Discrete Mathematics

The Foundations: Logic & Proofs

Prof. Steven Evans

1.1: Propositional Logic

Propositions

Definition

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

Propositions

Negation

Let p be a proposition. The *negation of* p, denoted by $\neg p$ or by $\bar{p}$ is the statement:

"It is not the case that p."

The proposition $\neg p$ is pronounced "not p."

p	$\neg p$
T	F
F	T

Propositions

Conjunction, disjunction, and exclusive or

Let p and q be propositions.

- The *conjunction* of p and q, denoted $p \wedge q$, is true when p and q are both true and false otherwise.

Propositions

Conjunction, disjunction, and exclusive or

Let p and q be propositions.

- The *conjunction* of p and q, denoted $p \wedge q$, is true when p and q are both true and false otherwise.
- The *disjunction* of p and q, denoted $p \vee q$, is false when p and q are false and true otherwise.

Propositions

Conjunction, disjunction, and exclusive or

Let p and q be propositions.

- The *conjunction* of p and q, denoted $p \wedge q$, is true when p and q are both true and false otherwise.
- The *disjunction* of p and q, denoted $p \vee q$, is false when p and q are false and true otherwise.
- The *exclusive or* of p and q, denoted $p \oplus q$, is the proposition that is true exactly when one of p and q is true.

Propositions

Conjunction, disjunction, and exclusive or

Let p and q be propositions.

- The *conjunction* of p and q, denoted $p \wedge q$, is true when p and q are both true and false otherwise.
- The *disjunction* of p and q, denoted $p \vee q$, is false when p and q are false and true otherwise.
- The *exclusive or* of p and q, denoted $p \oplus q$, is the proposition that is true exactly when one of p and q is true.

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

Conditional statements

Definition

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

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

Conditional statements

Some other ways to express conditionals:

- if p, then q
- if p, q
- p is sufficient for q
- q if p
- q when p
- a necessary condition for p is q
- a sufficient condition for q is p
- q unless $\neg p$
- p implies q
- p only if q
- q whenever p
- q is necessary for p
- q follows from p

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.
- The contrapositive refers to $\neg q \to \neg p$.

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.
- The contrapositive refers to $\neg q \to \neg p$.
- The inverse refers to $\neg p \to \neg q$.

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.
- The contrapositive refers to $\neg q \to \neg p$.
- The inverse refers to $\neg p \to \neg q$.

Equivalence

Two propositions are called equivalent when they have the same truth table.

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.
- The contrapositive refers to $\neg q \to \neg p$.
- The inverse refers to $\neg p \to \neg q$.

Equivalence

Two propositions are called equivalent when they have the same truth table.

- The contrapositive is equivalent to the original implication.

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.
- The contrapositive refers to $\neg q \to \neg p$.
- The inverse refers to $\neg p \to \neg q$.

Equivalence

Two propositions are called equivalent when they have the same truth table.

- The contrapositive is equivalent to the original implication.
- The converse and inverse are equivalent to each other.

Conditional statements

Converse, contrapositive, and inverse

Consider the implication $p \to q$.

- The converse refers to $q \to p$.
- The contrapositive refers to $\neg q \to \neg p$.
- The inverse refers to $\neg p \to \neg q$.

Equivalence

Two propositions are called equivalent when they have the same truth table.

- The contrapositive is equivalent to the original implication.
- The converse and inverse are equivalent to each other.
- The inverse is *not* equivalent to the original.

Conditional statements

Biconditionals

Let p and q be propositions. The *biconditional statement* $p \leftrightarrow q$ is the proposition "p if and only if q." These are also called "bi-implications."

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

Truth tables of compound propositions

Example

Construct the truth table of the compound proposition

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

Grammar rules

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

$$x \wedge \neg y \vee z \rightarrow w$$

Grammar rules

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

$$x \wedge \neg y \vee z \rightarrow w \equiv ((x \wedge (\neg y)) \vee z) \rightarrow w.$$

Logic and bit operations

Truth Value	Bit
T	1
F	0

Logic and bit operations

Truth Value	Bit
T	1
F	0

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

1.2: Applications of Propositional Logic

Examples

Smullyan posed many puzzles about an island that has two kinds of inhabitants: knights, who always tell the truth, and their opposites, knaves, who always lie. You encounter two people A and B. What are A and B if A says, "B is a knight," and B says, "The two of us are opposite types."?

Examples

A father tells his two children, a boy and a girl, to play in their backyard without getting dirty. However, while playing, both children get mud on their foreheads. When the children stop playing, the father says, "At least one of you has a muddy forehead," and then asks the children to answer "Yes" or "No" to the following question: "Do you know whether you have a muddy forehead?" The father asks this question twice. What will the children answer each time this question is asked?

(The children are honest, can see each others' foreheads, cannot see their own foreheads, and answer simultaneously.)

