

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**.

propositional (or statement; 문) *variables*(변수)

p, q, r, s, \dots

propositional constants(상수)

T: truth value(true)

F: falsehood value(false)

propositional calculus, propositional logic or FOL(First Order Logic)

Greek philosopher Aristotle

2300 years ago

Compounded propositions(복합명제)

*propositions that are formed from existing propositions
using logical operators(connectives; \neg , \wedge , \vee , \rightarrow , \leftrightarrow)*

Def. 1 Negation(Not; \neg)

*Let p be a proposition, $\neg p$ is a (new) **compounded** proposition,
called **negation** of p , or “**not p ”***.

Def. 2 Conjunction(And; \wedge)

*Let p and q be a propositions, $p \wedge q$ is a (compounded) proposition,
called **conjunction** of p and q , or “ **p and q ”***.

Def. 3 Disjunction(Or, Inclusive or; \vee)

*Let p and q be a propositions, $p \vee q$ is a proposition,
called **disjunction** of p and q , or “ **p or q ”***.

\neg **unary prefix operator**

\wedge , \vee , \oplus , \rightarrow , \leftrightarrow **binary infix operator**

Def. 4 Exclusive or (\oplus) See truth table (Table 4, p 6)

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

Def. 5 Conditional (Implication 조건 ; \rightarrow)

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 ”, ... (See p. 6)

p is called **hypothesis** (가정), **premise or antecedent** (전건) of $p \rightarrow q$
 q is called **conclusion** (결론) or **consequence** (후건) of $p \rightarrow q$

See truth table of **implication** (Table 5, p 6)

$p \rightarrow q$ is **false** only in the case that p is **true** and 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 $p \rightarrow q$ be a implication proposition. Then

$q \rightarrow p$ is a **converse** (역) of $p \rightarrow q$,

$\neg q \rightarrow \neg p$ is a **contrapositive** (대우) of $p \rightarrow q$, and

$\neg p \rightarrow \neg q$ is a **inverse** (이) of $p \rightarrow q$.

$p \rightarrow q$ and **contrapositive** $\neg q \rightarrow \neg p$ are **equivalent**.

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

Def. 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 $(p \rightarrow q) \wedge (q \rightarrow p)$.

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

Truth Table of Compound Proposition

Example 11(p. 10)

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

Table 7(p 10)

Precedence of Logical Operators

\neg *highest*

\wedge

\vee

...

\rightarrow

\leftrightarrow *lowest*

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

Logic and Bit Operations

T	<i>1</i>
F	<i>0</i>

Def. 7 A *bit string* is a sequence of zero or more bits.

The *length* of a string is the number of bits in the string.

1.2 Application of Logic Programs

Translating English Sentences

System Specifications

Boolean Searches

Logic Puzzle

Exa. 7 knight(truth teller) or knave(liar)

A says “B is a knight.”

*B says “Two of us are **opposite** types.”*

???

Logic or Digital Circuits

Three logic gates (Fig. 1, p 20)

1. inverter or NOT gate(\neg) 2. \vee : OR gate(\vee) 3. AND gate(\wedge)

Normal Forms(Sec. 1.7)

Combinatorial circuit(Fig. 2, p 20; Fig.3 p 21)

1.3 Propositional Equivalencies

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

A proposition that is always false(**F**): **contradiction**

Otherwise(**T** or **F**): **contingency**(우연성).

Ex. 1 $p \vee \neg p \equiv \mathbf{T}$ and $p \wedge \neg p \equiv \mathbf{F}$.

But $p \vee q$, $p \wedge q$, $\neg p$, $p \rightarrow q$, ... are **contingency!**

Logical Equivalences

Def. 2 Two propositions p and q are **logically equivalent**,

if $p \leftrightarrow q$ is a **tautology**, written, $p \equiv q$ (or $p \Leftrightarrow q$).

