DISCRETE MATHEMATICS
（离散数学）

云南大学数学系
李 建 平

Chapter 2 LOGIC

2.1 PROPOSITIONS AND LOGICAL OPERATIONS

A **statement** (命题) or **proposition** is a declarative sentence (陈述句) that is either true or false, but not both.

Example: Which of the following are statements?

(a) The earth is round.

(b) 2+3=5

(c) Do you speak English?

(d) 3-x=5

(e) Take two aspirins.

(f) The temperature on the surface of the planet Venus is 800° F.

(g) The sun will come out tomorrow.

Logical Connectives and Compound Statements

In logic, the letters p, q, r,…,denote **propositional variables** (命题变量) that can be replaced by statements. Statements or propositional variables can be combined by logical connectives to obtain **compound statements** (复合命题). The truth value of a compound statement depends only on the truth values of the statements being combined and on the types of connectives being used. If p is a statement, the **negation** (否定) of p is the statement not p, denoted by ~p.

From this definition, it follows that if p is true, then ~p is false, and if p is false, then ~p is true. The truth value of ~p relative to p is given in Table 2.1. Such a table, giving the truth values of a compound statement in terms of its component parts, is called a **truth table** (真值表).

If p and q are statements, the **conjunction** (合取) of p and q is the compound statement “p and q,” denoted by $p\wedge q$. The connective “and” is denoted by the symbol $\wedge$. The compound statement $p\wedge q$ is true when both p and q are true; otherwise, it is false. The truth values of $p\wedge q$ in terms of the truth values of p and q are given in the truth table 2.2.

Example 1: Form the conjunction of p and q for each of the following.

(a) p: It is snowing. q: I am cold.

Solution: the conjunction of p and q, i.e.,

$p \wedge q$: It is snowing and I am cold.

If p and q are statements, the **disjunction** (析取) of p and q is the compound statement “p or q”, denoted by $p \vee q$. The connective “or” is denoted by the symbol $\vee$. The compound statement $p \vee q$ is true if at least one of p or q is true; it is false when both p and q are false. The truth values of $p \vee q$ are given in the truth table shown in Table 2.3.

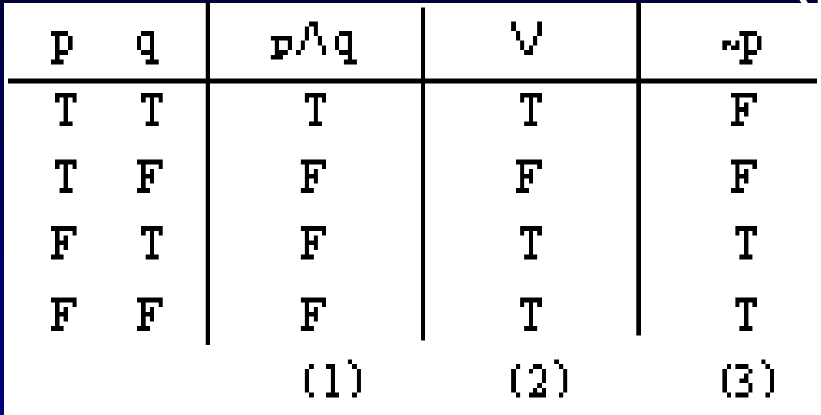
If a compound statement p contains n component statements, there will need to be 2^n rows in the truth table for p. Such a truth table may be systematically constructed in the following way.

Step 1: The first n columns of the table are labeled by the component propositional variables. Further columns are included for all intermediate combinations of the variables, reaching the highest point in a column for the full statement.

Step 2: Under each of the first n headings, we list the 2^n possible n-tuples of truth values for the n component statements.

Step 3: For each of the remaining columns, we compute, in sequence, the remaining truth values.

Make a truth table for the statement (p∧q)∨(~p).



p	q	p∧q	∨	~p
T	T	T	T	F
T	F	F	F	F
F	T	F	T	T
F	F	F	T	T
		(1)	(2)	(3)

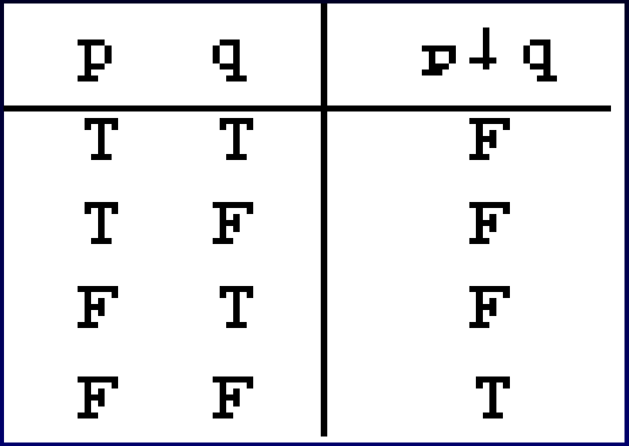
- Quantifiers (量词)

The **universal quantification** (全称量词) of a predicate P(x) is the statement “For all values of x, P(x) is true.” The universal quantification of P(x) is denoted ∀xP(x). The symbol ∀ is called the universal quantifier (全称量词).

The **existential quantification** (存在量词) of a predicate P(x) is the statement “There exists a value of x for which P(x) is true.” The existential quantification of P(x) is denoted $\exists x\, P(x)$. The symbol $\exists$ is called the existential quantifier.

Let p:$\forall x\, P(x)$. The negation of p is false when p is true, and true when p is false. For p to be false there must be at least one value of x for which P(x) is false. Thus, p is false if $\exists x \sim P(x)$ is true. On the other hand, if $\exists x \sim P(x)$ is false, then for every x,

~P(x) is false; that is, ∀x P(x) is true.

