1 The Foundation: Logic and Proofs

1.1 Propositional Logic

Propositions *(명제)*

a declarative ***sentence*** *that is either* ***true*** *or* ***false****,*

but ***not both nor neither***

letters denoting propositions *p, q, r, s, …*

T*: true value*

F*: false value*

propositional calculus *or* ***propositional logic***

compounded propositions

propositions *that are* ***formed*** *from* ***existing*** *propositions*

using ***logical operators(connectives)***

***Definition** 1 **negation**(**Not**)*

*Let p be a proposition, ¬p is a (new) **compounded** proposition,*
*called **negation** of p, or "**not** p".*
See truth table for negation of proposition
*¬: negation **operator**(unary, **prefix**)*

***Definition** 2 **conjunction**(**And**)*

Let p and q be a propositions, p ∧ q is a (compounded) proposition,
*called **conjunction** of p and q, or "p and q".*

***Definition** 3 **disjunction**(**Or**; **Inclusive or**)*

Let p and q be a propositions, p ∨ q is a proposition,
*called **disjunction** of p and q, or "p or q".*

*∧, ∨: **conjunctive**, **disjunctive connectives**(binary, **infix**)*

Definition** 4 **Exclusive or

Let p and q be a propositions, $p \oplus q$ is a proposition,
*called **exclusive or** of p and q, or "p xor q".*

Definition** 5 **implication(conditional)

Let p and q be a propositions, $p \rightarrow q$ is a proposition,
*called **implication** of p and q, or "p implies q".*
"if p, then q" "p, only if q" …
*p is called **hypothesis(antecedent**; **premise**) of $p \rightarrow q$*
*q is called **conclusion(consequence**) of $p \rightarrow q$*

*$p \rightarrow q$ is **false** only in the case that p is true an q is false.*
*logic says **nothing** when the **hypothesis** is **false***
$p \rightarrow q$ is true when p is false (inclusive) or q is true
*$\therefore$ $p \rightarrow q$ is **equivalent** to $\neg p \vee q$.*

Let $p \to q$ be a implication proposition. Then

*$q \to p$ is a **converse** (역) of $p \to q$,*
*$\neg q \to \neg p$ is a **contrapositive** (대우) of $p \to q$, and*
*$\neg p \to \neg q$ is a **inverse** (이) of $p \to q$.*

*$p \to q$ and **contrapositive** $\neg q \to \neg p$ are equivalent.*
***converse** $q \to p$ and **inverse** $\neg p \to \neg q$ are equivalent.*

Definition** 6 **biconditional (equivalence)

Let p and q be a propositions, $p \leftrightarrow q$ is a proposition,
*called **biconditional** of p and q, or "p, if and only if, q".*

$p \leftrightarrow q$ is equivalent to $(p \to q) \wedge (q \to p)$.
$p \leftrightarrow q$ is equivalent to $\neg(p \oplus q)$.

Precedence of Logical Operators

$\neg$ *high*

$\wedge$

$\vee$

$\rightarrow$

$\leftrightarrow$ *low*

$p \vee q \wedge \neg r \rightarrow s = (p \vee (q \wedge (\neg r))) \rightarrow s$

Syntax grammar for (composite) propositions

$p = \mathbf{T} \mid \mathbf{F} \mid v \mid \neg p \mid p \wedge p \mid p \vee p \mid p \rightarrow p \mid p \leftrightarrow p \mid (p)$

Truth Table of Compound Statement

n single propositions(variables) 2^n *rows in the truth table*

2 propositions *4 areas in Venn Diagram*

3 propositions *8 areas in Venn Diagram*

Translating English Sentences

System Specifications

Boolean Searches

Logic Puzzle

Logic and Bit Operations

T	*1*
F	*0*
$\neg$	*NOT*
$\wedge$	*AND*
$\vee$	*OR*

1.2 Propositional Equivalences

Def. *1 A (compound) proposition that is always true:* ***tautology***

A proposition that is always false: ***contradiction***

Otherwise: ***contingency***.

Logical Equivalences

Def. *2 Two propositions p and q are* ***logically equivalent****, if* $p \leftrightarrow q$ *is a* ***tautology****, written,* $p \equiv q$.

Remark: $p \equiv q$ *vs* $p \leftrightarrow q$.

