



CS 261

Mathematical Foundations of Computer Science

Chapter 2

Logic

Logic Notation

Universal Quantification: $\forall x P(x)$: For all values of x , predicate $P(x)$ is true.

Existential Quantification: $\exists x P(x)$. There exists at least one x , such that $P(x)$ is true.

Logically Equivalent: i.e. $p \equiv \sim(\sim p)$.

Implication: $p \Rightarrow q$: p implies q (if it is raining, then I get wet).

Converse: The converse of $p \Rightarrow q$ is $q \Rightarrow p$ (if I get wet, then it is raining).

Contrapositive: The contrapositive of $p \Rightarrow q$ is $\sim q \Rightarrow \sim p$ (if I do not get wet, then it is not raining). Note: $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$

Biconditional: $p \Leftrightarrow q$: p if and only if q (also written iff).

Tautology: Statement that is always true: $p \Rightarrow \sim(\sim p)$.

Contradiction: Statement that is always false: $p \Rightarrow \sim p$.

Contingency: Statement that can be either true or false.

Therefore: \therefore

Commutative Properties: $p \vee q \equiv q \vee p$

$$p \wedge q \equiv q \wedge p$$

Associative Properties: $p \vee (q \vee r) \equiv (p \vee q) \vee r$

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$

Distributive Properties: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

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

Idempotent Properties: $p \vee p \equiv p$

$$p \wedge p \equiv p$$

Negation Property: $\sim(\sim p) \equiv p$

De Morgan's Laws: $\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$

$$\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$$

Systematic Construction of a Truth Table

- 1) The first n columns of the table are labeled by the component propositional variables.
- 2) Additional columns are included for all intermediate combinations of the variables, culminating in a column for the full statement.
- 3) Under each of the first n headings, list all 2^n possible n -tuples of truth values for the n component statements.
- 4) Fill in all remaining columns with calculated values.

Example: $(p \wedge q) \vee \sim p$

p	q	(1) $(p \wedge q)$	(2) $\sim p$	(3) $(1) \vee (2)$
F	F	T	T	T
F	T	F	T	T
T	F	F	F	F
T	T	F	F	T

Exercise 2.1 #26

Make a truth table for the statement: $(\sim p \wedge q) \vee \sim r$

p	q	r	(1) $\sim p$	(2) $(1) \wedge q$	(3) $\sim r$	(4) $(2) \vee (3)$
1	1	1	0	0	0	0
1	1	0	0	0	1	1
1	0	1	0	0	0	0
1	0	0	0	0	1	1
0	1	1	1	1	0	1
0	1	0	1	1	1	1
0	0	1	1	0	0	0
0	0	0	1	0	1	1

Properties for Universal and Existential Quantifiers

1. $\sim(\forall x P(x)) \equiv \exists x \sim P(x)$
2. $\sim(\exists x P(x)) \equiv \forall x \sim P(x)$
3. $\exists x (P(x) \Rightarrow Q(x)) \equiv \forall x P(x) \Rightarrow \exists x Q(x)$
4. $\exists x (P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$
5. $\forall x (P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$
6. $((\forall x P(x)) \wedge (\forall x Q(x))) \Rightarrow \forall x (P(x) \vee Q(x))$ is a tautology
7. $\exists x (P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \vee \exists x Q(x)$ is a tautology

Tautologies – Verify with true tables

1. $(p \wedge q) \Rightarrow p$
2. $p \Rightarrow (p \vee q)$
3. $\sim p \Rightarrow (p \Rightarrow q)$
4. $p \wedge (p \Rightarrow q) \Rightarrow q$
5. $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
6. $\sim (p \Rightarrow q) \Rightarrow p$
7. $(\sim p \wedge (p \vee q)) \Rightarrow q$
8. $((p \Rightarrow q) \wedge (\sim q)) \Rightarrow \sim p$ (used in proof by contradiction)

Tautologies - True Tables

$$\sim p \Rightarrow (p \Rightarrow q)$$

p	q	(1) $(p \Rightarrow q)$	(2) $\sim p$	(3) $(2) \Rightarrow (1)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	0	1

Tautologies - True Tables

$$(\sim p \wedge (p \vee q)) \Rightarrow q$$

p	q	(1) $(p \vee q)$	(2) $\sim p$	(3) $(2) \wedge (1)$	(4) $(3) \Rightarrow q$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	0	0	1

Conjunctive Normal Form

In Boolean logic, Conjunctive Normal Form (CNF) is a method of standardizing and normalizing logical formulas.