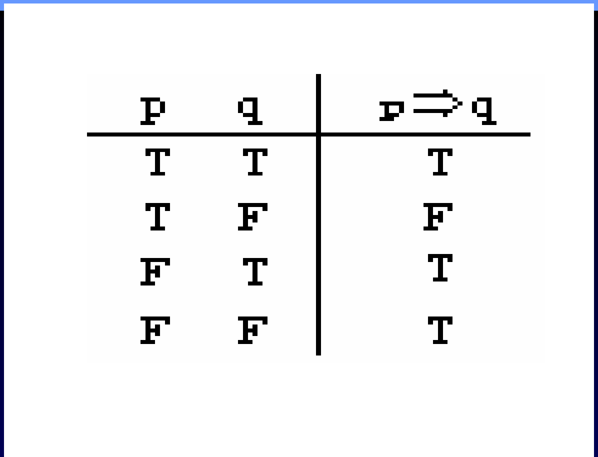


p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

2.2 CONDITIONAL STATEMENTS

If p and q are statements, the compound statement ‘if p then q,’ denoted $p \Rightarrow q$, is called a **conditional statement** (条件命题), or **implication** (蕴涵式). The statement p is called the **antecedent** (前件) or **hypothesis**, and the statement q is called the **consequent** (结论) or **conclusion**. The connective “if … then” is denoted by the symbol ⇒.

Table 2.4 describes the truth values of $p \Rightarrow q$ in terms of the truth of p and q. Notice that $p \Rightarrow q$ is considered false only if p is true and q is false. This fact is sometimes described by the statement: “A false hypothesis implies any conclusion.”



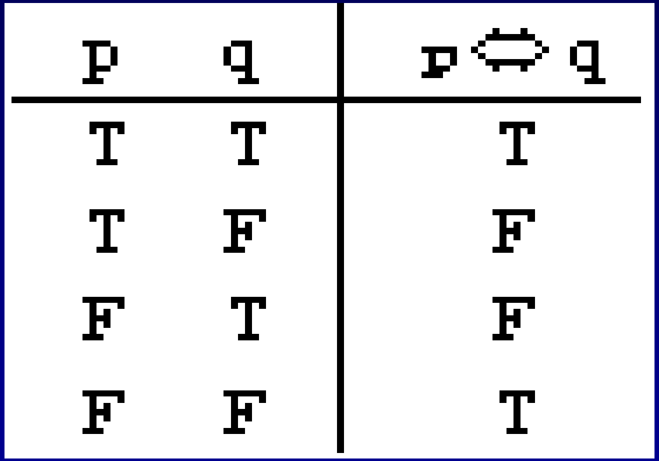
p	q	p⇒q
T	T	T
T	F	F
F	T	T
F	F	T

Table 2.4

If p ⇒ q is an implication, then the converse (逆) of p ⇒ q is the implication q ⇒ p, and the contrapositive (逆否) of p ⇒ q is the implication ~q ⇒ ~p.

If p and q are statements, the compound statement “p if and only if q”, denoted by p⇔q, is called an **equivalence** (等价式) or **biconditional**.

The connective “if and only if” is denoted by the symbol $\Leftrightarrow$. The truth values of $p \Leftrightarrow q$ are given in Table 2.5. $p \Leftrightarrow q$ is true only when both p and q are true or when both p and q are false.