$\equiv$ *has the* ***lowest*** *precedence(*$\neg \wedge \vee \rightarrow \leftrightarrow \equiv$*)*

Example 2 $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Example 3 $p \rightarrow q \equiv \neg p \vee q$

Proof *of logical equivalences*

1. truth tables n single propositions, 2^n *raws in the table*

2. algebraic rules of logical equivalences

Algebraic rules of logical equivalences

Logical equivalences laws

$p \vee \mathbf{F} \equiv p$	$p \wedge \mathbf{T} \equiv p$	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
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$	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

Since disjunction($\vee$) and conjunction($\wedge$) are ***associative****,*

$p \vee q \vee r$ *and* $p \wedge q \wedge r$ *are* ***well defined****.*

Let $p_1, p_2, \ldots, p_n$ *be n propositions. Then*

$$p_1 \vee p_2 \vee \ldots \vee p_n = \vee_{j=1}^{n} p_j = \vee_{j \in \{1, 2, \ldots, n\}} p_j \text{ and}$$

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n = \wedge_{j=1}^{n} p_j = \wedge_{j \in \{1, 2, \ldots, n\}} p_j \text{ are } \textbf{well defined}.$$

Extened De Morgan's law

$$\neg \vee_{j \in \{1, 2, \ldots, n\}} p_j \equiv \wedge_{j \in \{1, 2, \ldots, n\}} \neg p_j.$$

$$\neg \wedge_{j \in \{1, 2, \ldots, n\}} p_j \equiv \vee_{j \in \{1, 2, \ldots, n\}} \neg p_j.$$

Logical equivalences involving conditional statements

$p \to q \equiv \neg p \vee q$ *disjuntive normal form*

$\neg(p \to q) \equiv p \wedge \neg q$ *conjuntive normal form*

$p \to q \equiv \neg q \to \neg p$ *contrapositive*

$p \vee q \equiv \neg p \to q$

$p \wedge q \equiv \neg(p \to \neg q)$

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

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

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

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

Logical equivalences involving biconditional statements

$p \leftrightarrow q \equiv q \leftrightarrow p$ *commutative(symetric)*

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ *definition of biconditional*

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$ *symetricity of biconditional*

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ *disjuntive normal form(truth table)*

$\equiv (p \vee \neg q) \wedge (\neg p \vee q)$ *conjuntive normal form*

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$ *De Mogran's law for bicondi.*

1.3 Predicates and Quantifiers

Predicate**: a **proposition** with **variable

A predicate P(x) has the proposition P and the variable x

Example 1 Let P(x) denotes "x > 3". Then

P(4) denotes "4 > 3" is T. P(2) denote "2 > 3" is F.

Let $x_1, x_2, \ldots, x_n$ be n variables. Then

*$P(x_1, x_2, \ldots, x_n)$ is the value of **propositional(boolean) function***

(조건명제) P at the n-tuple $(x_1, x_2, \ldots, x_n)$, and

*P is also called **predicate**.*

Predicate is a proposition with variables.

Quantifiers

*A **predicate** is **not** a **proposition** only if, **variables** are **not fixed**.*
*If **all** the variables are fixed, the predicate **becomes** a propositions.*
How can we fix variables?

*Consider **universe of discourse(domain)** for each **variable**.*

*If P(x) is true for **all** values of x in the **universe of discourse**,*
$\forall xP(x)$ *is true*
otherwise $\forall xP(x)$ *is false.*
$\therefore\ \forall xP(x)$ *becomes a **proposition**.*

predicate calculus

Definition** 1 **Universal quantifier

$\forall xP(x)$ *is a proposition such that*

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

$\forall$ *is called* ***universal quantifier****.*

We read $\forall xP(x)$ *as "for all x P(x)".*

An element for which $\forall xP(x)$ *is* ***false*** *is called*

a ***counterexample*** *of* $\forall xP(x)$*.*

Let a set $\{x_1, x_2, \ldots, x_n\}$ *be the domain(****finite****). Then*

$$\forall xP(x) \equiv {}^{\forall}x \in \{x_1, x_2, \ldots, x_n\} \ni P(x_j) = \wedge_{j \in \{1, 2, \ldots, n\}} P(x_j).$$

Definition** 2 **Existential quantifier

$\exists xP(x)$ *is a proposition such that*

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

$\exists$ *is called* ***existential quantifier****.*

$$\exists xP(x) \equiv {}^{\exists}x \in \{x_1, x_2, \ldots, x_n\} \ni P(x_j) = \vee_{j \in \{1, 2, \ldots, n\}} P(x_j).$$

Binding variables

A variable is said to be ***bound****, if the variable binds to*

(1) quantifiers(∀, ∃) or

(2) specific value(in the domain), and

it is said to be ***free****, otherwise.*

scope *of* ***quantifier***

the ***part of logical expression*** *to which the quantifier is applied*

Example

$\exists x(P(x) \wedge R(x)) \vee \forall x R(x) \equiv \exists x(P(x) \wedge R(x)) \vee \forall y R(y)$.

Negations

$\forall x P(x)$ *where* $P(x)$

"Every student in this class has taken a course in calculus."