1.3: Propositional Equivalences

More kinds of propositions

- A proposition that is always true, no matter the truth values of the variables that occur in it, is called a *tautology*.
- A proposition that is always false is called a *contradiction*.
- A proposition that is neither of these is called a *contingency*.

More kinds of propositions

- A proposition that is always true, no matter the truth values of the variables that occur in it, is called a *tautology*.
- A proposition that is always false is called a *contradiction*.
- A proposition that is neither of these is called a *contingency*.

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

Logical equivalences

Definition

Propositions p and q are called *logically equivalent*, denoted $p \equiv q$, when $p \leftrightarrow q$ is a tautology.

Examples

DeMorgan's laws:

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$. (Check this one yourself!)
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Conditional expansion:

- $(p \rightarrow q) \equiv (\neg p \vee q)$. (Check this one too!)

Example: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

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

Example: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

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

Example: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

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

Example: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

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

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Idempotent laws:

- $p \vee p \equiv p$.
- $p \wedge p \equiv p$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Idempotent laws:

- $p \vee p \equiv p$.
- $p \wedge p \equiv p$.

Double negation law:

- $\neg(\neg p) \equiv p$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Idempotent laws:

- $p \vee p \equiv p$.
- $p \wedge p \equiv p$.

Double negation law:

- $\neg(\neg p) \equiv p$.

Commutative laws:

- $p \vee q \equiv q \vee p$.
- $p \wedge q \equiv q \wedge p$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Idempotent laws:

- $p \vee p \equiv p$.
- $p \wedge p \equiv p$.

Double negation law:

- $\neg(\neg p) \equiv p$.

Commutative laws:

- $p \vee q \equiv q \vee p$.
- $p \wedge q \equiv q \wedge p$.

Associative laws:

- $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Idempotent laws:

- $p \vee p \equiv p$.
- $p \wedge p \equiv p$.

Double negation law:

- $\neg(\neg p) \equiv p$.

Commutative laws:

- $p \vee q \equiv q \vee p$.
- $p \wedge q \equiv q \wedge p$.

Associative laws:

- $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

Distributive laws:

- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

Equivalence rules

Identity laws:

- $p \wedge T \equiv p$.
- $p \vee F \equiv p$.

Domination laws:

- $p \wedge F \equiv F$.
- $p \vee T \equiv T$.

Idempotent laws:

- $p \vee p \equiv p$.
- $p \wedge p \equiv p$.

Double negation law:

- $\neg(\neg p) \equiv p$.

Commutative laws:

- $p \vee q \equiv q \vee p$.
- $p \wedge q \equiv q \wedge p$.

Associative laws:

- $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

Distributive laws:

- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

DeMorgan's laws:

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$.
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Equivalence rules

Absorption laws:

- $p \lor (p \land q) \equiv p$.
- $p \land (p \lor q) \equiv p$.

Equivalence rules

Absorption laws:

- $p \vee (p \wedge q) \equiv p$.
- $p \wedge (p \vee q) \equiv p$.

Negation laws:

- $p \vee \neg p \equiv T$.
- $p \wedge \neg p \equiv F$.

Equivalence rules

Absorption laws:

- $p \vee (p \wedge q) \equiv p$.
- $p \wedge (p \vee q) \equiv p$.

Negation laws:

- $p \vee \neg p \equiv T$.
- $p \wedge \neg p \equiv F$.

Implication laws:

- $p \to q \equiv \neg p \vee q$.
- $p \to q \equiv \neg q \to \neg p$.
- $p \vee q \equiv \neg p \to q$.
- $p \wedge q \equiv \neg(p \to \neg q)$.
- $p \wedge \neg q \equiv \neg(p \to q)$.

Equivalence rules

Absorption laws:

- $p \vee (p \wedge q) \equiv p$.
- $p \wedge (p \vee q) \equiv p$.

Negation laws:

- $p \vee \neg p \equiv T$.
- $p \wedge \neg p \equiv F$.

Implication laws:

- $p \rightarrow q \equiv \neg p \vee q$.
- $p \rightarrow q \equiv \neg q \rightarrow \neg p$.
- $p \vee q \equiv \neg p \rightarrow q$.
- $p \wedge q \equiv \neg(p \rightarrow \neg q)$.
- $p \wedge \neg q \equiv \neg(p \rightarrow q)$.

Distribution and implication:

- $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$.
- $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$.
- $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$.
- $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$.

Equivalence rules

Absorption laws:

- $p \vee (p \wedge q) \equiv p$.
- $p \wedge (p \vee q) \equiv p$.

Negation laws:

- $p \vee \neg p \equiv T$.
- $p \wedge \neg p \equiv F$.

Implication laws:

- $p \rightarrow q \equiv \neg p \vee q$.
- $p \rightarrow q \equiv \neg q \rightarrow \neg p$.
- $p \vee q \equiv \neg p \rightarrow q$.
- $p \wedge q \equiv \neg(p \rightarrow \neg q)$.
- $p \wedge \neg q \equiv \neg(p \rightarrow q)$.