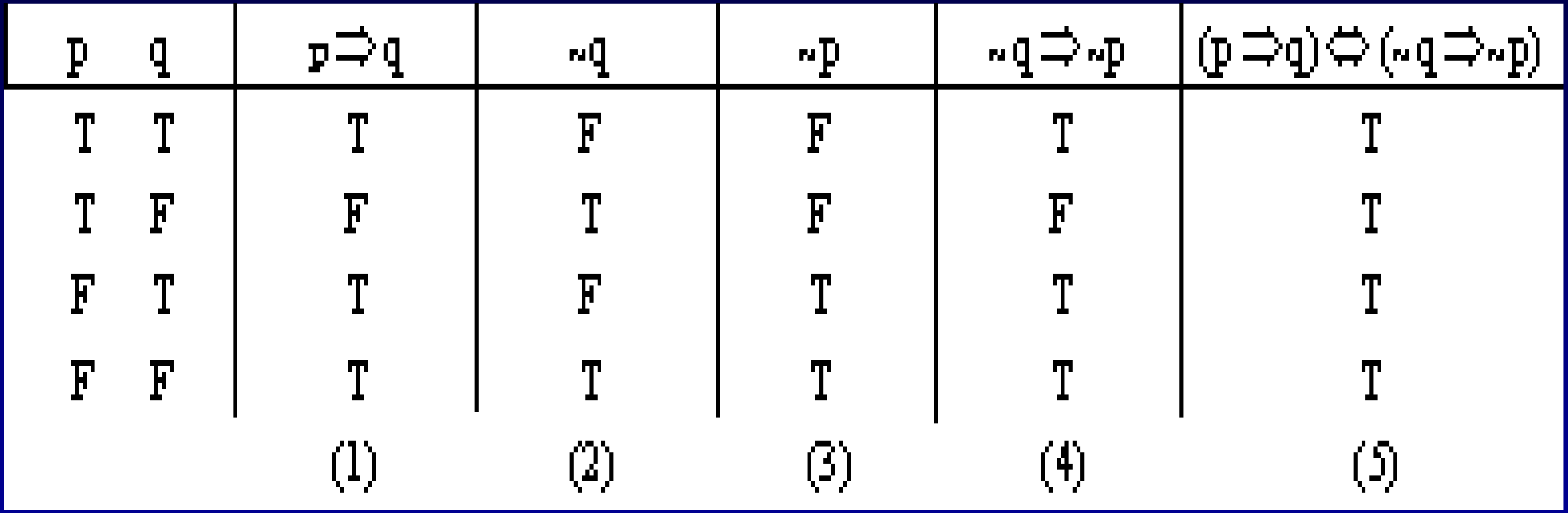


p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Table 2.5

Example 2 Compute the truth table of the statement

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



p	q	$p \Rightarrow q$	$\sim q$	$\sim p$	$\sim q \Rightarrow \sim p$	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T
		(1)	(2)	(3)	(4)	(5)

A statement that is true for all possible values of its propositional variables is called a **tautology** (永真式). A statement that is always false is called a **contradiction** or an **absurdity** (永假式), and a statement that can be either true or false, depending on the truth values of its propositional variables, is called a **contingency** (可满足式).

We say p and q are **logically equivalent**（逻辑等价）, or simply **equivalent**, if p⇔q is a tautology. We denote that p is equivalent to q by ‘p $\equiv$ q’.

Another way to use a truth table to determine if two statements are equivalent is to construct a column for each statement and compare these to see if they are identical.

The conditional statement $p \Rightarrow q$ is equivalent to $(\sim p) \vee q$, i.e., $(p \Rightarrow q) \equiv ((\sim p) \vee q)$.

Theorem 1: The operations for propositions have the following properties.

Commutative Properties

(1). $p \vee q \equiv q \vee p$

(2). $p \wedge q \equiv q \wedge p$

Associative Properties

(3). $p \vee (q \vee r) \equiv (p \vee q) \vee r$

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

Distributive Properties

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

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

Idempotent properties (幂等性)

(7). $p \vee p \equiv p$

(8). $p \wedge p \equiv p$

Properties of Negation

(9). $\sim(\sim p) \equiv p$

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

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

Here (10) and (11) are De Morgan's laws.

Theorem 2

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

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

(3) $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$

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

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

Theorem 3

(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) $((\forall x\, P(x)) \vee (\forall x\, Q(x))) \Rightarrow \forall x\, (P(x) \vee Q(x))$ is a tautology (永真式).

(7) $\exists x\, (P(x) \wedge Q(x)) \Rightarrow \exists\, x\, P(x) \wedge \exists\, x\, Q(x)$ is a tautology.

Theorem 4 Each of the following is a tautology.

(1) $(p \wedge q) \Rightarrow p$ (2) $(p \wedge q) \Rightarrow q$

(3) $p \Rightarrow (p \vee q)$ (4) $q \Rightarrow (p \vee q)$

(5) $\sim p \Rightarrow (p \Rightarrow q)$ (6) $\sim (p \Rightarrow q) \Rightarrow p$

(7) $(p \wedge (p \Rightarrow q)) \Rightarrow q$ (8) $(\sim p \wedge (p \vee q)) \Rightarrow q$

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

(10) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$

2.3 EQUIVALENT DEDUCTIONS (等值演算)

2.3.1 Statement Formulas and Classifications (命题公式与分类)

Definition 1.1 A statement formula is constructed by the following recursive steps:

1). a single statement or a propositional variable p, q, r, …, 0, 1 is a statement formula;

2). if A is a statement formula, then $\sim A$ is also statement formula;

3). if A and B are two statement formulas, then $(A\wedge B)$, $(A\vee B)$, $(A\Rightarrow B)$ and $(A\Leftrightarrow B)$ are statement formulas, too;

4). the strings constructed in preceding finite steps are statement formulas.

Definition 1.2 A layer of statement formula （命题公式层次） is constructed by the following recursive steps:

1). if A is a single statement or a propositional variable, p, q, r,…,p_i, q_i, r_i,…,0,1, then A is called the 0th layer formula;

2). the formula A is called the n+1th (n⩾0) formula， if A satisfies one of the following conditions：

① A=~B, where B is a nth formula;

② A=B∧C, where B is an ith formula and C is a jth formula, and n=max{i, j};

③ A= B∨C， where B and C are the same as ②

④ A= B⇒C， where B and C are the same as ②

⑤ A= B⇔C， where B and C are the same as ②

3). if the maximum layer of A is k, then A is called as a formula with layer k.

Definition 1.3 Let A be a statement formula, where p_1, p_2, …, p_n are all propositional variables of A. For any values (0 or 1) of p_1,p_2,…,p_n, A is called to be assigned an assignment or an explanation according to these values. If an assignment satisfies that the statement formula A is true (1), then this assignment is called a **true assignment** of A; if this assignment satisfies that the statement formula A is false (0), then this assignment is called a **false assignment** of A.

The statement formula A, which contains n propositional variables, has 2^n assignments.

For all 2^n assignments of statement formula A, we arrange these 2^n values as a table, and this table is called as a truth table (真值表) of A.

The following steps to compute the truth table of A:

1). For all propositional variables $p_1,p_2,\ldots,p_n$ of the statement formula A, find the 2^n assignments of A;

2). Write all layers of the sub-statement formula of A, according to the increasing order of the numbers of all layers;

3). For each assignment of A, compute the logical values of all layers, till compute the value of the last statement formula A.

