

MATH 2305: Discrete Mathematics

Janak Joshi, Dallas College, Fall 2024

1	Logic and Proofs	2
1.1	Propositional Logic	2
1.2	Propositional Equivalences	3
1.3	Predicates and Quantifiers	4
1.4	Nested Quantifiers	6
1.5	Rules of Inference	6
1.6	Introduction to Proofs	8
1.7	Proof Methods and Strategy	8
2	Sets, Functions, Sequences, Sums, and Matrices	10
2.1	Sets	10
2.2	Set Operations	11
2.3	Functions	11
2.4	Sequences and Summations	11
3	Algorithms	12
3.1	Algorithms	12
4	Number Theory and Cryptography	13
4.1	Divisibility and Modular Arithmetic	13
4.2	Integer Representation and Algorithms	13
4.3	Primes and Greatest Common Divisors	13
4.4	Solving Congruences	13
5	Induction and Recursion	14
5.1	Mathematical Induction	14
5.2	Strong Induction and Well-Ordering	14
5.3	Recursive Definitions and Structural Induction	14
5.4	Recursive Algorithms	14
6	Counting	15
6.1	The Basics of Counting	15
6.2	The Pigeonhole Principle	15
6.3	Permutations and Combinations	15
6.4	Binomial Coefficients and Identities	15
6.5	Generalized Permutations and Combinations	15
7	Discrete Probability	16
7.1	An Introduction to Discrete Probability	16
8	Advanced Counting Techniques	17
8.1	Applications of Recurrence Relations	17
8.2	Inclusion-Exclusion	17
9	Relations	18
9.1	Relations and Their Properties	18
10	Graphs	19
10.1	Graphs and Graph Models	19
10.2	Graph Terminology and Special Types of Graphs	19
11	Trees	20
11.1	Introduction to Trees	20

1 Logic and Proofs

1.1 Propositional Logic

A proposition is a declarative statement that is either true or false, but not both. We use letters to denote propositional variables. The conventional letters for propositional variables are p, q, r, s . True is notated as T and false is notated as F. An atomic proposition is a proposition that cannot be expressed in terms of simpler propositions.

Definition

Let p be a proposition. The negation of p , denoted by $\neg p$ (or \bar{p}) means "It is not the case that p ".

The proposition $\neg p$ is read as "not p ". The truth value of the negation of p , $\neg p$ is the opposite of the truth value of p .

The negation of a proposition can also be considered the result of the operation of the negation operator on a proposition.

The next operator is a connective and it is used to form new propositions from two or more existing propositions.

Definition

Let p and q be propositions. The conjunction of p and q , denoted by $p \wedge q$, is the proposition of " p and q ". The conjunction $p \wedge q$ is true when both are true, and false when both are false.

Definition

Let p and q be propositions. The disjunction of p and q , denoted by $p \vee q$, is the proposition " p or q ". The disjunction $p \vee q$ is false when both p and q are false, otherwise it is true.

Definition

Let p and q be propositions. The exclusive or of p and q , denoted by $p \oplus q$ is the proposition that is true when exactly one of p and q is true and is false otherwise.

There are other ways propositions can be combined.

Definition

Let p and q be propositions. The conditional statement $p \rightarrow q$, is the proposition, "if p , then q ". The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. p is called the hypothesis and q is called the conclusion.

A conditional statement is also called an implication.

With $p \rightarrow q$, we can form three related conditional statements.

The first is the proposition $q \rightarrow p$, which is the converse of $p \rightarrow q$.

The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$.

The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.

The contrapositive of a conditional statement is equal to it. We all two compound propositions equivalent when they always have the same truth values. The converse and inverse of a conditional statement are equivalent as well.

There is another way to combine propositions that expresses that two propositions have the same truth value.

Definition

Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition " p if and only q ". This statement is true if p and q have the same truth values, and is false otherwise.

The negation operator is applied before all logical operators. Another general rule is that the conjunction operator takes precedence over the disjunction operator. It is an accepted rule that conditional and biconditional operators have lower precedence than the conjunction and disjunction operators.

A bit is a symbol with two values, 0 and 1. 1 is true, and 0 is false.

1.2 Propositional Equivalences

Definition

A compound proposition that is always true, no matter what the truth values of the propositional values that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. If it is neither a tautology or a contradiction, it is called a contingency.

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

Definition

The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent.

We can establish logical equivalence of more than two compound propositions. Generally 2^n rows are required if a compound proposition involves n propositional variables.

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.

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

Credit: Rosen's Discrete Mathematics 8e

When using De Morgan's Laws, remember to change the logical connective after you negate.

De Morgan's Laws tell us how to negate conjunctions and how to negate disjunctions. The equivalence $\neg(p \vee q) \equiv \neg p \wedge \neg q$ tells us that the negation of a disjunction is formed from the conjunction of the negations of the component propositions. The negation of a conjunction also gives you the disjunction of the negations of component propositions.