Distribution and implication:

- $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$.
- $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$.
- $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$.
- $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$.

Biequivalence laws:

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

Using DeMorgan's laws

Example

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

1.4: Predicates and Quantifiers

Predicates

The statement "x is greater than 3" has two parts:

1. The variable x is referred to as the *subject*.
2. The clause "is greater than 3" is referred to as the *predicate*.

Symbolically, we express this sentence as $P(x)$, where P is the predicate, operating on the variable x. The statement $P(x)$ is said to be the *value of 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

Example

Let $Q(x, y)$ denote the statement "$x = y + 3$". What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Quantifiers

Universal quantifiers

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 this statement, and the symbol $\forall$ is called the *universal quantifier*.

Quantifiers

Universal quantifiers

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 this statement, and the symbol $\forall$ is called the *universal quantifier*.

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

Quantifiers

Universal quantifiers

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 this statement, and the symbol $\forall$ is called the *universal quantifier*.

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

Example

What is the truth value of $\forall x(x^2 \geq x)$ if the domain consists of all real numbers? What is the truth value if the domain consists only of all integers?

Quantifiers

Existential quantifiers

The *existential quantification* of $P(x)$ is the statement "There exists an element x in the domain such that $P(x)$." We use the notation $\exists x P(x)$ for the existential quantification of $P(x)$, and $\exists$ is called the *existential quantifier*.

Quantifiers

Existential quantifiers

The *existential quantification* of $P(x)$ is the statement “There exists an element x in the domain such that $P(x)$.” We use the notation $\exists x P(x)$ for the existential quantification of $P(x)$, and $\exists$ is called the *existential quantifier*.

Example

What is the truth value of $\exists x P(x)$, where $P(x)$ is the statement $x^2 > 10$ and the universe of discourse consists of the positive integers not exceeding 4?

Quantifiers

Alternative names for quantifiers:

Universal

- for all
- for every
- all of
- for each
- given any
- for arbitrary
- for each
- for any

Existential

- there exists
- for some
- for at least one
- there is

Quantifiers

Uniqueness quantifier

We can build more quantifiers by putting a size limit on the existential quantifier. The most important of these is the *uniqueness quantifier*, denoted by $\exists! x P(x)$ or $\exists_1 x P(x)$, corresponding to the statement "There exists a unique x (i.e., *exactly* one x) such that $P(x)$ is true."

Quantifiers

Example of restricted quantifiers

What do the statements $\forall x < 0(x^2 > 0)$, $\forall y \neq 0(y^3 \neq 0)$, and $\exists z > 0(z^2 = 2)$ mean, where the domain in each case consists of the real numbers?

The grammar of quantifiers

Precedence

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.

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

The grammar of quantifiers

Precedence

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.

$$\forall x P(x) \vee Q(x) \equiv (\forall x P(x)) \vee Q(x).$$

The grammar of quantifiers

Binding variables

When a quantifier is used on the variable x, we say that this occurrence of the variable is *bound*. An occurrence of a variable not bound by a quantifier or set to a value is *free*. The part of an expression to which a quantifier is applied is called its *scope*. So, a variable is free if it outside the scope of all quantifiers in the formula that specify it.

All variables that occur in a proposition function must be bound or set equal to a particular value to turn it into a proposition.

Logical equivalences involving quantifiers

Definition

Statements involving quantifiers are *logically equivalent* when they have the same truth value no matter which predicates are substituted or which domain of discourse is chosen. We denote this by $S \equiv T$.

Logical equivalences involving quantifiers

Definition

Statements involving quantifiers are *logically equivalent* when they have the same truth value no matter which predicates are substituted or which domain of discourse is chosen. We denote this by $S \equiv T$.

Example

Show that $\forall x(P(x) \wedge Q(x))$ and $\forall x P(x) \wedge \forall x Q(x)$ are logically equivalent.

Negating quantified expressions

There are two versions of DeMorgan's laws for quantified expressions:

1. $\neg \exists x P(x) \equiv \forall x \neg P(x)$.
2. $\neg \forall x P(x) \equiv \exists x \neg P(x)$.

Negating quantified expressions

There are two versions of DeMorgan's laws for quantified expressions:

1. $\neg \exists x P(x) \equiv \forall x \neg P(x)$.
2. $\neg \forall x P(x) \equiv \exists x \neg P(x)$.

Example

Show that $\neg \forall x (P(x) \rightarrow Q(x))$ and $\exists x (P(x) \wedge \neg Q(x))$ are logically equivalent.

Quantifiers

Example

Consider these statements, of which are the first three are premises and the fourth is a valid conclusion:

1. All hummingbirds are richly colored.
2. No large birds live on honey.
3. Birds that do not live on honey are dull in color.
4. Hummingbirds are small.

Let $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ be the statements "x is a hummingbird", "x is large", "x lives on honey", and "x is richly colored" respectively. Express the statements in the argument using quantifiers and these propositional functions.