2.3.2 Equivalent Deduction (等值演算)

Definition 1.4 For any two statement formulas A and B, if the equivalence ‘A $\Leftrightarrow$ B’ is a tautology (永真式), then A and B are equivalent, denote by “A $\equiv$ B”, where “ $\equiv$ ” is only a notation.

Definition 1.5 According to some equivalent formulas, we can deduce other equivalent formula by using these preceding formulas, till deducing the last formula, and we call this process as an equivalent deduction (等值演算).

There are some important equivalent formulas:

(1) $A \equiv \sim\sim A$ (双重否定律)

(2) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ (分配定律)

(3) $\sim(A \vee B) \equiv \sim A \wedge \sim B$ (德·摩根定律)

(4) $A \vee (A \wedge B) \equiv A$ (吸收律)

(5) $A \vee 0 \equiv A$ (同一律)

(6) $A \vee \sim A \equiv 1$ (排中律)

(7) $A \wedge \sim A \equiv 0$ (矛盾律)

(8) $A \Rightarrow B \equiv \sim A \vee B$ (蕴涵等值式)

(9) $A \Rightarrow B \equiv \sim B \Rightarrow \sim A$ (假言易位)

2.4 DUAL AND NORMAL FORM (对偶与范式)

Definition 1.6 In a statement formula A, only containing the connectives ‘~,∧ and ∨’, by substituting ∨ for ∧ and ∧ for ∨， and meanwhile A contains 0 or 1, by substituting 0 for 1 and 1 for 0 in the statement formula A, we obtain a new statement formula， and this new statement formula is called as a dual statement formula of A, denoted by A^*.

From the definition 1.6, $(A^*)^* = A$.

Theorem 1.1 Let A be a statement formula A^* as its dual statement formula and $p_1,p_2,\ldots,p_n$ all propositional variables in A and A^*. If A and A^* are treated as the n-functions, then

(1) $\sim A(p_1,p_2,\ldots,p_n) \equiv A^*(\sim p_1,\sim p_2,\ldots,\sim p_n)$;

(2) $A(\sim p_1,\sim p_2,\ldots,\sim p_n) \equiv \sim A^*(p_1,p_2,\ldots,p_n)$.

Theorem 1.2 （对偶定理）Let A and B be two statement formulas. If $A \equiv B$， then $A^* \equiv B^*$， where A^* and B^* are the dual statement formulas A and B, respectively, and vice versa.

Problem: For any given statement formula A, how to determine A to be a tautology (永真式), an absurdity (永假式), or a contingency (可满足式)?

We call this problem as a decision problem (判定性问题).

Definition 1.7 A disjunction (析取式), only containing finite propositional variables or their negations (否定)， is called a simple disjunction (简单析取式). And a conjunction (合取式), only containing finite propositional variables or their negations， is called a simple conjunction (简单合取式).

Theorem 1.3 (1) A simple disjunction is a tautology (永真式), if and only if this simple disjunction simultaneously contains a propositional variable and its negation；

(2) A simple conjunction is an absurdity (永假式), if and only if this simple conjunction simultaneously contains a propositional variable and its negation.

Definition 1.8 A **disjunction** (析取式), only containing finite simple conjunctions (简单合取式)，is called a **disjunction normal form** (析取范式) . And a **conjunction** (合取式), only containing finite simple disjunctions, is called a **conjunction normal form** (合取范式).

Example 3 (1) Let A_i be simple conjunctions, where j=1,2,…,n, then $A=A_1 \vee A_2 \vee \ldots \vee A_n$ is a disjunction.

(2) Let A_i be simple disjunction，where j=1,2,…,n, then $A=A_1 \wedge A_2 \wedge \ldots \wedge A_n$ is a conjunction normal form.

The dual statement formula of any disjunction is a conjunction; and the dual statement formula of any conjunction is a disjunction. And there are the following properties:

(1) a disjunction normal form (析取范式) is an absurdity (永假式), if and only if each simple conjunction is an absurdity;

(2) a conjunction normal form (合取范式) is a tautology (永真式), if and only if each simple disjunction is a tautology .

Theorem 1.4 （范式存在定理）Each statement formula A contains at least one disjunction normal form and a conjunction normal form, which of both are equivalent to A, but the expressions may not be sole.

The steps to compute a disjunction normal form (析取范式) or a conjunction normal form (合取范式):

(1) By using some equivalent formulas to reduce the other connectives except “~, ∧, ∨” in the statement formula A， i.e., the formula A or its equivalent formula only contains the connectives “~, ∧, ∨”；

(2) Reduce negative connectives or move negative connectives inside from outside；

(3) Utilize distributive properties： if computing disjunction normal forms, we should use distributive property by connective ∧ to connective ∨； if computing conjunction normal form , we should use distributive property by connective ∨ to connective ∧.

Remark: The disjunction normal form and the conjunction normal form of statement formula A may not be sole.

Example 4: Compute a disjunction normal form and a conjunction normal form of the following statement formula A.

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

Definition 1.9（极小项）In a simple conjunction consisting of n propositional variables, if each propositional variable and its negation do not exist simultaneously, but only one of both must exist once, and either the ith propositional variable or its negation must appear in the ith location from left to right (if the propositional variables have no lower labels, these propositional variables or their negations must arranged in lexical orders) , such a simple conjunction is called a **minimal item** (极小项).

For any minimal item, if we treat each propositional variable as 1 and its negation as 0, then this minimal item is corresponding to a binary Number, and it is also corresponding to a decimal number. This binary number is exactly the true assignment of such a minimal item, and this decimal number may described as lower label of a minimal item.

In general, a statement formula A consisting n propositional variable may produce 2^n minimal items, and denote them as $m_0, m_1, m_2, \ldots, m_{2^n-1}$.

