Discrete Mathematics 离散数学及其应用

1 The Foundations: Logic and Proofs

1.1 Propositional Logic

具有确切真值的陈述句称为命题（proposition）

TABLE 1 The Truth Table for the Negation of a Proposition.

p	$\neg p$
T	F
F	T

TABLE 2 The Truth Table for the Conjunction of Two Propositions.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

TABLE 3 The Truth Table for the Disjunction of Two Propositions.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

TABLE 4 The Truth Table for the Exclusive Or of Two Propositions.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

TABLE 5 The Truth Table for the Conditional Statement $p \rightarrow q$.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

TABLE 6 The Truth Table for the Biconditional $p \leftrightarrow q$.

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

TABLE 7 The Truth Table of $(p \vee \neg q) \rightarrow (p \wedge q)$.

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

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

- 复合命题有组成，则有2的n次方行
- n个命题变量可以构造 2^{2^n} 不同 (非等价) 命题propositions

TABLE 8
Precedence of Logical Operators.

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

TABLE 9 Table for the Bit Operators *OR*, *AND*, and *XOR*.

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

***p* $\vee$ *q* (*disjunction of p and q*):** the proposition "*p or q*," which is true if and only if at least one of p and q is true

p $\wedge$ q (conjunction of p and q): the proposition "*p and q*," which is true if and only if both p and q are true

p $\oplus$ q (exclusive or of p and q): the proposition "*p XOR q*," which is true when exactly one of p and q is true

***p* $\rightarrow$ *q* (p *implies q*):** the proposition "if *p*, then *q*," which is false if and only if p is true and q is false

1.2 Applications of Propositional Logic

1.3 Propositional Equivalences

TABLE 1 Examples of a Tautology and a Contradiction.

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

TABLE 8 Logical Equivalences Involving Biconditional Statements.

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

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

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

TABLE 6 Logical Equivalences.

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

TABLE 7 Logical Equivalences Involving Conditional Statements.

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

$p \rightarrow q \equiv \neg q \rightarrow \neg p$

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

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

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

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

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

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

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

A **minterm** is a conjunctive of literals in which each variable is represented exactly once. For example, If a formula has the variables p, q, r, then p∧¬q∧ r is a minterm, but p∧¬q and p∧¬p∧r are not.

If a formula is expressed as a disjunction of minterms, it is said to be in **full disjunctive normal form**.

For example, $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$，括号间用析取∨连接

Any formula A is tautologically equivalent to a formula in full disjunctive normal form

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

Sheffer stroke |:

$p|q \equiv \neg(p \wedge q)$ **NAND**

其他逻辑运算符

Peirce arrow ↓:

$p \downarrow q \equiv \neg(p \vee q)$ **NOR**

1.4 Predicates and Quantifiers

Disjunctive normal form 析取范式：取各命题变量或其否定的合取式 ∧ 的析取式∨，其中每一组合取试对应一组真值组合，从而使该复合命题为真。 eg, (a∧b)∨(c∧d)∨(e∧f)

∃：existential quantifier

∃∀ 有最高级优先权

TABLE 1 Quantifiers.

Statement	*When True?*	*When False?*
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

TABLE 2 De Morgan's Laws for Quantifiers.

Negation	*Equivalent Statement*	*When Is Negation True?*	*When False?*
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

Uniqueness

∃!x, P(x) == **one and only one x** in the universe of the discourse

More logical equivalences

$$\forall x(A(x) \wedge B(x)) \equiv \forall x A(x) \wedge \forall B(x)$$

$$\exists x(A(x) \vee B(x)) \equiv \exists x A(x) \vee \exists B(x)$$

$$\forall x(A(x) \vee B(x)) \not\equiv \forall x A(x) \vee \forall B(x)$$

$$\exists x(A(x) \wedge B(x)) \not\equiv \exists x A(x) \wedge \exists B(x)$$

$$\forall x A(x) \vee \forall x B(x) \rightarrow \forall x(A(x) \vee B(x))$$

$$\exists x(A(x) \wedge B(x)) \rightarrow \exists x A(x) \wedge \exists x B(x)$$

$$\forall x(B \rightarrow A(x)) \equiv B \rightarrow \forall x A(x) \quad \forall x A(x) \vee P \equiv \forall x(A(x) \vee P)$$

