Contents

1 Logic and Proofs

1.1 Propositional Logic

Proposition is a statement that is **either** true or false, but not both at the same time. We usually represent it with variables like p, q, and r.
e.g. "The sky is blue." is a proposition, but "Listen to me" is not.

1.1.1 Logical Connectives

- Negation: $\neg p$. It is not the case that p.
- Conjunction: $p \wedge q$. "and"
- Disjunction: $p \vee q$. "or"
- Implication: $p \to q$. If p then q, q if p, q is a consequence of p, p only if q
- biconditional: $p \leftrightarrow q$. $(p \to q) \wedge (q \to p)$, p if and only if q

1.1.2 Variations of Conditionals

- Implication: $p \to q$
- Converse: $q \to p$
- Inverse: $\neg p \to \neg q$
- Contrapositive: $\neg q \to \neg p$. This is logically equivalent to Implication

Truth Table

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

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

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

Example

Find the truth value of $\boldsymbol{(p \vee q) \to \neg r}$

p	q	r	$p \vee q$	$\neg r$	$(p \vee q) \to \neg r$
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	T	T
F	T	T	T	F	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	F	T	T

1.2 Application of Propositional Logic

1.2.1 Classification of Proposition

- Tautology: Always true. e.g. $p \lor \neg p$
- Contradiction: Always false. e.g. $p \land \neg p$
- Contingency: Depends on variable. e.g. $p \to q$

1.2.2 Logical Equivalence $p \equiv q$

Two statements are logically equivalent if they always have the same truth value in every possible scenario.
e.g. p and q are biconditional, i.e. $p \leftrightarrow q$, means that p and q are logically equivalent.

1.2.3 Laws of Logical Equivalence

Equivalence	Name
$p \land T \equiv p$ $p \lor F \equiv p$	Identity laws
$p \lor T \equiv T$ $p \land F \equiv F$	Domination laws
$p \lor p \equiv p$ $p \land p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \lor q \equiv q \lor p$ $p \land q \equiv q \land p$	Commutative laws
$(p \lor q) \lor r \equiv p \lor (q \lor r)$ $(p \land q) \land r \equiv p \land (q \land r)$	Associative laws
$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$ $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$	Distributive laws
$\neg(p \land q) \equiv \neg p \lor \neg q$ $\neg(p \lor q) \equiv \neg p \land \neg q$	De Morgan's laws
$p \lor (p \land q) \equiv p$ $p \land (p \lor q) \equiv p$	Absorption laws
$p \lor \neg p \equiv T$ $p \land \neg p \equiv F$	Negation laws
$p \to q \equiv \neg p \lor q$ $p \to q \equiv \neg q \to \neg p$	Conditional
$p \leftrightarrow q \equiv (p \to q) \land (q \to p)$ $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$	Biconditional

1.2.4 Determine Logical Equivalence:

1. Verify with Truth Table
2. Apply Known knowledge

Show that $p \to q$ is logically equivalent to $\neg q \to \neg p$

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

Show that $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

$$\begin{aligned}(p \to r) \vee (q \to r) &\equiv (\neg p \vee r) \vee (\neg q \vee r) \\ &\equiv (\neg p \vee \neg q) \vee (r \vee r) \\ &\equiv \neg(p \wedge q) \vee r \\ &\equiv (p \wedge q) \to r_{\#}\end{aligned}$$

1.3 Predicate and Quantifier

1.3.1 Predicate

A predicate is a statement with variables that becomes true or false only once specific values are substituted. $P(x)$ denotes a predicate involving x.
e.g. Let $P(x)$ be the statement "x¿4." We read $P(x)$ as "x is greater than 4."

- $P(x)$ is true if x = 5
- $P(x)$ is false if x = 3

General Form

$P(x_1, x_2, x_3, \ldots, x_n)$ where each x_i is a variable from the domain of discourse.

1.3.2 Quantifier

- Universal quantifier $\forall$: "for all", "every".
- Existential quantifier $\exists$: "there exists", "some", "at least one".