Example 5: The 8 minimal items, consisting propositional variables p, q, and r, are corresponding to the following items

$\sim p \wedge \sim q \wedge \sim r$ —— 000 —— 0, as m_0;

$\sim p \wedge \sim q \wedge r$ —— 001 —— 1, as m_1;

$\sim p \wedge q \wedge \sim r$ —— 010 —— 2, as m_2;

$\sim p \wedge q \wedge r$ —— 011 —— 3, as m_3;

$p \wedge \sim q \wedge \sim r$ —— 100 —— 4, as m_4;

$p \wedge \sim q \wedge r$ —— 101 —— 5, as m_5;

$p \wedge q \wedge \sim r$ —— 110 —— 6, as m_6;

$p \wedge q \wedge r$ —— 111 —— 7, as m_7.

Definition 1.10 Let A be a statement formula consisting of n propositional variables. If all simple conjunctions (合取式) in the disjunction normal form (析取范式) of A are minimal items, then this disjunction is called as the main disjunction normal form (主析取范式) of the statement formula A.

Theorem 1.4 Any statement formula contains its main disjunction normal form, and this expression is sole.

The steps to compute the main disjunction normal form (主析取范式):

(1) Compute a disjunction normal form of statement formula A, say A’;

(2) If A’ contains a conjunction B which has neither statement variable p_i nor its negation $\sim p_i$, then express B as the following form:

$$B \equiv B \wedge 1 \equiv B \wedge (p_i \vee \sim p_i) \equiv (B \wedge p_i) \vee (B \wedge \sim p_i)$$

(3) Delete the absurdities (矛盾式), some propositional variables and minimal items which appear repeatedly;

(4) Arrange all minimal items left in increasing orders of labels, and represent them as $\sum(*,*,\ldots,*)$.

Some uses of main disjunction normal form (主析取范式):

(1). Determine whether two statement formulas are equivalent: if $A \Leftrightarrow B$， then they have the same main disjunction normal forms, and vice versa.

(2). Determine the types of statement formulas: if A is a statement formula consisting of n propositional variables, then

(a) A is a tautology (永真式), if and only if the main disjunction normal form of A contains exactly 2^n minimal items;

(b) A is an absurdity (永假式), if and only if the main disjunction normal form of A contains no minimal items;

(c) A is a contingency (可满足式), if and only if the main disjunction normal form of A contains at least one minimal item;

(3). Compute the true assignments and false assignments of statement formulas.

Definition 1.11（极大项）In a simple disjunction consisting of n propositional variables, if each propositional variable and its negation do not exist simultaneously, but only one of both must exist once, and either the i^{th} propositional variable or its negation must appear in the i^{th} location from left to right (if the statement variables have no lower labels, these propositional variables must arranged in lexical orders) , such a simple disjunction is called a **maximal item** (极大项).

For any maximal item, if we treat each propositional variable as 1 and its negation as 0, then this maximal item is corresponding to a binary number and it is also corresponding to a decimal number. This binary number is exactly the false assignment of such a maximal item, and this decimal number may described as lower label of a maximal item.

In general, a statement formula A consisting n propositional variables may produce 2^n maximal items, and denote them as $M_0, M_1, M_2, \ldots, M_{2^n-1}$.

Example 5: The 8 maximal items, consisting 3 propositional variables p, q, and r, are corresponding to the following items

$p \vee q \vee r$ —— 000 —— 0， as M_0

$p \vee q \vee \sim r$ —— 001 —— 1， as M_1

$p \vee \sim q \vee r$ —— 010 —— 2， as M_2

$p \vee \sim q \vee \sim r$ —— 011 —— 3， as M_3

$\sim p \vee q \vee r$ —— 100 —— 4， as M_4

$\sim p \vee q \vee \sim r$ —— 101 —— 5， as M_5

$\sim p \vee \sim q \vee r$ —— 110 —— 6， as M_6

$\sim p \vee \sim q \vee \sim r$ —— 111 —— 7， as M_7

Definition 1.12 Let A be a statement formula consisting of n propositional variables. If all simple disjunctions (析取式) in the conjunction normal form (合取范式) of A are maximal items, then this conjunction normal form is called as the main conjunction normal form (合取范式) of the statement formula A.

Theorem 1.5 Any statement formula contains its main conjunction normal form, and this expression is sole.

The steps to compute the main conjunction normal form (主合取范式):

(1) Compute a conjunction normal form of statement formula A, say A’;

(2) If A’ contains a disjunction B which has neither propositional variable p_i nor its negation $\sim p_i$, then express B as the following form:

$$B \equiv B \vee 0 \equiv B \vee (p_i \wedge \sim p_i) \equiv (B \vee p_i) \wedge (B \vee \sim p_i)$$

(3) Delete the tautologies (永真式), some propositional variables and maximal items which appear repeatedly;

(4) Arrange all maximal items left in increasing orders of labels, and represent them as $\prod(*,*,\ldots,*)$.

Some uses of main conjunction normal form (主合取范式):

(1). Determine whether two statement formulas are equivalent: if $A \Leftrightarrow B$， then they have the same main conjunction normal forms, and vice versa.

(2). Determine the types of statement formulas: if A is a statement formula consisting of n propositional variables, then

(a) A is a tautology (永真式), if and only if the main conjunction normal form of A contains no maximal items;

(b) A is an absurdity (永假式), if and only if the main conjunction normal form of A contains exactly 2^n maximal items;

(c) A is a contingency (可满足式), if and only if the main conjunction normal form of A contains at most 2^n-1 maximal item;

(3). Compute the true assignments and false assignments of statement formulas.