$$\exists x(B \rightarrow A(x)) \equiv B \rightarrow \exists x A(x) \quad \forall x A(x) \wedge P \equiv \forall x(A(x) \wedge P)$$

$$\forall x(A(x) \rightarrow B) \equiv \exists x A(x) \rightarrow B \quad \exists x A(x) \vee P \equiv \exists x(A(x) \vee P)$$

$$\exists x(A(x) \rightarrow B) \equiv \forall x A(x) \rightarrow B \quad \exists x A(x) \wedge P \equiv \exists x(A(x) \wedge P)$$

1.5 Nested Quantifiers

TABLE 1 Quantifications of Two Variables.

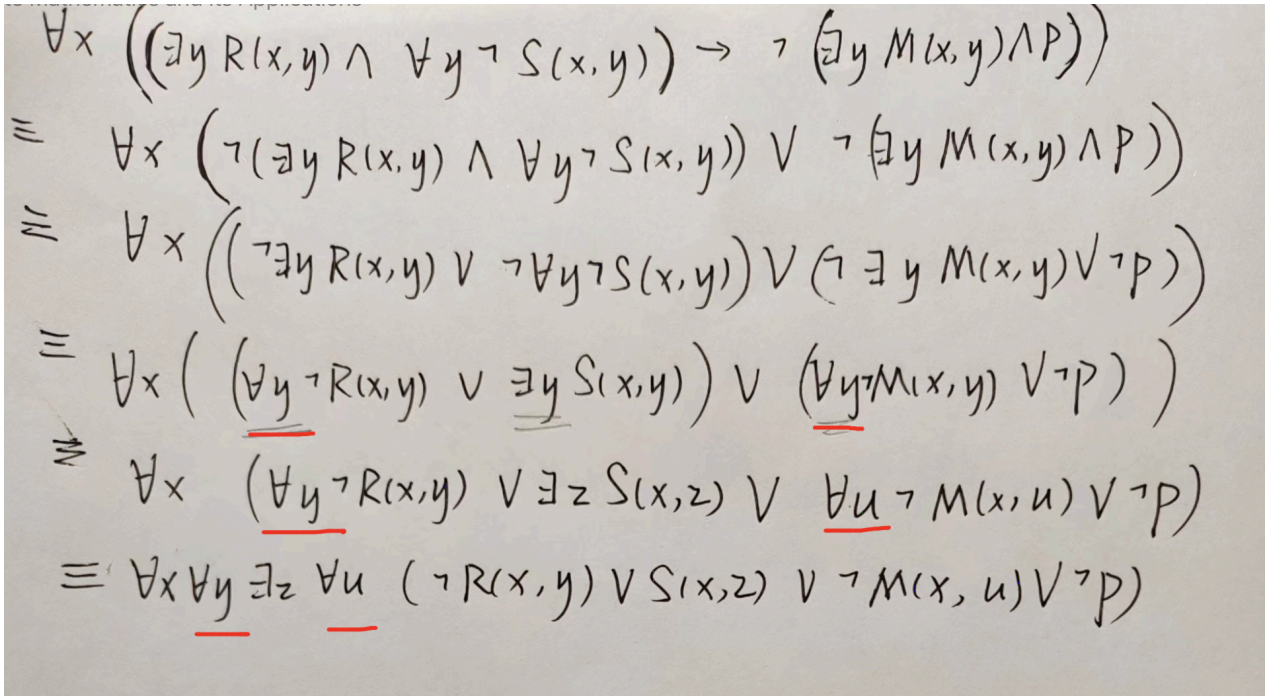
Statement	*When True?*	*When False?*
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Prenex normal form 前束范式

How to obtain prenex normal form?
1. Eliminate all occurrences of → and ↔ from the formula in question.
2. Move all negations inward such that, in the end, negation only appear as part of literals.
3. Standardize the variables a part (when necessary).
4. The prenex normal form can now be obtained by moving all quantifiers to the front of the formula.

