Study Guide

MATH 163: Discrete Mathematics 1 Fall 2022

Dr. Petrescu

Final: Monday, December 12, 2022

Denny Cao

December 10, 2022

Contents

1 Logic and Proofs

1.1 Propositional Logic

1.1.2 Propositions

Definition 1.1. Proposition: A statement that is either true or false.

p	$\neg p$
T	F
F	T

Figure 1: Truth table for **negation**

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

Figure 2: Truth table for **bit operations**

1.1.3 Conditional Statements

Definition 1.2. Conditional Statement: A statement of the form $p \rightarrow q$. The conditional statement is called the *hypothesis* (or *antecedent* or *premise*) and q is called the *conclusion* (or *consequence*).

Definition 1.3. Converse: The proposition $q \rightarrow p$ is the converse of the proposition $p \rightarrow q$.

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

Figure 3: Truth Table for converse of implication of two propositions p and q

Definition 1.4. Contrapositive: The proposition $\neg q \rightarrow \neg p$ is the contrapositive of the proposition $p \rightarrow q$.

- Same truth value as $p \rightarrow q$

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

Figure 4: Truth Table for contrapositive of implication of two propositions p and q

Definition 1.5. Inverse: The proposition $\neg p \to \neg q$ is the inverse of the proposition $p \to q$.

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

Figure 5: Truth Table for inverse of implication of two propositions p and q

1.1.5 Precedence of Logical Operators

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\to$	4
$\leftrightarrow$	5

Figure 6: Precedence of Logical Operators

1.3 Propositional Equivalences

1.3.1 Introduction

Definition 1.6. Tautology: A compound proposition that is always true.

Definition 1.7. Contradiction: A compound proposition that is always false.

Definition 1.8. Contingency: A compound proposition that is neither a tautology nor a contradiction.

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

Figure 7: Truth Table of an example of a Tautology and Contradiction

1.3.2 Logical Equivalences

Definition 1.9. Two propositions are **logically equivalent** if $p \leftrightarrow q$ is a tautology.

The following are important logical equivalences:

De Morgan's Laws
$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
$\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$

Conditional-Disjunction Equivalence
$p \to q \leftrightarrow \neg p \vee q$

Here are some other logical equivalences:

Logical Equivalences	
Equivalence	Name
$p \wedge \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Identity Laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \vee \mathbf{F} \equiv \mathbf{F}$	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

Logical Equivalences Involving Conditional Statements
$p \to q \equiv \neg p \vee q$
$p \to q \equiv \neg q \to \neg p$
$p \vee q \equiv \neg p \to q$
$p \wedge q \equiv \neg(\neg p \vee \neg q) \equiv \neg(p \to \neg q)$
$\neg(p \to q) \equiv p \wedge \neg q$
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$
$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

Logical Equivalences Involving Biconditonal Statements
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

$$\bigvee_{i=1}^{n} p_i = p_1 \vee p_2 \vee \cdots \vee p_n$$

$$\bigwedge_{i=1}^{n} p_i = p_1 \wedge p_2 \wedge \cdots \wedge p_n$$

By De Morgan's laws, it follows that:

$$\neg \bigvee_{i=1}^{n} p_i = \bigwedge_{i=1}^{n} \neg p_i$$

1.3.5 Satisfiability

Definition 1.10. A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that makes it true (When it is a tautology or a contigency).

Definition 1.11. A compound proposition is **unsatisfiable** if there is no assignment of truth values to its variables that makes it true (When it is a contradiction). To prove this, we can prove that the negation is a tautology.

1.4 Predicates and Quantifiers

1.4.2 Predicates

Definition 1.12. A **statement** contains 2 parts: a **subject** and a **predicate**.

- In the statement, x is greater than 3, x is the subject and greater than 3 is the predicate.
- The statement $P(x)$ is said to be the value of the **propositional function** P at x.

1.4.3 Quantifiers

Definition 1.13. Universal Quantifier: $\forall x P(x)$. $P(x)$ for all values of x in the domain.

- An element for which $P(x)$ is false is called a **counterexample**.

Definition 1.14. Existential Quantifier: $\exists x P(x)$. There exists an element x in the domain such that $P(x)$ is true.

Definition 1.15. Uniqueness Quantifier: $\exists! x P(x)$. There exists exactly one element x in the domain such that $P(x)$ is true.

A way to think about determining the truth value of quantifiers is to think about looping. To determine if $\forall x P(x)$ is true, we loop through all the elements in the domain and check if $P(x)$ is true for all of them. To determine if $\exists x P(x)$ is true, we loop through all the elements in the domain and check if $P(x)$ is true for at least one of them.

1.4.4 Quantifiers Over Finite Domains

When domain is finite, we can express statements using propositional logic:

$$\forall x P(x) \equiv \bigwedge_{i=1}^{n} P(x)$$

$$\exists x P(x) \equiv \bigvee_{i=1}^{n} P(x)$$

1.4.6 Precedence of Quantifiers

$\forall x$ and $\exists x$ have higher precedence than all logical operators from propositional calculus. For instance, $\forall P(x) \vee Q(x) \equiv (\forall P(x)) \vee Q(x)$.