Ex. 2 $\neg(p \vee q) \equiv \neg p \wedge \neg q$

De Morgan's law

Ex. 3 $p \rightarrow q \equiv \neg p \vee q$

normal form($\neg \wedge \vee$) *elimination of \rightarrow*

Ex. 4 $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Disitibutive law

truth table

Algebraic rules of logical equivalencies(Table 6, p. 25)

1. Identity laws	$p \vee \mathbf{F} \equiv p$	$p \wedge \mathbf{T} \equiv p$
2. Domination laws	$p \vee \mathbf{T} \equiv \mathbf{T}$	$p \wedge \mathbf{F} \equiv \mathbf{F}$
3. Idempotent laws	$p \vee p \equiv p$	$p \wedge p \equiv p$
4. Double negation law		$\neg(\neg p) \equiv p$
5. Commutative laws	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
6. Associative laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
7. Distributive laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
8. DeMorgan's laws	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
9. Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
10. Negation laws	$p \vee \neg p \equiv \mathbf{T}$	$p \wedge \neg p \equiv \mathbf{F}$
11. T/F laws	$\neg \mathbf{T} \equiv \mathbf{F}$	$\neg \mathbf{F} \equiv \mathbf{T}$

Logical equivalencies involving conditional statements (Table 7, p 26)

$$p \rightarrow q \equiv \neg p \vee q \quad \text{disjunctive normal form (elimination of } \rightarrow \text{)}$$

$$p \rightarrow q \equiv \neg q \rightarrow \neg p \quad \text{contrapositive}$$

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

$$\neg(p \rightarrow q) \equiv p \wedge \neg q \quad \text{conjunctive normal form}$$

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

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

Logical equivalencies involving biconditional statements (Table 8, p 26)

$$p \leftrightarrow q \equiv q \leftrightarrow p \quad \text{symmetricity of biconditional}$$

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p) \quad \text{definition of biconditional}$$

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q \quad \text{symmetricity of biconditional}$$

$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q) \quad \text{disjunctive normal form}$$

$$\equiv (p \vee \neg q) \wedge (\neg p \vee q) \quad \text{conjunctive normal form}$$

$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q \quad \text{De Morgan's law for bicond.}$$

Using De Morgan's Law

Constructing New Logical Equivalences

Two ways to prove the logical equivalencies

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

Venn diagram *n propositions, 2^n areas in the diagram*

2. *algebraic rules of logical equivalencies* *Ex. 6, 7, 8*

Propositional Satisfiability

*A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that make it true, otherwise **unsatisfiable**.*

Application of Satisfiability

Solving Satisfiability Problem

Assume n-variables, 2^n rows in the truth table,

Example $2^{10} = 1,024 \cong 1K$, $2^{32} = 2^2 2^{30} \cong 4 K^3 = 4G$.

Extension of Disjunction(\vee) and Conjunction(\wedge)

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

Let p_1, p_2, \dots, p_n be n propositions and $\mathbf{N}_{1,n} = \{1, 2, \dots, n\}$. Then

$$p_1 \vee p_2 \vee \dots \vee p_n = \bigvee_{i=1}^n p_i = \bigvee_{i \in \{1, 2, \dots, n\}} p_i = \bigvee_{j \in \mathbf{N}_{1,n}} p_j \text{ and}$$

$$p_1 \wedge p_2 \wedge \dots \wedge p_n = \bigwedge_{i=1}^n p_i = \bigwedge_{i \in \{1, 2, \dots, n\}} p_i = \bigwedge_{j \in \mathbf{N}_{1,n}} p_j \text{ are well defined.}$$

Extension of De Morgan's Laws

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

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

$$\neg \bigvee_{i \in \mathbf{N}_{1,n}} p_i \equiv \bigwedge_{i \in \mathbf{N}_{1,n}} \neg p_i$$

$$\neg \left(\bigwedge_{i \in \mathbf{N}_{1,n}} \neg p_i \right) \equiv \bigvee_{i \in \mathbf{N}_{1,n}} p_i.$$

Truth table of n propositions

1 proposition

2 rows in the truth table

2 propositions

4 rows in the truth table

...

n propositions

2^n rows in the truth table

1.4 Predicates and Quantifiers

Predicate(조건명제): a **proposition** with **variable**

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

Ex. 1 Let $P(x)$ denotes “ $x > 3$ ”. Then

$P(4)$ denotes “ $4 > 3$ ” is **T**. $P(2)$ denote “ $2 > 3$ ” is **F**.

Let D be an **universe(or domain) of discourse (set)** for x . Then

$P: D \rightarrow \{\mathbf{T}, \mathbf{F}\}$ **propositional(boolean) function**

Ex. Let $O(n)$ denotes “ n is an odd number”. Then

$O(3)$ is **T** and $P(4)$ **F** are **propositions**.

But $O(n)$ is **not a proposition**.

Predicate is a boolean function, but not a proposition.

But! ...

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 set) for each variable.