CNF is useful in both manual and automated theorem proving.

A logical formula is in CNF iff:

- It is a single conjunction of one or more disjunctions of one or more literals.
- The only propositional operators in CNF are AND, OR, and NOT.
- The NOT operator can only be used as part of a literal.

Examples: CNF

$$x \wedge y$$

$$\bar{x} \wedge (y \vee z)$$

$$(x \vee y) \wedge (\bar{y} \vee z \vee \bar{w}) \wedge (w \vee \bar{x})$$

Not CNF

$$\sim (x \wedge y)$$

$$(x \wedge y) \vee z$$

$$x \wedge (y \vee (z \wedge w))$$

Conversion to Conjunctive Normal Form

Note that all logical formulas can be converted into conjunctive normal form, thus when making proofs on formulas or on the structure of formulas it is often convenient to assume that everything is in CNF.

In some cases conversion to CNF can lead to an exponential explosion of the formula. In particular, given that each clause up to k -literals, what is the maximum number of clauses?

Convert the following to Conjunctive Normal Form:

- 1) $\sim (x \wedge y)$
- 2) $(x \wedge y) \vee z$
- 3) $x \wedge (y \vee (z \wedge w))$

3-Satisfiability (3SAT)

The boolean satisfiability problem (SAT) is a decision problem considered in complexity theory. An instance of the problem is defined by a boolean expression in CNF. The question is: given the expression, is there some assignment of TRUE and FALSE values to the variables that will make the entire expression true?

3SAT is a special case of satisfiability when each clause contains at most three literals.

Are each of the following 3SAT formulas satisfiable, and if so, then find a satisfying vector of variables:

- 1) $(x \vee y \vee \bar{z}) \wedge (\bar{x} \vee \bar{y} \vee z) \wedge (\bar{x} \vee y \vee z)$
- 2) $(x \vee y \vee z) \wedge (\bar{x} \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$
- 3) $(x \vee y \vee \bar{z}) \wedge (\bar{x} \vee y \vee z) \wedge (\bar{z} \vee \bar{y} \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z})$
- 4) $(x \vee z \vee \bar{x}) \wedge (x \vee y \vee \bar{z}) \wedge (x \vee \bar{y} \vee \bar{x}) \wedge (y \vee \bar{x} \vee \bar{z})$

Methods of Proof

Virtually all mathematical theorems are composed of implications of the type:

$$(p_1 \wedge p_2 \wedge p_2 \wedge \dots p_n) \Rightarrow q$$

Each p_i is called a **hypotheses** or **premises** and q is called the **conclusion**.

To prove a theorem means to show that the implication is a tautology.

A proof is not an attempt to show that q is true, but only that q will be true if all the p_i 's are true.

An argument is said to be **valid** if it follows universally correct methods of reasoning and the rules of inference.

Is this Valid? (part 1 of 2)

From Plato (ca. 428 - 348 BC) the Republic.
Argument of Socrates to Glaucon



Would not he who is fitted to be a guardian, besides the spirited nature, need to have the qualities of a philosopher?

I do not apprehend your meaning.

The trait of which I am speaking, may be also seen in the dog, and is remarkable in the animal.

What trait?

Why, a dog, whenever he sees a stranger, is angry; when an acquaintance, he welcomes him, although the one has never done him any harm, nor the other any good. Did this never strike you as curious?

The matter never struck me before; but I quite recognize the truth of your remark.

And surely this instinct of the dog is very charming; your dog is a true philosopher.

Why?

Is this Valid? (part 2 of 2)

Why, because he distinguishes the face of a friend and of an enemy only by the criterion of knowing and not knowing. And must not an animal be a lover of learning who determines what he likes and dislikes by the test of knowledge and ignorance?

Most assuredly.

And is not the love of learning the love of wisdom, which is philosophy?

They are the same, he replied.

And may we not say confidently of man also, that he who is likely to be gentle to his friends and acquaintances, must by nature be a lover of wisdom and knowledge?