Example

$$\forall x((\exists y R(x,y) \wedge \forall y \neg S(x,y)) \rightarrow \neg(\exists y M(x,y) \wedge P))$$



第二个任意y可以不用换成任意u，直接把任意y提到前边就OK

1.6 Rules of Inference

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*	名 称
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens	假言推理
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens	取拒式
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism	假言三段论
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism	析取三段论
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition	附加律
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification	化简律
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction	合取律
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution	消解律

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization

Example

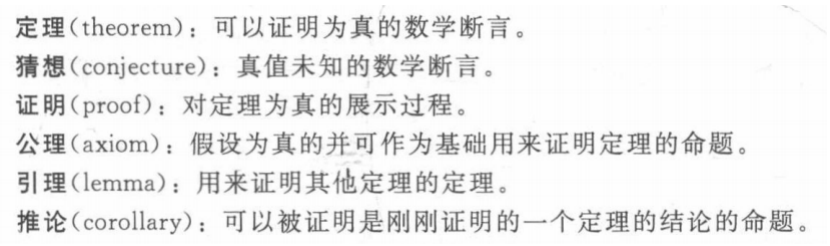
Show that the premises “A student in this class has not read the book,” and “Everyone in this class passed the first exam” imply the conclusion “Someone who passed the first exam has not read the book.

Solution: Let C(x) be “x is in this class,” B(x) be “x has read the book,” and P(x) be “x passedthe first exam.” The premises are $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \to P(x))$. The conclusion is $\exists x(P(x) \wedge \neg B(x))$. These steps can be used to establish the conclusion from

the premises.
Step Reason:

1.	$\exists x(C(x) \wedge \neg B(x))$	Premise
2.	$C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3.	$C(a)$	Simplification from (2)
4.	$\forall x(C(x) \rightarrow P(x))$	Premise
5.	$C(a) \rightarrow P(a)$	Universal instantiation from (4)
6.	$P(a)$	Modus ponens from (3) and (5)
7.	$\neg B(a)$	Simplification from (2)
8.	$P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9.	$\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

1.7 Introduction to Proofs


定理(theorem)：可以证明为真的数学断言。
猜想(conjecture)：真值未知的数学断言。
证明(proof)：对定理为真的展示过程。
公理(axiom)：假设为真的并可作为基础用来证明定理的命题。
引理(lemma)：用来证明其他定理的定理。
推论(corollary)：可以被证明是刚刚证明的一个定理的结论的命题。

1.8 Proof Methods and Strategy

proof by contraposition 反证法**:** a proof that $p \rightarrow q$ *is true that proceeds by showing that p must be false when q is false*
proof by contradiction *归谬法***:** *a proof that p is true based on the truth of the conditional statement* $\neg p \rightarrow q$, where q is a contradiction
exhaustive proof 穷举法**:** a proof that establishes a result by checking a list of all possible cases
proof by cases: a proof broken into separate cases, where these cases cover all possibilities
counterexample 反例

2 Basic Structures: Sets, Functions, Sequences, Sums, and Matrices

2.1 Sets

N = {0, 1, 2, 3, ...}, the set of all **natural numbers**
Z = {..., −2, −1, 0, 1, 2, ...}, *the set of all* ***integers***
Z+ = {1, 2, 3, ...}, *the set of all* ***positive integers***
Q = {p/q | p ∈ **Z**, q ∈ **Z**, *and* q ≠ 0}, *the set of all* ***rational numbers***
R, the set of all **real numbers**
R+, the set of all **positive real numbers**
C, the set of all **complex numbers**

$A \subseteq B$: $\forall x(x \in A \rightarrow x \in B)$

For every set S, $\emptyset \subseteq S$

S = T (set equality): S and T have the same elements

S ⊆ T (S is a subset子集 of T): every element of S is also an element of T

S ⊂ T (S is a **proper subset真子集** of T): S is a subset of T and S ≠ T

finite set 有限集: a set with n elements, where n is a nonnegative integer

infinite set 无限集: a set that is not finite

|S| (the cardinality of *S*): the number of elements in *S*

Power set P(S)：S的所有子集

Definition 4 Let S be a set. If there are exactly n distinct elements in S where n is a nonnegative integer, we say that S is a *finite set* and that n is the *cardinality* of S. The cardinality of S is denoted by $|S|$.