Rules for Quantifier

Negation of quantifier

$$\begin{cases}\neg\forall x\, P(x) \equiv \exists x\, \neg P(x) \\ \neg\exists x\, P(x) \equiv \forall x\, \neg P(x)\end{cases}$$

Nested quantifier

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

Negation of nested quantifier

$$\neg\left(\forall x\,\exists y\,P(x,y)\right) \equiv \exists x\,\forall y\,\neg P(x,y)$$
$$\neg\left(\exists x\,\forall y\,P(x,y)\right) \equiv \forall x\,\exists y\,\neg P(x,y)$$

1.4 Rule of Inference

An **argument** is an implication of the form:

$$\bigwedge_{i\in D} p_i \to q$$

where D is domain of discourse, p_i is a premise, and q is a conclusion
Notation:

$$(p\to q)\wedge p \quad \therefore q \quad \Rightarrow \quad \begin{array}{ll} & p\to q \\ \wedge & p \\ \hline \therefore & q \end{array} \quad \Rightarrow \quad \begin{array}{l} p\to q \\ p \\ \hline \therefore q \end{array}$$

Name	Expression	Name	Expression
Modus Ponens	$\begin{array}{l} p\to q \\ p \\ \hline \therefore q \end{array}$	Modus Tollens	$\begin{array}{l} p\to q \\ \neg q \\ \hline \therefore \neg p \end{array}$
Hypothetical Syllogism	$\begin{array}{l} p\to q \\ q\to r \\ \hline \therefore p\to r \end{array}$	Conjunction	$\begin{array}{l} p \\ q \\ \hline \therefore p\wedge q \end{array}$
Disjunctive Syllogism	$\begin{array}{l} p\vee q \\ \neg p \\ \hline \therefore q \end{array}$	Addition	$\begin{array}{l} p \\ \hline \therefore p\vee q \end{array}$
Simplification	$\begin{array}{l} p\wedge q \\ \hline \therefore p \\ \therefore q \end{array}$	Resolution	$\begin{array}{l} p\vee q \\ \neg p\vee r \\ \hline \therefore q\vee r \end{array}$

Rules for Quantified Statement

Universal Instantiation: From a universal statement $\forall x\,P(x)$, we may infer $P(c)$ for any particular c.

$$\forall x\,P(x) \quad\Rightarrow\quad P(a)$$

Universal Generalization: If $P(c)$ holds for an arbitrary element c, then we may conclude $\forall x\,P(x)$.

$$P(c) \quad\Rightarrow\quad \forall x\,P(x)$$

Existential Instantiation: From $\exists x\,P(x)$, we may introduce a new symbol c such that $P(c)$ holds.

$$\exists x\,P(x) \quad\Rightarrow\quad P(c)$$

Existential Generalization: From $P(c)$ for a particular c, we may conclude $\exists x\, P(x)$.

$$P(c) \quad \Rightarrow \quad \exists x\, P(x)$$

1.5 Introduction to Proofs

1.5.1 Some Mathematical Terminology

- **Theorem:** A major, important mathematical statement that has been proved true.
- **Lemma:** A proved result used mainly as a stepping stone toward a larger theorem.
- **Corollary:** A statement that follows directly and easily from a theorem or proposition.
- **Proposition:** A proved statement that is true but of smaller or less central importance than a theorem.
- **Conjecture:** A mathematical claim believed to be true but not yet proved.
- **Proof:** A logical argument that establishes the truth of a mathematical statement beyond doubt.

1.5.2 Types of Proof

- **Direct Proof:** Show a statement is true by straightforward logical reasoning from definitions and known results.

  Example: Prove that if n is odd, then $5n + 3$ is even.
  Proof:
  Let $n = 2k + 1, k \in \mathbb{Z}$, then

  $$5n + 3 = 2(2k + 1) + 3 = 10n + 8 = 2(5k + 4)$$

  So, $5n + 3 = 2(5k + 4)$ and $5k + 4 \in \mathbb{Z}$

  $$\therefore 5n + 3 \text{ is even}_{\#}$$

- **Proof by Contrapositive:** Show a statement is true by proving that if the conclusion is false, then the premise must also be false.

  Example: Prove that if n is odd, then $5n + 3$ is even.
  Proof:

- **Proof by Contradiction:** Show a statement is true by assuming the opposite and deriving a contradiction.

  Example: Prove that $\sqrt{2}$ is irrational
  Proof:
  Let

  $$\sqrt{2} = \frac{p}{q},\ q \neq 0,\ p, q \in \mathbb{N},\ \gcd(p, q) = 1$$
  $$\Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$$

Thus, $2 \mid p^2$, so $2 \mid p$. We have

$$p = 2k,\ k \in \mathbb{N},\ 4k^2 = 2q^2 \Rightarrow 2k^2 = q^2$$

Similarly, $2 \mid q$. Concluding

$$2 \mid \gcd(p,q) \Rightarrow\!\Leftarrow$$

Thus $\sqrt{2}$ is irrational.