In fact, whenever we compute the main disjunction normal form (主析取范式) of any statement formula A, we can directly compute its main conjunction normal form (主合取范式) from its main disjunction normal form, and vice versa.

Any minimal item and its maximal item satisfy the following properties:

$$\sim m_i \equiv M_i \qquad \sim M_i \equiv m_i$$

If statement formula A, consisting of n propositional variables, has its main conjunction normal form which consists k minimal items $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$, then the main disjunction normal form of its dual ~A has exactly 2^n-k minimal items $m_{j_1}, m_{j_2}, \ldots, m_{j_{2^n-k}}$, thus we have

$$\begin{aligned}
\sim A &\equiv m_{j_1} \vee m_{j_2} \vee \ldots \vee m_{j_{2^n-1}} \\
A &\equiv \sim\sim A \equiv \sim (m_{j_1} \vee m_{j_2} \vee \ldots \vee m_{j_{2^n-1}}) \\
&\equiv \sim m_{j_1} \wedge \sim m_{j_2} \wedge \ldots \wedge \sim m_{j_{2^n-1}} \\
&\equiv M_{j_1} \wedge M_{j_2} \wedge \ldots \wedge M_{j_{2^n-1}} .
\end{aligned}$$

For any statement formula A, the steps to compute the main conjunction normal form from the main disjunction normal form of A are the following ways:

(1)Compute all minimal items of the main disjunction normal form of A, say $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$;

(2) Present all other minimal items different from the minimal items in (1), say $m_{j_1}, m_{j_2}, \ldots, m_{j_{2^n-k}}$, i.e.,

$$\{m_{j_1}, m_{j_2}, \ldots, m_{j_{2^n-k}}\} = \{m_0, m_1, m_2, \ldots, m_{2^n-1}\} - \{m_{i_1}, m_{i_2}, \ldots, m_{i_k}\}$$

(3) Describe the maximal items $M_{j_1}, M_{j_2}, \ldots, M_{j_{2^n-k}}$, which is exactly the main conjunction normal of the statement formula A.

Example 6: Let A be a statement formula consisting of 3 propositional variables, whose main disjunction normal form is the following version:

$$A \equiv m_0 \vee m_1 \vee m_5 \vee m_7 \equiv \sum(0,1,5,7);$$

Then the main conjunction normal form of A is the following version:

$$A \equiv M_2 \wedge M_3 \wedge M_4 \wedge M_6 \equiv \prod(2,3,4,6).$$

2.5 METHODS OF PROOF

If an implication $p \Rightarrow q$ is a tautology, where p and q may be compound statements involving any number of propositional variables, we say that q **logically follows** from p. Suppose that an implication of the form $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$ is a tautology. In this case, we say that q logically follows from $p_1, p_2, \ldots, p_n$. When q logically follows from $p_1, p_2, \ldots, p_n$, we write.

$$\begin{array}{rl} & p_1 \\ & p_2 \\ & \ldots \\ & \underline{p_n} \\ \therefore & q \end{array}$$

This means if we know that p_1 is true, p_2 is true, …,and p_n is true, then we know q is true.

All mathematical theorems are composed of implications of the type

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

The p_i's are called the **hypotheses** or **premises**, and q is called the **conclusion**.

A very important rule of inference is

$$\begin{array}{l} p \\ \underline{p \Rightarrow q} \\ \therefore q. \end{array}$$

i.e., p is true, and $p \Rightarrow q$ is true, then q is true.

An important proof technique, called an **indirect method** (间接法) of proof, follows from the tautology $(p \Rightarrow q) \Leftrightarrow ((\sim q) \Rightarrow (\sim p))$.

Thus to prove $p \Rightarrow q$ indirectly, we assume q is false (the statement ~q) and show that p is then false (the statement ~p).

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

Another important proof technique is **proof by contradiction**(归谬法或反证法). This method is based on the tautology $((p \Rightarrow q) \wedge (\sim q)) \Rightarrow (\sim p)$.

$$\begin{array}{ll} & p \Rightarrow q \\ & \sim q \\ \hline \therefore & \sim p \end{array}$$

Suppose we wish to show that a statement q logically follows from statements $p_1, p_2, \ldots, p_n$. Assume that ~q is true (that is, q is false) as an extra hypothesis, and that $p_1, p_2, \ldots, p_n$ are also true. If this enlarged hypothesis $p_1 \wedge p_2 \wedge \ldots \wedge p_n \wedge$ (~q) implies a contradiction, then at least one of the statements $p_1, p_2, \ldots, p_n$, ~q must be false. This means that if all the p_i's are true, then ~q must be false, so q must be true.

Example 7: Prove there is no rational number p/q whose square is 2, i.e., show that $\sqrt{2}$ (the arithmetic square root of 2) is irrational.

Solution: This statement is a good candidate for proof by contradiction, because we could not check all possible rational numbers to demonstrate that none had a square equal to 2. Assume $(p/q)^2=2$ for some integers p and q, which have no common factors. If the original choice of p/q is not in lowest terms, we can replace it with its equivalent lowest-term form. Then $p^2=2q^2$, so p^2 is even. This implies p is even, since the square of an odd number is odd. Thus, $p=2n$ for some integer n. We see that $2q^2=p^2=(2n)^2=4n^2$, so $q^2=2n^2$. Thus q^2 is even, and so q is even. We now have that both p and q are even, and therefore have a common factor 2. This is a contradiction to the assumption. Thus the assumption must be false.

