Logic and Proofs

1.1 Propositional Logic

Propositions

Definition

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

Examples:

- "Cal Poly is a university."
- $4+5 = 17$

What about the following?:

- "How are you today?"
- $x + 5 = 17$

Propositions

Definition

We use letters to denote **propositional variables**, variables that represent propositions.
The **truth value** of a proposition is true (T) if it is a true proposition and false (F) if it is a false proposition.

The area of logic that deals with propositions was first developed systematically by Aristotle 2300 years ago.

Propositions

We will now create new propositions from those we already have.

Definition

Let p be a proposition. The negation of p ($\neg p$ or $\bar{p}$) is the statement

"It is not the case that p"

$\neg p$ is read "not p". The truth value for $\neg p$ is always the opposite of the truth value for p.

Truth Table:

p	$\neg p$
T	**F**
F	**T**

Examples.

Propositions

Definition

Let p and q be propositions. The **conjunction** of p and q ($p \wedge q$) is the proposition

"p and q".

$p \wedge q$ is true when both p and q are true and false otherwise.

Truth Table:

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

Examples.

Propositions

Definition

Let p and q be propositions. The **disjunction** of p and q ($p \vee q$) is the proposition

"p or q".

$p \vee q$ is false when both p and q are false and true otherwise.

Truth Table:

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

Examples.

Propositions

Definition

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

Truth Table:

p	q	$p \oplus q$
T	T	**F**
T	F	**T**
F	T	**T**
F	F	**F**

Examples.

Conditional Statements

Definition

Let p and q be propositions. The **conditional statement** $p \to q$ is the proposition

"if p, then q".

$p \to q$ is false when p is true and q is false, and true otherwise.
In the conditional statement $p \to q$, p is called the **hypothesis** and q is called the **conclusion**.

Truth Table:

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

Conditional Statements

Example:

- Let p be: "I do all of my CPE348 homework."
- Let q be: "I will do well on the exam."

Express the statement $p \rightarrow q$ in English.
How about $q \rightarrow p$?

Conditional Statements

Definition

- The proposition $q \to p$ is the **converse** of $p \to q$.
- The proposition $\neg q \to \neg p$ is the **contrapositive** of $p \to q$.
- The proposition $\neg p \to \neg q$ is the **inverse** of $p \to q$.

Example:
Give the converse, contrapositive, and inverse of the conditional statement:

If they are selling cupcakes, then we will stop.

Conditional Statements

Definition

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

Truth Table:

p	q	$p \leftrightarrow q$
T	T	**T**
T	F	**F**
F	T	**F**
F	F	**T**

Examples.

Truth Tables for Compound Propositions

Construct the truth table for the following compound proposition:

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

p	q	$(p \wedge \neg q)$	$(p \vee q)$	$(p \wedge \neg q) \rightarrow (p \vee q)$
T	T	F	T	**T**
T	F	T	T	**T**
F	T	F	T	**T**
F	F	F	F	**T**

Precedence of Logical Operators

Just as there is an order of precedence among arithmetic operators (PEMDAS), there is precedence among logical operators:

1. $\neg$
2. $\wedge$
3. $\vee$
4. $\rightarrow$
5. $\leftrightarrow$

However, we often use parentheses to clarify intent.

Truth Tables for Compound Propositions

Construct the truth table for the following compound proposition:

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

p	q	r	$(p \wedge \neg r)$	$(p \vee q)$	$(r \wedge q)$	$(p \wedge \neg r) \vee (p \vee q) \wedge (r \wedge q)$
T	T	T	F	T	T	**T**
T	T	F	T	T	F	**T**
T	F	T	F	T	F	**F**
T	F	F	T	T	F	**T**
F	T	T	F	T	T	**T**
F	T	F	F	T	F	**F**
F	F	T	F	F	F	**F**
F	F	F	F	F	F	**F**

Logic and Bit Operations

Definition

A **bit** is a symbol with two possible values: 0 and 1.

We often associate bits with truth values:

- 1 represents true.
- 0 represents false.

Truth Table:

x	y	$(x \vee y)$	$(x \wedge y)$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

Logic and Bit Operations

Definition

A **bit string** is a sequence of zero or more bits. The **length** of this string is the number of bits in the string.

Definition

The **bitwise OR, bitwise AND**, and **bitwise XOR** of two strings of the same length are the strings that have as their bits the OR, AND, and XOR of the corresponding bits of the two strings, respectively.

Example: Find the bitwise OR and the bitwise AND of the following two bit strings:

$$0011010 \text{ and } 1010001$$

1.3 Propositional Equivalences

Tautologies and Contradictions

Definition

A compound proposition that is always true, no matter what values of the propositional variables that occur in it, is called a **tautology**.
A compound proposition that is always false, no matter what values of the propositional variables that occur in it, is called a **contradiction**.
A compound proposition that is neither a tautology nor a contradiction is called a **contingency**.