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

"It is ***not*** *the case that every student in this class has taken a course in calculus."*

is ***logically equivalent*** *to*

"There is a student in this class who has ***not*** *taken a course in calculus."*

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

"It is not the case that there is a student who has ***not*** *taken a course in the calculus"*

"Every student in this class has ***not*** *taken class"*

Proof*: De Morgan's Law*

Let $\{x_1, x_2, \ldots, x_n\}$ *be a set of discourse. Then*

$$\neg\forall x P(x) = \neg\wedge_{j\in\{1, 2, \ldots, n\}} P(x_j) \equiv \vee_{j\in\{1, 2, \ldots, n\}} \neg P(x_j) = \exists x \neg P(x).$$

$$\neg\exists x P(x) = \neg\vee_{j\in\{1, 2, \ldots, n\}} P(x_j) \equiv \wedge_{j\in\{1, 2, \ldots, n\}} \neg P(x_j) = \forall x \neg P(x).$$

Translating from English into Logical expressions

Examples from Lewis Carroll

Alice in Wondeland

Logic Programming

1.4 Nested Quantifier

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

The Order of Quantifiers

Example 15 Let Q(x, y) denotes "x+y=0"

$\forall x \exists y(x+y=0)$ *vs* $\exists y \forall x(x+y=0)$

Translating Statements involving Nested Quantifiers

Translating Sentences into Logical Expressions

Negating Nested Quantifier

Example 12 Negate $\forall x \exists y(xy=1)$

$\neg \forall x \exists y(xy=1) \equiv \exists x \neg \exists y(xy=1) \equiv \exists x \forall y(\neg xy=1) \equiv \exists x \forall y(xy \neq 1)$.

1.5 Rules of Inference

Proof: ***valid arguments*** *that*
establish the truth of mathematical statements

arguments *a sequence of statement that ends with a* ***conclusion***

valid *the* ***conclusion*** *must follow from the truth of the* ***preceding statements*** *or* ***premises of the argument***

An ***argument*** *is* ***valid****, if and only if,*

it is impossible for ***all premises*** *to be* ***true*** *and* ***conclusion*** *to be* ***false***

or If all premises are true, then the conclusion is true.

Rules of inference

deducing *new statements from statements we already have.*

propositional logic

Incorrect reasoning

fallacies

rules of inference for ***qualified*** *statements*

Valid Arguments in Propositional Logic

Definition ***argument*** *a sequence of propositions preceding* ***premises*** *and finally a* ***conclusion***.

argument form

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

valid *argument*

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ *is* ***tautology***.

$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$.

p_1

p_2

$\ldots$

p_n

q.

Modus ponen

$$\begin{array}{l} p \\ \underline{p \to q} \\ \therefore\ q \end{array} \qquad [p \wedge (p \to q)] \Rightarrow q$$

Modus tollen

$$\begin{array}{l} \neg q \\ \underline{p \to q} \\ \therefore\ \neg p \end{array} \qquad [\neg q \wedge (p \to q)] \Rightarrow \neg p$$

Hypothetical syllogism

$$\begin{array}{l} p \to q \\ \underline{q \to r} \\ \therefore\ p \to r \end{array} \qquad [(p \to q) \wedge (q \to r)] \Rightarrow (p \to r)$$

Disjunctive syllogism

$$\begin{array}{l} p \vee q \\ \underline{\neg p\ \ \ } \\ \therefore\ q \end{array} \qquad [(p \vee q) \wedge \neg p] \Rightarrow q$$

Addition

$$\begin{array}{l} \underline{p\ \ \ \ } \\ \therefore\ p \vee q \end{array} \qquad p \Rightarrow (p \vee q)$$

Simplification

$$\begin{array}{l} \underline{p \wedge q} \\ \therefore\ p \end{array} \qquad (p \wedge q) \Rightarrow p$$

Conjunction

$$\begin{array}{l} p \\ \underline{q\ \ \ \ } \\ \therefore\ p \wedge q \end{array} \qquad [(p) \wedge (q)] \Rightarrow (p \wedge q)$$

Resolution

$$\begin{array}{l} p \vee q \\ \underline{\neg p \vee r} \\ \therefore\ q \vee r \end{array} \qquad [(p \vee q) \wedge (\neg p \vee r)] \Rightarrow (q \vee r)$$

Example 6 Prove that four hypotheses

(H1) "It is not sunny and its cold."	$\neg sunny \wedge cold$
(H2) "We will swim only if it is sunny."	$swim \rightarrow sunny$
(H3) "If we do not swim, then we will canoe."	$\neg swim \rightarrow canoe$
(H4) "If we canoe, then we will be home early,"	$canoe \rightarrow early$

