By (1)–(3) we eliminate $\rightarrow$ and $\leftrightarrow$.
- By (4)–(6) we eliminate $\neg$, $\wedge$, $\vee$, from the scope of $\neg$ such that any $\neg$ has only a literal as its scope.
- By (7) we eliminate $\vee$ from the scope of $\wedge$.
- By (8) we eliminate $\wedge$ from the scope of $\vee$.

Full Disjunctive Normal Form

A ***minterm*** is a conjunction of literals in which **each variable is represented exactly once.**

If a formula is expressed as a disjunction of minterms, it is said to be in ***full disjunctive normal form***.

$$(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$$

Transforming to Full Disjunctive Normal Form

1. Obtain disjunctive normal form,
2. Make use of negation laws and distributive laws to obtain full disjunctive normal form.

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

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

Full Disjunctive Normal Form from Truth Table

$$f = (p \wedge q) \vee (\neg p \wedge r) \vee (q \wedge r)$$

p	q	r	f
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	T
F	F	F	F

$$f \equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$$

Prenex Normal Form

A statement is in ***prenex normal form*** iff it is of the form $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n B$, where $Q_i (i = 1, \cdots, n)$ is $\forall$ *or* $\exists$ and the predicate B is quantifier free.

- Any expression can be converted into a prenex normal form.

Transforming to Prenex Normal Form

1. Eliminate all occurrences of $\rightarrow$ and $\leftrightarrow$ from the formula in question;
2. Move all negations inward such that, in the end, negations only appear as part of literals;
3. Rename the variables (when necessary);
4. The prenex normal form can now be obtained by moving all quantifiers to the front of the formula.

Step 1:

1. $A \rightarrow B \Leftrightarrow \neg A \vee B$
2. $A \leftrightarrow B \Leftrightarrow (\neg A \vee B) \wedge (A \vee \neg B)$
3. $A \leftrightarrow B \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$

Step 2:

4. $\neg\neg A \Leftrightarrow A$
5. $\neg \exists x A(x) \Leftrightarrow \forall x \neg A(x)$
6. $\neg \forall x A(x) \Leftrightarrow \exists x \neg A(x)$

Step 3: Rename all variables in the statement

Step 4:

$A \wedge \exists x B(x) \Leftrightarrow \exists x\, (A \wedge B(x))$

$A \wedge \forall x B(x) \Leftrightarrow \forall x\, (A \wedge B(x))$

$A \vee \exists x B(x) \Leftrightarrow \exists x\, (A \vee B(x))$

$A \vee \forall x B(x) \Leftrightarrow \forall x\, (A \vee B(x))$

$\forall x \forall y\, A(x,y) \Leftrightarrow \forall y \forall x\, A(x,y)$

$\exists x \exists y\, A(x,y) \Leftrightarrow \exists y \exists x\, A(x,y)$

$Q_1 x A(x) \wedge Q_2 y B(y) \Leftrightarrow Q_1 x Q_2 y (A(x) \wedge B(y))$

$Q_1 x A(x) \vee Q_2 y B(y) \Leftrightarrow Q_1 x Q_2 y (A(x) \vee B(y))$

Prenex CNF and DNF

Step1: Prenex normal form

Step 2: Prenex DNF or CNF

1.6 Rules of Inference

Using Rules of Inference to Build Arguments

- An argument is valid if

whenever all premises are true, the conclusion is also true

- To prove that an argument is valid:

Assume the premises are true

Use the rules of inference and logical equivalences to determine that the conclusion is true

If the conclusion is given in a form of $p \rightarrow q$, we can convert the argument $p_1 \wedge p_2 \wedge \cdots \wedge p_n \rightarrow (p \rightarrow q)$

to $p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge p \rightarrow q$

Because

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge p) \rightarrow q \equiv (p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow (p \rightarrow q)$$

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

Resolution rule

proposition $p \vee (q \wedge r)$ can be written as

two clauses $p \vee q$ and $p \vee r$

TABLE 2 Rules of Inference for Quantified Statements.

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

Universal modus ponens

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

$P(a)$, where a is a particular element in the domain

$\therefore Q(a)$

Universal modus tollens

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

$\neg Q(a)$, where a is a particular element in the domain

$\therefore \neg P(a)$

1.7 Introduction to Proofs

Some Terminology

- A **proof** is a valid argument that establishes the truth of a mathematical statement.
- A **theorem** 定理 (proposition/fact/result) is a statement that can be shown to be true.
- **Axioms** 公理 (postulates 假定) are statements we assume to be true
- A **lemma** 引理 is a less important theorem that is helpful in the proof of other results
- A **corollary** 推论 is a theorem that can be established directly from a theorem that has been proved.
- A **conjecture** 猜想 is a statement that is being proposed to be a true statement
  A conjecture becomes a theorem once it has been proved to be true.

Direct Proofs

$P(c) \rightarrow Q(c)$

- Assumes the hypotheses $P(c)$ are true
- Uses the rules of inference, axioms and any logical equivalences to establish the truth of the conclusion $Q(c)$

Proof by Contraposition

$P \rightarrow Q \equiv \neg Q \rightarrow \neg P$

- Assumes that $\neg Q$ is true
- Uses the rules of inference, axioms and any logical equivalences to establish $\neg P$ is true

Vacuous Proof

- If we know P is false then $P \rightarrow Q$ is *vacuously* true.
- F → T and F → F are both true.

Trivial Proof

- If we know Q is true, then $P \rightarrow Q$ is true
- F → T and T → T are both true.

Proof *p* by Contradiction

- assumes p is false, $\neg p$ is true
- deduces 推出 that $\neg p \rightarrow (q \wedge \neg q)$, which $q \wedge \neg q$ is a contradiction
- hence ¬p is false, so that p is true

Proof $p \rightarrow q$ by Contradiction

- assumes that both p and $\neg q$ are true
- shows that $(p \wedge \neg q) \rightarrow \mathrm{F}$, We have obtained a contradiction
- hence $p \wedge \neg q$ s false, p → q is ture

prove that several propositions p_1 , p_2,...,p_n are equivalent

- establish the implications $p_1 \rightarrow p_2$, ..., $p_{n-1} \rightarrow p_n$, $p_n \rightarrow p_1$

  $[p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n] \equiv [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge ... \wedge (p_n \rightarrow p_1)]$

1.8 Proof Methods and Strategy

Proof by Cases

- Break the premise of $p \rightarrow q$ into an equivalent disjunction of the form $p_1 \vee p_2 \vee \ldots \vee p_n$
- Then use the rule $((p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q) \equiv ((p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q))$

Existence Proof

We wish to establish the truth of $\exists x P(x)$

Constructive existence proof:

- Establish $P(c)$ is true for some c in the domain.
- Then $\exists x P(x)$ is true by Existential Generalization (EG).

Nonconstructive existence proof:

- Assume no c exists which makes $P(c)$ true and derive a contradiction

Uniqueness Proof

To show that a theorem assert the existence of a unique element with a particular property.

$\exists x\ (P(x) \wedge \forall\ y\ (y \neq x \rightarrow \neg P(y)))$

There are two parts of a *uniqueness proof*:

- *Existence*: We show that an element *x with* the desired property exists.
- *Uniqueness*: We show that if $y \neq x$, then y does not have the desired property. Equivalently, we can also show that if x and y both have the desired property, then $x=y$.