Example:

- Construct examples of tautologies and contradictions using only one variable.
- Construct examples of tautologies and contradictions using two variables.

Logical Equivalences

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.

One way to determine if two compound propositions are logically equivalent is to use a truth table. In particular, the compound propositions p and q are equivalent if and only if the columns giving their truth values agree.

Logical Equivalences

Examples:
Show that the following two sets of compound propositions (known as **De Morgan laws**) are logically equivalent.

- $\neg(p \wedge q)$ and $\neg p \vee \neg q$
- $\neg(p \vee q)$ and $\neg p \wedge \neg q$

Show that the following two compound propositions (known as the distributive law of disjunction) are logically equivalent.

- $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$

Show that the following two compound propositions are logically equivalent.

- $(p \rightarrow q) \vee (p \rightarrow r)$ and $p \rightarrow (q \vee r)$

Propositional Satisfiability

Definition

A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that makes it true.
If there is no such assignment the compound proposition is **unsatisfiable**.

Example:
Determine whether the each of the compound propositions are satisfiable.

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

1.4 Predicates and Quantifiers

Predicates

Consider the following statements:

- "$x > 17$"
- "$x + y = z$"
- "Student x aced the exam."

These statements are neither true nor false unless the values of the variables are specified.

Predicates

In the statement "$x > 17$":

- We call the variable x the subject of the statement.
- We call "is greater than 17" the **predicate**.
- We can represent the statement "$x > 17$" by $P(x)$ where P denotes the predicate "is greater than 17" and x is the variable.
- The statement $P(x)$ is said to be the **propositional function** P at x.
- Once a value has been assigned to x, $P(x)$ becomes a proposition and has a truth value.

Predicates

Examples:

Let $P(x)$ denote the statement "$x + 5 < 10$.

- What is the truth value for $P(2)$?
- What is the truth value for $P(9)$?

Let $F(x, y, z)$ denote the statement "$x^2 + 2y = z$".

- What is the truth value for $F(2, 1, 3)$?
- What is the truth value for $F(1, 1, 3)$?

Let $A(x, y)$ denote the statement "x and y are months of the year.".

- What is the truth value for $A(\text{May, bubblegum})$?
- What is the truth value for $A(\text{June, July})$?

Quantifiers

Definition

The **universal quantification** of $P(x)$ is the statement:
"$P(x)$ for all values of x in the domain."
$\forall x P(x)$ denotes the universal quantification of $P(x)$.
An element for which $P(x)$ is false is called a **counterexample** of $\forall x P(x)$.

Example:
Let $P(x)$ be the statement "$x + 1 > x$".

- What is the truth value for $\forall x P(x)$ when the domain consists of all real numbers?

Quantifiers

Examples:

Let $P(x)$ be the statement "$x + 4 > 10$".

- What is the truth value for $\forall x P(x)$ when the domain consists of all real numbers?
- What is the truth value for $\forall x P(x)$ when the domain consists of $\{8, 9, 10, 11\}$?
- What is the truth value for $\forall x P(x)$ when the domain consists of $\{5, 6, 7, 8, 9, 10, 11\}$?

Let $Q(x)$ be the statement "Student x can legally drive."

- What is the truth value for $\forall x Q(x)$ when the domain consists of all students in San Luis Obispo?
- What is the truth value for $\forall x Q(x)$ when the domain consists of all students in San Luis Obispo with a valid drivers license?

Quantifiers

Definition

The **existential quantification** of $P(x)$ is the statement:
"There exists an element x in the domain such that $P(x)$."
$\exists x P(x)$ denotes the existential quantification of $P(x)$.

Example:
Let $P(x)$ be the statement "$x = 7$".

- What is the truth value for $\exists x P(x)$ when the domain consists of all real numbers?

Quantifiers

Examples:
Let $P(x)$ be the statement "$x + 4 > 10$".

- What is the truth value for $\exists x P(x)$ when the domain consists of all real numbers?
- What is the truth value for $\exists x P(x)$ when the domain consists of $\{4, 5, 6\}$?

Let $Q(x)$ be the statement "Student x can legally drive."

- What is the truth value for $\exists x Q(x)$ when the domain consists of all students in San Luis Obispo?
- What is the truth value for $\exists x Q(x)$ when the domain consists of all 4th grade students in San Luis Obispo?

Quantifiers

Definition

The **uniqueness quantifier** $\exists! x P(x)$ states "there exists a unique x such that $P(x)$ is true.".

Example:
Let $P(x)$ be the statement "$x^2 = 4$".

- What is the truth value for $\exists! x P(x)$ when the domain is all positive real numbers?
- What is the truth value for $\exists! x P(x)$ when the domain is all real numbers?