Definition 6 Given a set S, the *power set* of S is the set of all subsets of the set S. The power set of S is denoted by $\mathcal{P}(S)$.

|S|=n implies |P(S)| = 2^n
S is finite and so is P(S).

$$\begin{cases} x \in P(S) \Rightarrow x \subseteq S \\ x \in S \Rightarrow \{x\} \in P(S) \\ S \in P(S) \end{cases}$$

$A \subseteq B \Rightarrow P(A) \subseteq P(B)$

〖Example 6〗 Show that $P(A) \in P(B) \Rightarrow A \in B$ **?**

Proof:

$$P(A) \in P(B) \Rightarrow P(A) \subseteq B$$

$$A \in P(A) \subseteq B \Rightarrow A \in B$$

Definition 8 Let A and B be sets. The *Cartesian product* of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Hence,

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Example 1

What is the ***Cartesian product*** 笛卡尔积 of $A = \{1, 2\}$ *and* $B = \{a, b, c\}$*?*
Solution: *The Cartesian product* $A \times B$ *is*

$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$.

But the Cartesian product $B \times A$ *is*

$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$. *This is not equal to* $A \times B$.

Example 2

What is the Cartesian product $A \times B \times C$, where $A = \{0, 1\}$, $B = \{1, 2\}$, *and* $C = \{0, 1, 2\}$*?*
Solution: *The Cartesian product* $A \times B \times C$ *consists of all ordered triples* (a, b, c)*, where* $a \in A$, $b \in B$, and $c \in C$.
Hence, $A \times B \times C = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2)\}$.

Note that when A, B, and C *are sets,* $(A \times B) \times C$ is not the same as $A \times B \times C$

The elements of $A \times B \times C$ consist of 3-tuples (a, b, c), where $a \in A$, $b \in B$, and $c \in C$, whereas the elements of $(A \times B) \times C$ look like $((a, b), c)$—ordered pairs, the first coordinate of which is again an ordered pair.

Example 3

Suppose that $A = \{1, 2\}$.
It follows that $A2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$
and $A3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$.

2.2 Set Operations

容斥原理：$|A \cup B| = |A| + |B| - |A \cap B|$

Difference $A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \overline{B}$ A非B的部分

Symmetric $A \oplus B = (A \cup B) - (A \cap B)$ A,B不重合的部分

TABLE 1 Set Identities.

Identity	*Name*	名　称
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws	恒等律
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws	支配律
$A \cup A = A$ $A \cap A = A$	Idempotent laws	幂等律
$\overline{(\overline{A})} = A$	Complementation law	补律
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws	交换律
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws	结合律
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws	分配律
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws	德·摩根律
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws	吸收律
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws	互补律

Example

Use set builder notation and logical equivalences to establish the first De Morgan law A∩B=A∪B.

Solution: We can prove this identity with the following steps.

$$
\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement}\\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol}\\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection}\\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences}\\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol}\\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement}\\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union}\\
&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}
\end{aligned}
$$

Let A, B, and C be sets. Show that A ∪ (B ∩ C) = (C ∪ B) ∩ A.

Solution: We have

$$\begin{aligned}
\overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{(B \cap C)} && \text{by the first De Morgan law} \\
&= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{by the second De Morgan law} \\
&= (\overline{B} \cup \overline{C}) \cap \overline{A} && \text{by the commutative law for intersections} \\
&= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{by the commutative law for unions.}
\end{aligned}$$

Suppose that P and Q are the multisets $\{4 \cdot a, 1 \cdot b, 3 \cdot c\}$ and $\{3 \cdot a, 4 \cdot b, 2 \cdot d\}$, respectively. Find $P \cup Q$, $P \cap Q$, $P - Q$, and $P + Q$.