If $P(x)$ is true for all values of x in the universe of discourse(U),

$\forall xP(x)$ is true

otherwise $\forall xP(x)$ is false.

*$\therefore \forall xP(x)$ becomes a **proposition**.*

predicate calculus

Def. 1 Universal quantifier(\forall)

$\forall xP(x)$ 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 $P(x)$.”

Let a set $D = \{x_1, x_2, \dots, x_n\}$ be the **domain of discourse** for x . Then

$$\forall x \in D P(x) \equiv P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)$$

An element $c \in D$. \exists . $P(c) = \mathbf{F}$ is a **counterexample** of $\forall xP(x)$.

function “ $\forall x \in D P(x)$ ” $\in \mathbf{B}$ (Exa. 1.5.7, Johnsonbaugh)

for $d \in D$ do if $P(d) \rightarrow \text{skip}$ / $\neg P(d) \rightarrow \text{return F}$ fi od; return T.

건너뛰기

Def. 2 Existential quantifier(\exists)

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

“There **exists** an element x in the **domain** such that $P(x)$.”

\exists is called **existential quantifier**.

We read $\exists xP(x)$ as “**there is at least one** x such that $P(x)$.”

Let a set $D = \{x_1, x_2, \dots, x_n\}$ be the **domain of discourse** for x . Then

$$\exists x \in D P(x) \equiv P(x_1) \vee P(x_2) \vee \dots \vee P(x_n).$$

An element $c \in D$. \exists . $P(c) = \mathbf{T}$ is a **good example** of $\exists xP(x)$.

function “ $\exists_{x \in D} P(x)$ ” $\in \mathbf{B}$ (Exa. 1.5.12, Johnsonbaugh)
for $d \in D$ **do** **if** $P(d) \rightarrow$ **return** \mathbf{T} **|** $\neg P(d) \rightarrow$ **skip** **fi** **od**; **return** \mathbf{F} .

Indexed set notation

Let a set $D = \{x_1, x_2, \dots, x_n\}$ be the **domain of discourse** for x . Then

$$\begin{aligned}\forall x \in D P(x) &\equiv P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n) \equiv \bigwedge_{i=1}^n P(x_i) \\ &\equiv \bigwedge_{i \in \{1, 2, \dots, n\}} P(x_i) \equiv \bigwedge_{x \in D} P(x) \quad \textit{indexed set notation.}\end{aligned}$$

$$\begin{aligned}\exists x \in D P(x) &\equiv P(x_1) \vee P(x_2) \vee \dots \vee P(x_n) \equiv \bigvee_{i=1}^n P(x_i) \\ &\equiv \bigvee_{i \in \{1, 2, \dots, n\}} P(x_i) \equiv \bigvee_{x \in D} P(x).\end{aligned}$$

Uniqueness quantifier

$$\exists! x \in D P(x) \textit{ or } \exists_1 x \in D P(x)$$

“There is a **unique** x such that $P(x)$.”

Binding variables

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

(1) quantifiers(\forall , \exists) or

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

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

If **all** of the variables in a predicate is **bound**,

then the predicate is a **proposition**.

Otherwise [Or there is **one or more free** variables] it is **not**.

Negating Quantified Expressions

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

\forall and \exists has higher precedence than \neg , \wedge , or \vee .

Proof: De Morgan's Law

Let D be a universe of discourse. Then

$$\neg \forall x \in D P(x) = \neg \bigwedge_{x \in D} P(x_j) \equiv \bigvee_{x \in D} \neg P(x_j) = \exists x \neg P(x).$$

$$\neg \exists x \in D P(x) = \neg \bigvee_{x \in D} P(x_j) \equiv \bigwedge_{x \in D} \neg P(x_j) = \forall x \neg P(x).$$

Translating from English into Logical expressions

Examples from Lewis Carroll

Alice in Wonderland

Ex. 26

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

$$\underline{\exists x (P(x) \wedge \neg R(x))}$$

$$\exists x (Q(x) \wedge \neg R(x))$$

$$\exists x (P(x) \not\rightarrow \wedge \neg R(x))$$

$$\exists x (Q(x) \not\rightarrow \wedge \neg R(x))$$

Logic Programming(Prolog)

Disjunction of **predicates**(literals) with **at most one un-negated** literals.