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

1.3 Predicates and Quantifiers

We will introduce predicate logic now. For example in the statement x is greater than 3, the variable is x and the predicate is "is greater than 3".

In general a statement involving n variables x_1, x_2, \dots, x_n can be denoted as $P(x_1, x_2, \dots, x_n)$.

Definition

The universal quantification of $P(x)$ is the statement:

" $P(x)$ for all values of x in the domain."

The notation $\forall x P(x)$ denotes the universal quantification of $P(x)$. Here \forall is called the universal quantifier. An element for which $P(x)$ is false is called a counterexample to $\forall x P(x)$.

Definition

The existential quantification of $P(x)$ is the proposition:

"There exists an element in x in the domain such that $P(x)$ "

We use the notation $\exists x P(x)$ for the existential quantification of $P(x)$.

Remember the truth value for both $\forall x P(x)$ and $\exists x P(x)$ depends on the domain.

TABLE 2 De Morgan's Laws for Quantifiers.			
Negation	Equivalent Statement	When Is Negation True?	When False?
$\neg \exists x P(x)$	$\forall x \neg P(x)$	For every x , $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x .

Credit: Rosen's Discrete Mathematics 8e

1.4 Nested Quantifiers

A nested quantifier is when one quantifier is in the scope of another.

Here is table that summarizes different quantifications involving two variables.

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 .

1.5 Rules of Inference

Rules of inference are our basic tools for establishing the truth of statements.

An argument in propositional logic is a sequence of propositions. All but the final proposition in the argument are called premises and the final proposition is called the conclusion. An argument is valid if the truth of all its premises implies the conclusion is true.

An argument form in propositional logic is a sequence of compound propositions involving propositional variables. An argument form is valid if no matter what particular propositions are substituted for the propositional variables in the premises, the conclusion is true if the premises are all true.

The tautology $(p \wedge (p \rightarrow q)) \rightarrow q$ is the basis of the rule of inference modus ponens, or the law of detachment, basically: if p and $p \rightarrow q$ $\therefore q$

Yet again another chart I took from Rosen.

TABLE 1 Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\frac{p \quad p \rightarrow q}{\therefore q}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\frac{p \vee q \quad \neg p}{\therefore q}$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \quad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \vee q \quad \neg p \vee r}{\therefore q \vee r}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

Fallacies resemble rules of inference, the difference lies in that they are based in contingencies rather than tautologies.

There are also some rules of inference for statements involving quantifiers. This is what Rosen summarized:

TABLE 2 Rules of Inference for Quantified Statements.

<i>Rule of Inference</i>	<i>Name</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalization
$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalization

Because universal instantiation and modus ponens are so often used together, the combination of rules is called universal modus ponens. This rule tells us if $\forall x(P(x) \rightarrow Q(x))$ is true, and if $P(a)$ is true for a particular element a in the domain of the universal quantifier, then $Q(a)$ must also be true. Note that by universal instantiation $P(a) \rightarrow Q(a)$ is true. By modus ponens, $Q(a)$ must also be true.

This is how it is described:

$$\frac{\forall x (P(x) \rightarrow Q(x))}{P(a), \text{ where } a \text{ is a particular element in the domain}} \\ \therefore Q(a)$$

There is also universal modus tollens:

$$\frac{\forall x (P(x) \rightarrow Q(x))}{\neg Q(a) \text{ where } a \text{ is a particular element in the domain}} \\ \therefore \neg P(a)$$

1.6 Introduction to Proofs

A proof is a valid argument that establishes the truth of a mathematical statement.

A theorem is a statement that can be shown to be true. We show the truth using a proof.

A less important theorem that is helpful in the proof of other results is called a lemma.

A corollary is a theorem that can be established directly from a theorem that has been proved.

A conjecture is a statement that is being proposed to be a true statement.

A direct proof of a conditional statement $p \rightarrow q$ is constructed with the assumption that p is true with the goal for the combination of p being true and q being false to never happen.

Definition

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$. Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.

An indirect proof is a type of proof that is not direct. One example is proof by contraposition. Proofs by contraposition use the fact that $p \rightarrow q$ is equal to $\neg q \rightarrow \neg p$. We have to show $\neg q \rightarrow \neg p$ is true to show that $p \rightarrow q$ is true as well.

We can prove that $p \rightarrow q$ is true if p is false as well. This is called a vacuous proof.

If we show that q is true in $p \rightarrow q$ this is called a trivial proof.

Definition

The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is irrational.

Suppose we want to prove a statement p is true. Suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude $\neg p$ is false, meaning p is true.

To find a contradiction q that might help us find that p is true, we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r . This is called a proof by contradiction.

To prove a theorem in the form $p \leftrightarrow q$, we show that both $p \rightarrow q$ and $q \rightarrow p$ are both true.

Many incorrect arguments are based on a fallacy called begging the question or circular reasoning. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved.