Solution: We have

$$\begin{aligned}
P \cup Q &= \{\max(4, 3) \cdot a, \max(1, 4) \cdot b, \max(3, 0) \cdot c, \max(0, 2) \cdot d\} \\
&= \{4 \cdot a, 4 \cdot b, 3 \cdot c, 2 \cdot d\},
\end{aligned}$$

$$\begin{aligned}
P \cap Q &= \{\min(4, 3) \cdot a, \min(1, 4) \cdot b, \min(3, 0) \cdot c, \min(0, 2) \cdot d\} \\
&= \{3 \cdot a, 1 \cdot b, 0 \cdot c, 0 \cdot d\} = \{3 \cdot a, 1 \cdot b\},
\end{aligned}$$

$$\begin{aligned}
P - Q &= \{\max(4 - 3, 0) \cdot a, \max(1 - 4, 0) \cdot b, \max(3 - 0, 0) \cdot c, \max(0 - 2, 0) \cdot d\} \\
&= \{1 \cdot a, 0 \cdot b, 3 \cdot c, 0 \cdot d\} = \{1 \cdot a, 3 \cdot c\}, \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
P + Q &= \{(4 + 3) \cdot a, (1 + 4) \cdot b, (3 + 0) \cdot c, (0 + 2) \cdot d\} \\
&= \{7 \cdot a, 5 \cdot b, 3 \cdot c, 2 \cdot d\}.
\end{aligned}$$

2.3 Functions

Functions are sometimes also called **mappings** or **transformations**.

Definition 2 If f is a function from A to B, we say that A is the *domain* of f and B is the *codomain* of f. If $f(a) = b$, we say that b is the *image* of a and a is a *preimage* of b. The *range*, or *image*, of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f *maps* A to B.

Definition 3 Let f_1 and f_2 be functions from A to $\mathbf{R}$. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from A to $\mathbf{R}$ defined for all $x \in A$ by

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

Definition 4 Let f be a function from A to B and let S be a subset of A. The *image* of S under the function f is the subset of B that consists of the images of the elements of S. We denote the image of S by $f(S)$, so

$$f(S) = \{t \mid \exists s \in S\ (t = f(s))\}.$$

We also use the shorthand $\{f(s) \mid s \in S\}$ to denote this set.

Definition 5 A function f is said to be *one-to-one*, or an *injection*, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. A function is said to be *injective* if it is one-to-one.

即 $\forall a \forall b\ (f(a)=f(b) \rightarrow a=b)$

单射 injection/one-to-one：对X中任意两个不同的x1、x2，f(x1)不等于f(x2)，集合x的元素数 < 集合y

Definition 7 A function f from A to B is called *onto*, or a *surjection*, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function f is called *surjective* if it is onto.

即 $\forall y\ \exists x\ (f(x)=y)$

满射 surjective/onto：Y中的任何一个元素都是X中某元素的像

Definition 8 The function f is a *one-to-one correspondence*, or a *bijection*, if it is both one-to-one and onto. We also say that such a function is *bijective*.

双射bijection：既单又满

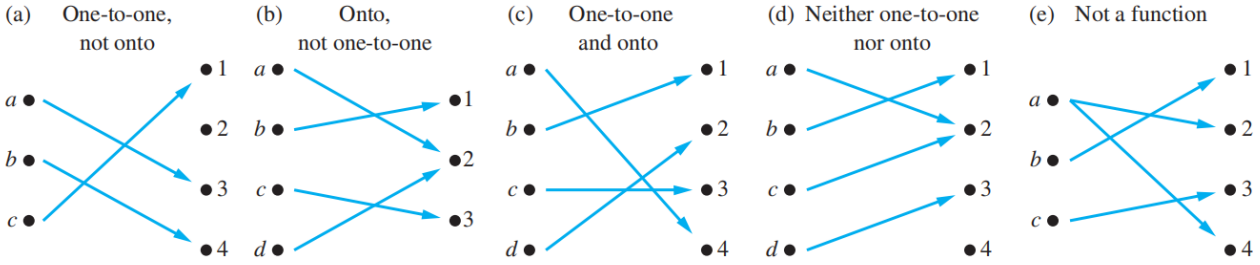
Suppose that $f : A \to B$.