$$\neg P_1(X_1) \vee \neg P_2(X_2) \vee \dots \vee \neg P_n(X_n) \vee P(X)$$

$$\equiv \neg(P_1(X_1) \wedge P_2(X_2) \wedge \dots \wedge P_n(X_n)) \wedge P(X)$$

$$\equiv (P_1(X_1) \wedge P_2(X_2) \wedge \dots \wedge P_n(X_n)) \Rightarrow P(X)$$

$$H(X) \Leftarrow B_1(X_1) \wedge B_2(X_2) \wedge \dots \wedge B_n(X_n)$$

Four cases for **head** and body literals and **three** clauses

1. **query** clause $\Leftarrow B_1(X_1) \wedge B_2(X_2) \wedge \dots \wedge B_n(X_n)?$

2. **rule** clauses $H(X) \Leftarrow B_1(X_1), B_2(X_2), \dots, B_n(X_n).$

3. **fact** clauses $H(X).$

4. **tautology** $.$

Logic program(Prolog)

A **query** clause and **rules** and **facts**.

database *Ex. 28*

Syntax of Prolog

<i>Clause</i>	<i>query clause</i>	<i>body Literals ?</i>
	<i>rule clause</i>	<i>head Literal :- body Literals .</i>
	<i>fact clause</i>	<i>head Literal .</i>
<i>Literal</i>		<i>predicate (termS)</i>
<i>Term</i>		<i>constant variable literal</i>

Ex. *map coloring*

:- map(A, B, C, D, E)?

*map(A, B, C, D, E) :- next(A, B), next(A, C), next(A, D),
next(B, C), next(B, E), next(C, D), next(C, E), next(D, E).*

next(X, Y) :- diff(X, Y) | diff(Y, X).

<i>diff(red, blue).</i>	<i>diff(red, green).</i>	<i>diff(red, yellow).</i>
	<i>diff(blue, green).</i>	<i>diff(blue, yellow).</i>
		<i>diff(green, yellow).</i>

1.5 Nested Quantifier

Ex. 1 $\forall x \in \mathbf{R} \forall y \in \mathbf{R} (x+y = y+x)$

$\forall x \in \mathbf{N} \exists y \in \mathbf{Z} (x+y = 0)$

$\forall x \in \mathbf{R} \forall y \in \mathbf{R} \forall z \in \mathbf{R} (x+(y+z) = (x+y)+z)$

*commutative law for +
extend \mathbf{N} to \mathbf{Z} for –*

associative law for +

The Order of Quantifiers

$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$

function “ $\forall x \in D \forall y \in E P(x, y)$ or $\forall y \forall x P(x, y)$ ” $\in \mathbf{B}$ $\forall x \forall y P(x, y)$

for $x \in D$ **do** **for** $y \in E$ **do** **if** $P(x, y) \rightarrow \text{skip} \mid \neg P(x, y) \rightarrow \text{return } F$ **fi** **od**; **return** T

for $y \in E$ **do** **for** $x \in D$ **do** **if** $P(x, y) \rightarrow \text{skip} \mid \neg P(x, y) \rightarrow \text{return } F$ **fi** **od**; **return** T

for $(x, y) \in D \times E$ **do** **if** $P(x, y) \rightarrow \text{skip} \mid \neg P(x, y) \rightarrow \text{return } F$ **fi** **od**; **return** T

$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$

function “ $\exists x \in D \exists y \in E P(x, y)$ or $\exists y \exists x P(x, y)$ ” $\in \mathbf{B}$ $\exists x \exists y P(x, y)$

for $(x, y) \in D \times E$ **do** **if** $P(x, y) \rightarrow \text{return } F \mid \neg P(x, y) \rightarrow \text{skip}$ **fi** **od**; **return** F

Ex. 4 $\exists y \in \mathbf{R} \forall x \in \mathbf{R} (x+y = 0) \equiv \mathbf{F}$ $\forall x \in \mathbf{R} \exists y \in \mathbf{R} (x+y = 0) \equiv \mathbf{T}$