In order to prove a theorem of the (typical) form $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$, we begin with the hypothesis $p_1, p_2, \ldots, p_n$ and show that the some result r_1 logically follows. Then, using $p_1, p_2, \ldots, p_n, r_1$, we show that some other statement r_2 logically follows. We continue this process, producing intermediate statements $r_1,r_2,\ldots, r_k$, called **steps in the proof**, until we can finally shows that the conclusion q logically follows from $p_1,p_2,\ldots, p_n$, r_1, $r_2,\ldots, r_k$.

Proof method of additional hypothesis (附加前提证明法)

If the conclusion which will be proved is in the version of implication (蕴涵式), such as：

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow (A \Rightarrow B) \tag{a}$$

By utilizing equivalent deductions (等值演算), we obtain the following forms:

$$\begin{aligned}
\text{(a)} \quad & \equiv \sim (A_1 \wedge A_2 \wedge \cdots \wedge A_n) \vee (A \Rightarrow B) \\
& \equiv \sim (A_1 \wedge A_2 \wedge \cdots \wedge A_n) \vee (\sim A \vee B) \\
& \equiv \sim (A_1 \wedge A_2 \wedge \cdots \wedge A_n) \vee (\sim A) \vee B \\
& \equiv \sim (A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge A) \vee B \\
& \equiv (A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge A) \Rightarrow B \qquad \text{(b)}
\end{aligned}$$

By the preceding method, the hypothesis A in the conclusion becomes a hypothesis in the whole statement formula. If the formula (a) is a tautology (永真式), then the formula (b) also becomes a tautology, which shows that this process of deductive method is **true**.

By treating the hypotheses in the conclusion as the hypotheses in the whole statement formula, we call this process of deductive method as **a proof method of additional hypothesis** (附加前提的证明法), meanwhile the hypothesis A is called as an additional hypothesis (附加前提) .

2.6 MATHEMATICAL INDUCTION

Suppose the statement to be proved can be put in the form $\forall n \geq n_0 P(n)$, where n_0 is some fixed integer. Suppose that (a) $P(n_0)$ is true and (b) If P(k) is true for some $k \geqslant n_0$, then P(k+1) must also be true. Then P(n) is true for all $n \geqslant n_0$. This result is called the **principle of mathematical induction**. Thus to prove the truth of a statement $\forall n \geq n_0 P(n)$, using the principle of mathematical induction, we must begin by proving directly that the first proposition $P(n_0)$ is true. This is called the **basis step** of the induction.

Then we must prove that P(k) $\Rightarrow$ P(k+1) is a tautology for any choice of k$\geqslant$n$_0$. This step is called the **induction step**.

Example Show, by mathematical induction, that for all n$\geqslant$1,

$$1+2+3+\ldots+n=\frac{n(n+1)}{2}.$$

Solution: Let P(n) be the predicate

$$1+2+3+\ldots+n=\frac{n(n+1)}{2}.$$

In this example, n$_0$=1.

Basis Step: We must first show that P(1) is true.

P(1) is the statement $1=\frac{1(1+1)}{2}$.

which is clearly true.

Induction Step: We must now show that for k⩾1, if P(k) is true, then P(k+1) must also be true. We assume that for some fixed k⩾1,

$$1+2+3+\ldots+k=\frac{k(k+1)}{2}. \qquad (1)$$

We now wish to show the truth of P(k+1):

$$1+2+3+\ldots+(k+1)=\frac{(k+1)((k+1)+1)}{2}.$$

The left-hand side of P(k+1) can be written as

$$1+2+3+\ldots+k+(k+1)$$

and we have

$$1+2+3+...+k+(k+1)$$

$$=\frac{k(k+1)}{2}+(k+1) \quad \text{using (1) to replace } 1+2+3+...+k$$

$$=(\mathrm{k}+1)\left[\frac{\mathrm{k}}{2}+1\right] \quad \text{factoring}$$

$$=\frac{(k+1)(k+2)}{2}$$

$$=\frac{(k+1)((k+1)+1)}{2} \quad \text{the right-hand side of P(k+1)}$$

Thus, we have shown the left-hand side of P(k+1) equals the right-hand side of P(k+1). By the principle of mathematical induction, it follows that

P(n) is true for alll n⩾1.

Example Let A_1, A_2, A_3,…, A_n be any n sets. We show by mathematical induction that

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}$$

(This is an extended version of one of De Morgan’s laws.)

Solution: Let P(n) be the predicate that the equality holds for any n sets. We prove by mathematical induction that for all n⩾1, P(n) is true.

Basis Step: P(1) is the statement $\overline{A_1} = \overline{A_1}$, which is obviously true.

Induction Step: We use P(k) to show P(k+1). The left-hand side of P(k+1) is

$$\left(\bigcup_{i=1}^{k+1} A_i\right) = \overline{A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1}}$$

$$= \overline{\left(A_1 \cup A_2 \cup \ldots \cup A_k\right) \cup A_{k+1}} \quad \text{associative property of } \cup$$

$$= \overline{\left(A_1 \cup A_2 \cup \ldots \cup A_k\right)} \cap \overline{A_{k+1}} \quad \text{by De Morgan's law for two sets}$$

$$= \left(\bigcap_{i=1}^{k} \overline{A_i}\right) \cap \overline{A_{k+1}} \quad \text{using P(k)}$$

$$= \bigcap_{i=1}^{k+1} \overline{A_i} \quad \text{right-hand side of P(k+1)}$$

Thus, the implication P(k) $\Rightarrow$ P(k+1) is a tautology, and by the principle of mathematical induction P(n) is true for all n$\geqslant$1.