That we may safely affirm.

Then he who is to be a really good and noble guardian of the State will require to unite in himself philosophy and spirit and swiftness and strength?

Undoubtedly.

Exercises 2.3

State whether the argument given is valid. If it is valid, identify the tautology or tautologies on which it is based.

1. If I drive to work, then I will arrive tired.
I am not tired when I arrive at work.
 \therefore I do not drive to work. $(d \Rightarrow t) \wedge \sim t \Rightarrow \sim d$
2. If I drive to work, then I will arrive tired.
I arrive at work tired.
 \therefore I drive to work. **Not Valid**
3. If I drive to work, then I will arrive tired.
I do not drive to work.
 \therefore I will not arrive tired work. **Not Valid**
5. I will become famous or I will not become a writer.
I will become a writer.
 \therefore I will become a writer. $((f \vee \sim w) \wedge w) \Rightarrow f$

Contrapositive Truth Table

A conditional statement and its contrapositive are logically equivalent.

$$(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$$

p	q	Conditional $p \supset q$
0	0	1
0	1	1
1	0	0
1	1	1

(1) $\sim p$	(2) $\sim q$	Contrapositive (2) \supset (1)
1	1	1
1	0	1
0	1	0
0	0	1

Contrapositive: an Indirect Method of Proof

An important proof technique, which is an example of the Indirect method of proof, follows from the tautology of a conditional and its contrapositive $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$

Example:

Let n be an integer. Prove that if n^2 is odd, then n is odd.

Proof:

1. Let p : $\{n^2 \text{ is odd}\}$, and q : $\{n \text{ is odd}\}$.
2. We have to prove $(p \Rightarrow q)$ is true. Instead, prove the contrapositive.
3. Suppose that n is not odd, thus that n is even.
4. Then $n = 2k$, where k is an integer.
5. This gives: $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
6. Therefore, n^2 is even, and the contrapositive is true.
7. Therefore, the given statement has been proved.

Proof by Contradiction

Proof by contradiction is based on the tautology: $((p \Rightarrow q) \wedge (\neg q)) \Rightarrow \neg p$.

Informally, this states that if a statement p implies a false statement q , then p must be false.

Example: Prove that there is no rational number n/m whose square is 2. In other words, prove that $\sqrt{2}$ is irrational.

Proof:

1. Assume $(n/m)^2 = 2$ for some integers n and m , which have no common factors.
2. If n and m do have a common factor, then replace the fraction with its equivalent lowest-term form.
3. Then, $n^2 = 2m^2$, so n^2 is even.
4. This implies that n is even, since the square of an odd number is odd.
5. Thus, $n=2k$ for some integer k .
6. This gives: $2m^2 = n^2 = (2k)^2 = 4k^2$. Thus $m^2 = 2k^2$.
7. Thus, m is even.
8. Thus, n and m both have a factor of two, which contradicts the assumption.

Exercise 2.3 #23

Prove or disprove that

$$p = n^2 + 41n + 41$$

is prime for every positive integer n .

Exercise 2.3 #23

Prove or disprove that

$$p = n^2 + 41n + 41$$

is prime for every positive integer n .

Counterexample:

let $n = 41$, then

$$\begin{aligned} p &= n^2 + 41n + 41 \\ &= 41^2 + 41^2 + 41 \\ &= 41(41 + 41 + 1) \\ &= 41(83) \end{aligned}$$

Exercise 2.3 #25

Prove or disprove that $3 \mid (n^3 - n)$ for every positive integer n .

Hint: Factor $(n^3 - n)$

Exercise 2.3 #25

Prove or disprove that $3 \mid (n^3 - n)$ for every positive integer n .

Proof:

1. $(n^3 - n) = n(n^2 - 1) = n(n + 1)(n - 1)$
2. Since this is the product of three consecutive integers, one must be a multiple of 3.
3. Thus, $3 \mid (n^3 - n)$

Homework

Exercises 2.1: #9, #12, #13, #15, #23, #33, #35

Exercises 2.2: #1, #7, #21

Exercises 2.3: #7, #9, #15, #24, #26.

Becky to present the solution to #24.

Dianah to present the solution to #26.