- **Proof by Cases:** Show a statement is true by dividing into cases and proving it holds in each case.

  Example:
  Proof:

- **Methametical Induction:** Show a statement is true by proving a base case and then proving the inductive step from n to n+1.

  Example:
  Proof:

- **Existence and Uniqueness Proof** Show a statement is true by first proving that at least one object with the required property exists (existence), and then proving that no more than one such object can exist (uniqueness).

  Example: Prove that if $r \in \mathbb{Q}^c$, then $\exists!\, n \in \mathbb{Z}\ |r - n| < \dfrac{1}{2}$.
  Proof:
  Let

  $$n = \lfloor r + \frac{1}{2} \rfloor$$

  By definition we have

  $$n \le r + \frac{1}{2} < n + 1$$

  Hence

  $$|r - n| < \tfrac{1}{2}$$

  , so such an integer n exists. (Existence)
  Suppose

  $$\exists m,\ m \neq n,\ |r - m| < \frac{1}{2}$$

  Consider

  $$\begin{aligned} |n - m| &= |(n - r) + (r - m)| \\ &\le |n - r| + |r - m| \\ &= \frac{1}{2} + \frac{1}{2} = 1 \end{aligned}$$

  Since n and m are integers, the inequality $|n - m| < 1$ implies $n = m$. Therefore, the integer n is unique. (Uniqueness)

2 Sets

2.1 Definition and Notation

A **set** is a well-defined collection of distinct objects, called **elements**. If a is an element of the set A, we write $a \in A$. If a is not an element of A, we write $a \notin A$. Sets are usually denoted by capital letters $A, B, C \ldots$

- Roster Method: List all of its elements within curly braces $\{a, b, c, \ldots\}$
- Set-builder Notations: $\{x \mid \text{condition on } x\}$

Example: The set of all positive integers less than 100: $\{x \in \mathbb{Z}^+ \mid x < 100\}$

2.2 Common Sets of Numbers and their Definitions

- $\mathbb{N}$: The set of **natural numbers**. (Sometimes defined to include 0.)

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

- $\mathbb{Z}$: The set of **integers**. These can be expressed as the difference of two natural numbers.

$$\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}\}$$

- $\mathbb{Q}$: The set of **rational numbers**. These are ratios of two integers with nonzero denominator.

$$\mathbb{Q} = \left\{\frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0\right\}$$

- $\mathbb{R}$: The set of **real numbers**. Formally constructed as the set of equivalence classes of The limits of infinite convergent Cauchy sequences of rational numbers. That is,

$$\mathbb{R} = \left\{\lim_{n\to\infty} a(n) \mid a : \mathbb{N} \to \mathbb{Q}, \forall \epsilon > 0, \exists N \in \mathbb{N}, |a(n) - a(N)| < \epsilon\right\}$$

  where a sequence $a(n)$ is *Cauchy* if $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ such that $\forall m, n > N$, $|a(m) - a(n)| < \varepsilon$.

- $\mathbb{C}$: The set of **complex numbers**. Defined as ordered pairs of real numbers with special addition and multiplication rules

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1\}.$$

2.3 Subsets, Subsets, Cardinality, and Power Sets

Subsets: A set A is a subset of B if every element of A is also in B.

$$A \subseteq B \iff \forall x\ (x \in A \implies x \in B)$$

Proper Subsets: A set A is a proper subset of B if $A \subseteq B$ and $A \neq B$.

$$A \subset B \iff A \subseteq B \text{ and } A \neq B$$

Cardinality: The number of elements in a set A, denoted $|A|$.

$$|\{1, 2, 3\}| = 3, \quad |\varnothing| = 0$$

Power Set: The set of all subsets of A.