Concludes

"We will be home early"	*early*

proof

1. $\neg sunny \wedge cold$	*Hypothesis(H1)*
2. $\neg sunny$	*Simplification using (1)*
3. $swim \rightarrow sunny$	*Hypothesis(H2)*
4. $\neg swim$	*Modus tollen using (2) and (3)*
5. $\neg swim \rightarrow canoe$	*Hypothesis(H3)*
6. $canoe$	*Modus ponen using (4) and (5)*
7. $canoe \rightarrow early$	*Hypothesis(H4)*
8. $early$	*Q.E.D.*

Resolution

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

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

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

Fallacies

$((p \rightarrow q) \wedge q) \not\Rightarrow p$ ***fallacy** of **affirming** the **conclusion***

$((p \rightarrow q) \wedge \neg p) \not\Rightarrow \neg q$ ***fallacy** of **denying** the **hypothesis***

Logic says nothing when hypotheses are false!

Rules of inferences for qualified Statements

Universal instantiation

$\underline{\forall x P(x)}$

$\therefore P(c)$

Universal generalization

$\underline{P(c) \text{ for a arbitrary } c}$

$\therefore \forall x P(x)$

Existential instantiation

$\underline{\exists x P(x)}$

$\therefore P(c)$ for some element c

Existential generalization

$\underline{P(c) \text{ for some element } c}$

$\therefore \exists x P(x)$

1.6 Introduction to Proofs

Some Terminologies

***Theorem**: A statement that has been proven to be **true**.*

***Axiom: Assumption** to be true (often unproven)*
*defining the **structures** about which we are reasoning.*

Rules of inference**: **Patterns** of logically valid **deductions
*from **hypotheses to conclusion.***

Lemma**: A **minor** theorem used as a **stepping stone
to prove a major theorem

***Corollary**: A **minor** theorem proven*
*as an **easy consequence** of a major theorem*

***Conjecture**: A statement whose truth value has not been proven.*
(A conjecture may be widely believed to be true, regardless)

***Theory**: The set of **all theorems** that*
*can be proven from a **given** set of **axioms***

Direct Proof

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

$P(c) \rightarrow Q(c)$ *universal generalization* ($\Uparrow$)

$p \rightarrow q$ *propositional calculus*

Example 1 "If n is odd integer, then n^2 *is odd"*

proof $\forall n(O(n) \Rightarrow O(n^2))$ *where O(n) is "n is odd"*

$n = 2k + 1$ $O(n)$

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ $O(n^2)$

$O(n) \Rightarrow O(n^2)$ *implication*

$\forall n(O(n) \Rightarrow O(n^2))$ *universal generalization*

Proof by Contrapositive

$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

Example 3 "If n is an integer and 3n + 2 is odd, then n is odd"

proof $3n + 2 = 2k + 1$, $n = ?$

If n is even, then 3n+2 is even.
n = 2k, 3n+2 = 6k + 2 = 2(3k + 1) is even.

Vacuous proof

*If p = **F**, p ⇒ q is a tautology.*
See Section 4.1 Mathematical induction

Trivial proof

*If q= **T**, p ⇒ q is a tautology.*
See Section 4.1 Mathematical induction

Proofs by Contradiction

*If ¬p ⇒ q, q = **F**, p is a tautology.*
If ¬p ⇒ (r ∧ ¬r), p is a tautology.
*If ¬p ⇒ **F**, p is a tautology.*

Example 9

p = "At least four of any 22 days must fall on the same day of the week"

$\neg p$ = "At most three of 22 days ..."

r = "22 days are chosen"

$\neg p \rightarrow (r \wedge \neg r)$, p is a tautology.

Example 10 Prove that $\sqrt{2}$ is irrational.

p = "$\sqrt{2}$ is irrational" *$\neg p$ = "$\sqrt{2}$ is rational"*

$\sqrt{2}$ = a/b, a and b are integers.

$2 = a^2/b^2$ *$2b^2 = a^2$.*

a^2 is even, a is also even. a = 2c.

$a^2 = 4c^2 = 2b^2$. *$b^2 = 2c^2$.*

b^2 is even. b is even.

*$\sqrt{2}$ = a/b, a and b are **even** integers*

Proof of Equivalence

$(p \Leftrightarrow q) \equiv [(p \Rightarrow q) \wedge (q \Rightarrow p)]$

$(p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n) \equiv [(p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \ldots \wedge (p_n \Rightarrow p_1)]$

Counter Example

To prove $\forall x P(x)$ is false

an example x P(x) is false

Mistakes in Proof

Example 16 divide by zero

Example 17 $(p \Rightarrow q)$ does not implies $(q \Rightarrow p)$

Example 18 $(p \Rightarrow q)$ does not implies $(\neg p \Rightarrow \neg q)$

1.7 Proof Methods and Strategy

Exhaustive Proof and Proof by Case

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \Rightarrow q] \equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \ldots \wedge (p_n \Rightarrow q)$$