1.7 Proof Methods and Strategy

Suppose we have a conditional $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$. We can separate the proof into different cases, called proof by cases by proving each of the n conditional statements.

Some theorems can be proved by examining a relatively small number of examples. This is called proof by exhaustion.

The phrase "without loss of generality" (WLOG) means that we assert by proving one case of a theorem, no additional argument is required to prove other specified cases.

Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition in the form $\exists xP(x)$, where P is a predicate. A proof of a proposition in this form is called an existence proof. Sometimes an existence proof can be given by finding an element a , called a witness, such that $P(a)$ is true. This existence proof is called constructive. If we prove $\exists xP(x)$ is true in another way it can be nonconstructive.

For a uniqueness proof, we need two parts:

- Existence: We show that an element x with the desired property exists.
- Uniqueness: We show that if x and y both have the desired property, $x = y$

Forward reasoning is a proof when you start with your premises. You construct a proof with steps leading to the conclusion. It may sometimes be helpful to use backwards reasoning, we find a statement p that we can prove $p \rightarrow q$.

2 Sets, Functions, Sequences, Sums, and Matrices

2.1 Sets

Sets are used to group objects together.

A set is an unordered collection of objects, called elements or members of the set. A set contains its elements. We write $a \in A$ to denote a is in an element of set A . The notation $a \notin A$ denotes a is not an element of set A .

Here are some sets to remember:

- \mathbb{N} is the set of all natural numbers
- \mathbb{Z} is the set of all integers
- \mathbb{Z}^+ is the set of all positive integers
- \mathbb{Q} is the set of all rational numbers
- \mathbb{R} is the set of all real numbers
- \mathbb{R}^+ is the set all positive real numbers
- \mathbb{C} is the set of all complex numbers

Two sets are equal only if they contain the same elements.

An empty set is notated as \emptyset .

A set with one element is a singleton set.

Set A is a subset of set B and set B is the superset of set A if every element of A is also an element of B . To indicate A is a subset of B we write $A \subseteq B$. For the equivalent superset, we write $B \supseteq A$.

For every nonempty set S , there is a guarantee to have at least two subsets, the empty set and the set S itself.

When we want to say that A is a subset of B , but $A \neq B$, we can write $A \subset B$.

If there are n distinct elements in a set S , then the set is finite and n is the cardinality of S . The cardinality of S is denoted as $|S|$.

Otherwise, the set is infinite if it is not finite.

Definition

Given a set S , the power set of S is the set of all subsets of the set S . The power set of S is defined as $\mathcal{P}(S)$.

The power set of a set has 2^n elements. Because sets are unordered, we need to represent ordered collections using ordered n -tuples.

Definition

The ordered n -tuple (a_1, a_2, \dots, a_n) is the ordered collection that has a_1 as its first element,

2.2 Set Operations

If we let A and B be sets, the union of the sets, $A \cup B$, is the set that contains those elements that are either in A or B , or in both.

The intersection of the sets, $A \cap B$, is the set containing those elements in both A and B .

Two sets are called disjoint if the intersection of the sets is an empty set.

The difference of sets A and B , or $A - B$ is the set containing those elements that are in A but not in B . It is also called the complement of B with respect to A .

Definition

Let U be the universal set. The complement of set A denoted as \bar{A} is the complement of A with respect to U . Therefore the complement of the set A is $U - A$.

Much like the last chapter, there are some set identities and properties

TABLE 1 Set Identities.	
Identity	Name
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\bar{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cap C) = (A \cup B) \cap C$ $A \cap (B \cup C) = (A \cap B) \cup C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \bar{A} \cup \bar{B}$ $\overline{A \cup B} = \bar{A} \cap \bar{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \bar{A} = U$ $A \cap \bar{A} = \emptyset$	Complement laws

Credits to Rosen again.

The union of a collection of sets is the set that contains those elements that are members of at least one set in the collection.

The intersection of a collection of sets is the set that contains those elements that are members of all sets in the collection.

2.3 Functions

2.4 Sequences and Summations

3 Algorithms

3.1 Algorithms

4 Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

4.2 Integer Representation and Algorithms

4.3 Primes and Greatest Common Divisors

4.4 Solving Congruences

5 Induction and Recursion

5.1 Mathematical Induction

5.2 Strong Induction and Well-Ordering

5.3 Recursive Definitions and Structural Induction

5.4 Recursive Algorithms

6 Counting

6.1 The Basics of Counting

6.2 The Pigeonhole Principle

6.3 Permutations and Combinations

6.4 Binomial Coefficients and Identities

6.5 Generalized Permutations and Combinations

7 Discrete Probability

7.1 An Introduction to Discrete Probability

8 Advanced Counting Techniques

8.1 Applications of Recurrence Relations

8.2 Inclusion-Exclusion

9 Relations

9.1 Relations and Their Properties

10 Graphs

10.1 Graphs and Graph Models

10.2 Graph Terminology and Special Types of Graphs

11 Trees

11.1 Introduction to Trees