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}, \quad |\mathcal{P}(A)| = 2^{|A|}$$

2.4 Set Operations

- Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- Difference: $A - B$ or $A/B = \{x \mid x \in A \text{ and } x \notin B\}$
- Complement: $\bar{A}$ or $A^c = \{x \in U \mid x \notin A\}$
- Cartesian Product of A and B is defined by:

  $$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}$$

  if $A_1 = A_2 = \cdots = A_n$, then $A_1 \times A_2 \times \cdots \times A_n = A_1^n$

3 Functions

3.1 Definition and Notation

A function f from a set A to B, written $f : A \to B$ is a mapping defined by

$$a \in A \to f(a) \in B$$

To check if $f : A \to B$ is a function

1. Algebraically: if $a_1 = a_2$, then it follows $f(a_1) = f(a_2)$
2. Geometrically: Vertical Line Test, i.e., for every vertical line $x = a$, the graph of f interescts the line in at most one point.

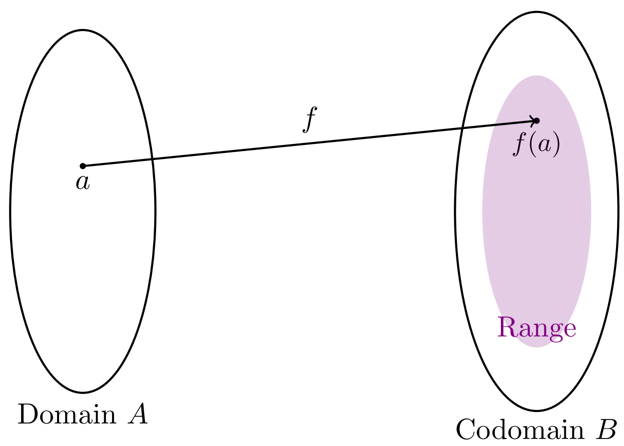
3.2 Domain, Codomain, and Range

Let $f : A \to B$ be a function.

- The set A is called the **domain** of f.
- The set B is called the **codomain** of f.
- For each $a \in A$, the element $f(a) \in B$ is called the **image** of a under f.
- The set

  $$\text{Range}(f) = \{f(a) \mid a \in A\}$$

  is called the **range** (or image) of f. Note that $\text{Range}(f) \subseteq B$, i.e., the range is always a subset of the codomain.



3.3 One-to-one and Onto

Let $f : A \to B$ be a function.

- f is **onto (surjective)** if for every $b \in B$, there exists at least one a such that $f(a) = b$.

$$\forall b \in B, \exists a \in A, f(a) = b$$

- f is **one-to-one (injective)** if for every $b \in B$, there exists only one a such that $f(a) = b$.

$$\forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

- f is **bijective** if f is both **surjective** and **injective**. Bijection is also called one-to-one correspondenc.

3.4 Sum and Product

Let f_1, f_2 be functions $A \to B$. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from $A \to B$.
Defined for all $x \in A$

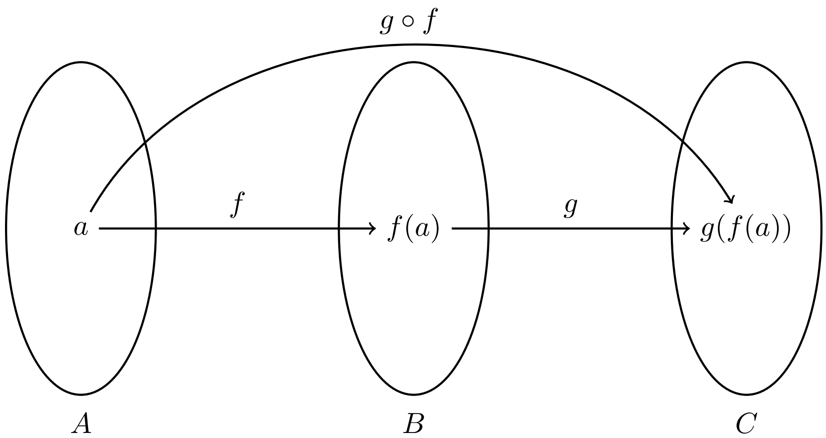
$$f_1(x) + f_2(x) = (f_1 + f_2)(x)$$
$$f_1(x) \cdot f_2(x) = (f_1 f_2)(x)$$

3.5 Composite and Inverse Function

3.5.1 Composite Function

Let $f : A \to B$ and $g : B \to C$. We denote function composition as $g \circ f : A \to C$, where

$$(g \circ f)(x) = g(f(x))$$



3.5.2 Inverse Function

A function $f : A \to B$ has inverse $f^{-1} : B \to A$ such that

$$f^{-1}(b) = a \iff f(a) = b$$

if f is **bijective**.