$\forall x \exists y P(x, y) \not\equiv \exists y \forall x P(x, y)$

function “ $\forall x \in D \exists y \in E P(x, y)$ ” $\in \mathbf{B}$ $\forall x \exists y P(x, y)$

for $x \in D$ *do* $\forall x$
 for $y \in E$ *do* $\exists y$

if $P(x, y) \rightarrow \mathit{break} \mid \neg P(x, y) \rightarrow \mathit{skip}$ *fi od*;

if $P(x, y) \rightarrow \mathit{skip} \mid y \notin E \rightarrow \mathit{return F}$ *fi od*;

return T

function “ $\exists x \in D \forall y \in E P(x, y)$ ” $\in \mathbf{B}$ $\exists x \forall y P(x, y)$

for $x \in D$ *do* $\exists x$
 for $y \in E$ *do* $\forall y$

if $P(x, y) \rightarrow \mathit{skip} \mid \neg P(x, y) \rightarrow \mathit{break}$ *fi od*;

if $y \notin E \rightarrow \mathit{return T} \mid \neg P(x, y) \rightarrow \mathit{skip}$ *fi od*;

return F

$\exists y \forall x P(x, y) \Rightarrow \forall x \exists y P(x, y)$ *but* $\forall x \exists y P(x, y) \not\Rightarrow \exists y \forall x P(x, y)$.

Let x_1, x_2, \dots, x_n be n variables with **domain of discourses** D_1, D_2, \dots, D_n .

Then **predicate** $P(x_1, x_2, \dots, x_n)$ is

$$P: (D_1 \times D_2 \times \dots \times D_n) \rightarrow \{\mathbf{T}, \mathbf{F}\}$$

Ex. 4 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

Ex. 12 $\neg \forall x \exists y (xy=1) \equiv \exists x \neg \exists y (xy=1) \equiv \exists x \forall y (\neg xy=1) \equiv \exists x \forall y (xy \neq 1)$.

1.6 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

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

valid argument

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

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

p_1

p_2

...

p_n

$q.$

Modus ponens 전건긍정

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

Modus tollens 후건부정

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

Hypothetical syllogism

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

Disjunctive syllogism

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

Addition

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

Simplification

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

Conjunction

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

Resolution

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

Example 6 Prove that four hypotheses

(H1) “It is not sunny and its cold.”

$\neg \text{sunny} \wedge \text{cold}$

(H2) “We will swim only if it is sunny.”

$\text{swim} \rightarrow \text{sunny}$

(H3) “If we do not swim, then we will canoe.”

$\neg \text{swim} \rightarrow \text{canoe}$

(H4) “If we canoe, then we will be home early.”

$\text{canoe} \rightarrow \text{early}$

Concludes

“We will be home early”

early

<i>proof</i>	1. $\neg \text{sunny} \wedge \text{cold}$	<i>Hypothesis(H1)</i>
	2. $\neg \text{sunny}$	<i>Simplification using (1)</i>
	3. $\text{swim} \rightarrow \text{sunny}$	<i>Hypothesis(H2)</i>
	4. $\neg \text{swim}$	<i>Modus tollens using (2) and (3)</i>
	5. $\neg \text{swim} \rightarrow \text{canoe}$	<i>Hypothesis(H3)</i>
	6. <i>canoe</i>	<i>Modus ponens using (4) and (5)</i>
	7. $\text{canoe} \rightarrow \text{early}$	<i>Hypothesis(H4)</i>
	8. <i>early</i>	<i>Q.E.D.</i>

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***

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

$$\therefore P(c)$$

Universal generalization

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

$$\therefore \forall xP(x)$$

Existential instantiation

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

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

Existential generalization

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

$$\therefore \exists xP(x)$$

1.7 Normal Forms

A **well formed formula**(wff) of propositional logic is a **string** over propositional **constants**(**T**, **F**), propositional **variables**, **connectives** \neg , \wedge , \vee , \rightarrow , \leftrightarrow , and parenthesis in **proper manner**.

Syntax grammar for (**well-formed**) propositions

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

Def. 0 A **constants**, **variable** or the **negation** of variable is a **literal**.

$$p, q, r, \dots, \neg p, \neg q, \dots$$

An **elementary product** is a **product**(conjunction; \wedge) of **literals**.

$$p \wedge q \wedge \dots \wedge \neg p \wedge \dots \equiv \dots \wedge \mathbf{F} \wedge \dots \equiv \mathbf{F}.$$

An **elementary sum** is a **sum**(disjunction; \vee) of **literals**.

$$p \vee q \vee \dots \vee \neg q \vee \dots \equiv \dots \vee \mathbf{T} \vee \dots \equiv \mathbf{T}.$$

Def. 1 A formula which is **equivalent** to a given formula and consists of

*a **sum**(\vee) of elementary product is called a **disjunctive**(\vee) normal form(DNF).*