1.4.8 Negating Quantified Expressions

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

Figure 8: De Morgan's Laws for Quantifiers

1.5 Nested Quantifiers

Statement	When True	When False
$\forall x \forall y P(x, y)$	$P(x, y)$ is true for all values of x and y	$\exists x \exists y \neg P(x, y)$
$\forall x \exists y P(x, y)$	For every x there is a y such that $P(x, y)$ is true	$\exists x \forall y \neg P(x, y)$
$\exists x \forall y P(x, y)$	There is an x such that $P(x, y)$ is true for all values of y	$\forall x \exists y \neg P(x, y)$
$\exists x \exists y P(x, y)$	There is an x and a y such that $P(x, y)$ is true	$\forall x \forall y \neg P(x, y)$

Figure 9: Quantifications of Two Variables

1.6 Rules of Inference

Rule of Inference	Tautology	Name
p $p \to q$ $\therefore \; q$	$(p \wedge (p \to q)) \to q$	Modus Ponens
$\neg q$ $p \to q$ $\therefore \; q$	$(\neg q \wedge (p \to q)) \to \neg p$	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

Figure 10: Rules of Inference for Propositional Logic

Note: Resolution is saying, regardless of what p is, q or r is true.

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

Figure 11: Rules of Inference for Quantified Statements

Universal Modus Ponens: The usage of universal instantiation and modus ponens together.

$$\begin{array}{l} \forall x(P(x) \to Q(x)) \\ P(a), \text{ where } a \text{ is a particular element in the domain} \\ \therefore \; Q(a) \end{array}$$

1.7 Introduction to Proofs

Prove $\forall x(P(x) \to Q(x))$ by showing that $P(c) \to Q(c)$ is true, where c is an arbitrary element of the domain, and then apply universal generalization.

1.7.5 Direct Proofs

Show $p \to q$ by first assuming p is true and then showing that q is true using the rules of inference.

Definition 1.16. The integer n is **even** if $\exists k \in \mathbb{Z} \mid n = 2k$.

Definition 1.17. The integer n is **odd** if $\exists k \in \mathbb{Z} \mid n = 2k + 1$.

Definition 1.18. Two integers have the same **parity** if they are both even or both odd. They have **opposite parity** if one is even and the other is odd.

1.7.6 Proof by Contraposition

Definition 1.19. An **indirect proof** is a proof that does not start with the premise and ends with the conclusion. One type is **proof by contraposition**. This is a proof that shows $p \to q$ by showing $\neg q \to \neg p$.

1.7.7 Proof by Contradiction

Another type of indirect proof is **proof by contradiction**. We can prove p is true by showing that $\neg p \to (r \wedge \neg r)$. Assume the negation of p is true, and then show that r and $\neg r$ are both true. This is a contradiction, so p must be true.

Important example of proof by contradiction: Prove that $\sqrt{2}$ is irrational.

Proof. By contradiction. Let p be the proposition that $\sqrt{2}$ is irrational. Assum $\neg p$ is true, that is, assume $\sqrt{2}$ is rational. By definition of rational numbers, there exist integers a and b such that $\sqrt{2} = \frac{a}{b}$, where $\frac{a}{b}$ is in simplest terms. Then, we have:

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned}$$

Since a^2 is a multiple of 2, a^2 is even. Therefore, a is even, and $a = 2k$ for some integer k.

$$\begin{aligned} 2b^2 &= 4k^2 \\ b^2 &= 2k^2 \end{aligned}$$

Since b^2 is a multiple of 2, b^2 is even. Therefore, b is even, and $b = 2l$ for some integer l.

$$\sqrt{2} = \frac{2k}{2l}$$

Since both a and b are even, we can divide both the numerator and denominator by 2. Because our assumption of $\neg p$ leads to the contradiction that 2 divides both a and b and 2 does not divide both a and b, $\neg p$ is false. Therefore, p is true. □

1.8 Proof Methods and Strategy

1.8.2 Exhaustive Proof and Proof by Cases

Exhaustive Proof: Prove that $p \to q$ by showing:

$$\bigvee_{i=1}^{n} p_i \to q$$

Proof by Cases: Prove that $p \to q$ by breaking p into cases and showing that q is true in each case.

2 Basic Structures

2.1 Sets

2.1.1 Introduction

Definition 2.1. A **set** is an unordered collection of distinct objects called **elements** or **members** of the set. A set is said to **contain** its elements. We write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A.

Sets of types of numbers:

- Natural Numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\} = \{\mathbb{Z}^+ \cup 0\}$
- Integers: $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, \dots\}$
- Positive Integers: $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$
- Rational Numbers: $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$
- Real Numbers: $\mathbb{R}$
- Positive Real Numbers: $\mathbb{R}^+$
- Complex Numbers: $\mathbb{C}$

Equality of Sets: $A = B$ if and only if $\forall x(x \in A \leftrightarrow x \in B)$

Empty Set: $\emptyset = \{\}$

2.1.3 Subsets

$$A \subseteq B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B) \leftrightarrow B \supseteq A$$

To show that $A \not\subseteq B$, show $\exists x(x \in A \wedge x \notin B)$.
For every set S, $\emptyset \subseteq S$ and $S \subseteq S$.