Precedence of Quantifiers

The quantifiers $\forall$ and $\exists$ have a higher precedence than all other logical operators.

Example:

$\forall x P(x) \vee Q(x)$ means:

- $(\forall x P(x)) \vee Q(x)$
- NOT $\forall x(P(x) \vee Q(x))$

Logical Equivalences Involving Quantifiers

De Morgan's Laws for Quantifiers:

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

Example:

- Show that $\neg\forall x(P(x) \wedge Q(x))$ is logically equivalent to $\exists(\neg P(x) \vee \neg Q(x))$.

1.5 Nested Quantifiers

Nested Quantifiers

Consider the following logical expression:

- $\forall x \exists y (x + y = 0)$

This is equivalent to the expression:

- $\forall x (\exists y (x + y = 0))$

We could use nested quantifiers to describe the commutative law of addition for real numbers:

- $\forall x \forall y (x + y = y + x)$

We could also use nested quantifiers to describe the associative law of addition for real numbers:

- $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$

Introduction to Proofs

Definition

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

Definition

A **theorem** is a statement that can be shown to be true. We demonstrate that a theorem is true using a proof.

Definition

- A less important theorem 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.

Proofs

To prove a theorem of the form:

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

We show that for some arbitrary element c in the domain:

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

Then apply *universal generalization*.

Direct Proofs

Direct Proof: $p \to q$

> Assume p
> $\ldots$
> Therefore, q.
> Thus $p \Rightarrow q$.

Here the $\ldots$ represent axioms, definitions, previously proved theorems, and rules of inference.

Direct Proofs

Prove the following theorems using direct proofs.

Theorem

If n is an even integer, then $(-1)^n = 1$.

Theorem

The sum of an even integer and odd integer is odd.

Hint: First try to restate as an "If-then" proposition.
Recall the definition of division: $x|y$ means there exists an integer c such that $y = x \cdot c$

Theorem

For all integers a, b, and c, if $a|b$ and $b|c$, then $a|(b+c)$.

Proofs by Contrapositive

Contraposition: $p \rightarrow q$

Assume $\neg q$ $\ldots$ Therefore, $\neg p$. Therefore, $\neg q \rightarrow \neg p$ Thus $p \rightarrow q$.

Again, the $\ldots$ represent axioms, definitions, previously proved theorems, and rules of inference.

Proofs by Contrapositive

Prove the following theorems using proofs by contrapositive.

Theorem

If a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Theorem

If a does not divide bc, then a does not divide b.

Theorem

If $x^2 - 6x + 5$ is even, then x is odd.

Proofs by Contradiction

Contradiction: p

Assume $\neg p$.
$\ldots$
Therefore, something untrue.
Therefore, $\rightarrow\leftarrow$.
Thus p.

Proofs by Contradiction

Prove the following theorems using proofs by contradiction.

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 called **irrational**.

Theorem

Prove that $\sqrt{2}$ is irrational.

Theorem

At least 5 of any 29 days must fall on the same day of the week.

Theorem

There is no greatest even integer.

Proofs of Equivalence

To prove the biconditional statement: $p \leftrightarrow q$ we show:

- $p \rightarrow q$ AND
- $q \rightarrow p$

Example:
Prove the following theorem:

Theorem

An integer n is even if and only if its square (n^2) is even.

1.8 Proof Methods and Strategy

Exhaustive Proof

The **exhaustive proof** technique works well when the number of possible cases is relatively small.
Example:
Prove the following theorem:

Theorem

$n^2 \leq 2^n$ when n is a positive integer, $n < 3$.

Proof by Cases

A **proof by cases** must cover all possible cases that arise in the theorem.
Example:
Prove the following theorems:

Theorem

$|xy| = |x||y|$ *for all real numbers* x *and* y.

Sometimes we can eliminate all but a few cases.

Theorem

There are no integers x *and* y *such that* $x^2 + 3y^2 = 8$

Without Loss of Generality

The term **without loss of generality** is used before an assumption in a proof which narrows the premise to some special case; it implies that the proof for that case can be easily applied to all others, or that all other cases are equivalent or similar.
Example:

Theorem

If there are three mustangs, each painted either green or gold, then there must be at least two mustangs of the same color.

Proof.

Without loss of generality, suppose that the first mustang is green. . . □

Existence Proofs

Examples:
Prove the following theorems:

Theorem

There exist integers x and y such that $3x^2 - 17y = 10$.

Theorem

There exists an integer a such that $\frac{4 \cdot a + 10}{9 \cdot a - 30} = 2$.

Uniqueness Proofs

Example:
Prove the following theorems:

Theorem

There exists a unique integer a such that $3 \cdot a + 6 = 0$.

Theorem

There exists a unique positive real number whose square is 4.