***Def. 2** A formula which is **equivalent** to a given formula and consists of a **product**(\wedge) of elementary sum is called a **conjunctive**(\wedge) normal form(CNF).*

*DNF and CNF are **not** unique.*

*Let p_1, p_2, \dots, p_n be n propositions in a formula. Then a **minterm** of the formula is an elementary **product**(\wedge).*

$$m_n = q_1 \wedge q_2 \wedge \dots \wedge q_n \text{ where } q_i = p_i \text{ or } q_i = \neg p_i.$$

*a **Maxterm** of the formula is an elementary **sum**(\vee).*

$$M_n = q_1 \vee q_2 \vee \dots \vee q_n \text{ where } q_i = p_i \text{ or } q_i = \neg p_i.$$

2^n minterms and 2^n Maxterms.

Example $m_0 = p_1 \wedge p_2 \wedge \dots \wedge p_n$, $M_{2^n-1} = \neg p_1 \vee \neg p_2 \vee \dots \vee \neg p_n$.

$$m_0 \equiv \neg M_{2^n-1}.$$

Def. 3 A formula consisting of a **sum of minterms** only is called a **principal disjunctive normal form (PDNF)**.

sum of true rows in the truth table

Def. 4 A formula consisting of a **product of maxterms** only is called a **principal conjunctive normal form (PCNF)**.

Consider a binary number $i = b_1 b_2 \dots b_n$ with $0 \leq i < 2^n$,

where $b_i = 1$, if $q_i = p_i$ and $b_i = 0$, if $q_i = \neg p_i$.

Let a PCNF of a logical formula be $\bigwedge_{b_i} m_i$. Then an equivalent PDNF is

$$m_i \equiv \neg \neg \bigvee_{b_i} m_i \equiv \neg \bigwedge_{b_i} \neg m_i \equiv \neg \bigwedge_{\bar{b}_i} M_i. \text{ where } \bar{b}_i \text{ is a complement of } b_i.$$

The **negation** of product of **false** rows in the truth table is PCNF.

PDNF and PCNF are **unique**.

Example

p	q	b	<i>minterm</i>	<i>maxterm</i>	$p \rightarrow q$	$\neg(p \rightarrow q)$
F	F	00	$\neg p \wedge \neg q$	$\neg p \vee \neg q$	T	F
F	T	01	$\neg p \wedge q$	$\neg p \vee q$	T	F
T	F	10	$p \wedge \neg q$	$p \vee \neg q$	F	T
T	T	11	$p \wedge q$	$p \vee q$	T	F

$$\begin{aligned}
 p \rightarrow q &\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q) && \equiv \overline{p}q + \overline{p}q + pq && \text{PDNF} \\
 &\equiv (\neg p \vee q) && \equiv (\overline{p} + q) && \text{PCNF} \\
 \neg(p \rightarrow q) &\equiv \neg(\neg p \vee q) \equiv p \wedge \neg q && \equiv p\overline{q} && \text{PDNF} \\
 &\equiv \neg[(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q)] && \equiv (p + q)(p + \overline{q})(\overline{p} + \overline{q}) && \text{PCNF}
 \end{aligned}$$

1.8 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

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

$$P(c) \rightarrow Q(c) \quad \text{universal generalization } (\uparrow\uparrow)$$

$$p \rightarrow q \quad \text{propositional calculus}$$

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”

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

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

$$O(n) \Rightarrow O(n^2) \quad \text{implication}$$

$$\forall n(O(n) \Rightarrow O(n^2)) \quad \text{universal generalization}$$

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 $p = \mathbf{F}$, $p \Rightarrow q$ is a tautology.

See Section 4.1 Mathematical induction

Trivial proof

If $q = \mathbf{T}$, $p \Rightarrow q$ is a tautology.

See Section 4.1 Mathematical induction

Proofs by Contradiction

If $\neg p \Rightarrow q$, $q = \mathbf{F}$, p is a tautology.

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

If $\neg p \Rightarrow \mathbf{F}$, 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

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

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

Counter Example

To prove $\forall xP(x)$ 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 $(\neg p \Rightarrow \neg q)$

1.9 Proof Methods and Strategy

Exhaustive Proof and Proof by Case

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

Existence Proofs

Uniqueness Proofs

Proof Statuettes

Looking for Counterexamples

Proof Strategy in Action

Tilings

The Role of Open Problems

Additional Proof Methods