Example Consider the following function given in pseudocode.

```
FUNCTION SQ(A)
1. $C \leftarrow 0$
2. $D \leftarrow 0$
3. WHILE ($D \neq A$)
   a. $C \leftarrow C+A$
   b. $D \leftarrow D+1$
4. RETURN (C)
END OF FUNCTION SQ
```

The name of the function, SQ, suggests that it computes the square of A. Step 3b shows A must be a positive integer if the looping is to end. A few trials with particular values of A will provide evidence that the function does carry out this task. However, suppose we now want to prove that SQ always computes the square of the positive integer A, no matter how large A might be. We shall give a proof by mathematical induction.

For each integer $n \geqslant 0$, let C_n and D_n be the values of the variables C and D, respectively, after passing through the WHILE loop n times. In particular, C_0 and D_0 represent the values of the variables before looping starts. Let P(n) be the predicate $C_n = A \times D_n$. We shall prove by induction that $\forall n \geq 0\, P(n)$ is true. Here n_0 is 0.

Basis Step: P(0) is the statement $C_0=A\times D_0$, which is true since the value of both C and D is zero "after" zero passes through the **WHILE** loop.

Induction Step: We must now use

$$P(k): C_k=A\times D_k \qquad (2)$$

to show that $P(k+1): C_{k+1}=A\times D_{k+1}$. After a pass through the loop, C is increased by A, and D is increased by 1, so $C_{k+1}=C_k+A$ and $D_{k+1}=D_k+1$.

left-hand side of P(k+1):

$C_{k+1}=C_k+A$

$=A\times D_k+A$ using (2) to replace C_k

$=A\times (D_k+1)$ factoring

$=A\times D_{k+1}$ right-hand side of P(k+1).

By the principle of mathematical induction, it follows that as long as looping occurs, $C_n=A\times D_n$. The loop must terminate. (Why?) When the loop terminates, D=A, so C=A×A, or A^2, and this is the value returned by the function SQ.

Use the technique of Example 5 to prove that the pseudocode program given in Section 1.4 does compute the greatest common divisor of two positive integers.

Solution: Here is the pseudocode given earlier.

```
FUNCTION GCD(X,Y)
1. WHILE ($X \neq Y$)
   a. IF($X>Y$) THEN
      1. $X \leftarrow X-Y$
   b. ELSE
      1. $Y \leftarrow Y-X$
2. RETURN (X)
END OF FUNCTION GCD
```

We claim that if X and Y are positive integers, then GCD returns GCD(X,Y). To prove this, let X_n and Y_n be the values of X and Y after $n \geqslant 0$ passes through the WHILE loop. We claim that P(n): $GCD(X_n,Y_n)=GCD(X,Y)$ is true for all $n \geqslant 0$, and we prove this by mathematical induction. Here n_0 is 0.

Basis Step: $X_0=X$, $Y_0=Y$, since these are the values of the variables before looping begins; thus P(0) is the statement $GCD(X_0,Y_0)=GCD(X,Y)$, which is true.

Induction Step: Consider the left-hand side of P(k+1), that is, $GCD(X_{k+1},Y_{k+1})$. After the k+1 pass through the loop, **either** $X_{k+1}=X_k$ and $Y_{k+1}=Y_k-X_k$ **or** $X_{k+1}=X_k-Y_k$ and $Y_{k+1}=Y_k$. Then if P(k): $GDC(X_k,Y_k)=GCD(X,Y)$ is true, we have, by Theorem 5, Section 1.4, that $GCD(X_{k+1},Y_{k+1})=GCD(X_k,Y_k)=GCD(X,Y)$. Thus, by the principle of mathematical induction, P(n) is true for all $n \geqslant 0$. The exit condition for the loop is $X_n=Y_n$ and we have $GCD(X_n,Y_n)=X_n$. Hence the function always returns the value GCD(X,Y).

- Strong induction

In the **strong form of mathematical induction**, or strong induction, the induction step is to show that

$P(n_0) \wedge P(n_0+1) \wedge P(n_0+2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$

is a tautology.

Example Prove that every positive integer n >1 can be written uniquely as $p_1^{a1} p_2^{a2} \ldots p_s^{as}$, where the p_i are primes and $p_1<p_2<\ldots<p_s$.

(See Theorem 3, Section1.4)

Proof (by strong induction)

Basis Step: Here n_0 is 2. P(2) is clearly true, since 2 is prime.

Induction Step: We use P(2), P(3),…, P(k) to show P(k+1): k+1 can be written uniquely as $p_1^{a1}p_2^{a2}\ldots p_s^{as}$, where the p_i s are primes and $p_1<p_2<\ldots<p_s$. There are two cases to consider. If k+1 is a prime, then P(k+1) is true. If k+1 is not prime, then k+1=lm, $2\leqslant l\leqslant k, 2\leqslant m\leqslant k$. Using P(l) and P(m),we have $k+1=lm=q_1^{b1}q_2^{b2}\ldots q_t^{bt}r_1^{c1}r_2^{c2}\ldots r_u^{cu}$ $=p_1^{a1}p_2^{a2}\ldots p_s^{as}$, where each $p_i=q_j$ or r_k, $p_1<p_2<\ldots<p_s$, and if $q_j=r_k=p_i$, then $a_i=b_j+c_k$, otherwise $p_i=q_j$ and $a_i=b_j$ or $p_i=r_k$ and $a_i=c_k$. Since the factorization of l and m are unique, so is the factorization of k+1.

The end !