To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$, then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.



arbitrary means 任意

Definition 10 Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The *composition* of the functions f and g, denoted for all $a \in A$ by $f \circ g$, is the function from A to C defined by

$$(f \circ g)(a) = f(g(a)).$$

TABLE 1 Useful Properties of the Floor and Ceiling Functions.
(n is an integer, x is a real number)

(1a)	$\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$
(1b)	$\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$
(1d)	$\lceil x \rceil = n$ if and only if $x \leq n < x + 1$
(2)	$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x + n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x + n \rceil = \lceil x \rceil + n$

2.4 Sequences and Summations

TABLE 2 Some Useful Summation Formulae.

Sum	*Closed Form*
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x\rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

Definition 3 A set that is either finite or has the same cardinality as the set of positive integers is called *countable*. A set that is not countable is called *uncountable*. When an infinite set S is countable, we denote the cardinality of S by $\aleph_0$ (where $\aleph$ is aleph, the first letter of the Hebrew alphabet). We write $|S| = \aleph_0$ and say that S has cardinality "aleph null."

Every real number has a unique decimal expansion (when the possibility that the expansion has a tail end that consists entirely of the digit 9 is excluded). Therefore, the real number r is not equal to any of $r_1, r_2, \ldots$ because the decimal expansion of r differs from the decimal expansion of r_i in the ith place to the right of the decimal point, for each i.

Because there is a real number r between 0 and 1 that is not in the list, the assumption that all the real numbers between 0 and 1 could be listed must be false. Therefore, all the real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable. Any set with an uncountable subset is uncountable (see Exercise 15). Hence, the set of real numbers is uncountable. ◀

2.5 Cardinality of Sets

集合的基数

2.5.1 Introduction

The sets A and B have the **same cardinality** (denoted by | A |= | B |) iff there exists a **one-to-one correspondence** (bijection) from A to B. 基数相同，当且仅当有一一对应关系。

如果B是A的子集，则|B|≤|A|;

2.5.2 Countable sets

Countable sets 可数集：A set that is either finite or has the same cardinality as the set of positive integers 和正整数集的基数相同的集合是可数的

An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers) 无限集可数，当且仅当可以用序列列出集合的元素

Example 1

Example 4: Show that the set of positive even integers E is countable set.

Solution: Let $f(x) = 2x$.

1	2	3	4	5	6	…..
↕	↕	↕	↕	↕	↕	
2	4	6	8	10	12	……

Then f is a bijection from N to E since f is both one-to-one and onto.

- **To show that it is one-to-one, suppose that $f(n) = f(m)$. Then $2n = 2m$, and so $n = m$.**
- **To see that it is onto, suppose that t is an even positive integer. Then $t = 2k$ for some positive integer k and $f(k) = t$.**

Note :

- **E is countable infinite.**
- **E is a proper subset of Z^+! But $|E| = |Z^+|$.**

Example 2

- The Positive Rational Numbers are Countable

Example 6: Show that the positive rational numbers are countable.

- **$\forall x \in Q^+, x = q/p$, $p, q \in N, q \neq 0$, $N=\{1,2,3,4,5,\ldots\}$**
- **Let $S=\{(p, q) | p, q \in N\} = N \times N$.**
- $$\left.\begin{array}{l} |Q^+| \leq |S| \\ |S| = |N| \\ |N| \leq |Q^+| \end{array}\right\} \Rightarrow |Q^+| = |N|$$

- The set of all rational numbers Q, positive and negative, is countable infinite. 所有有理数集是无限可数集
- The set of rational numbers and the set of natural numbers have same cardinality，namely |Q| = |N| 有理数集和自然数集基数相同

Conclusion

1) No infinite set has a smaller cardinality than a countable set.
2) The union of two countable sets is countable.
3) The union of finite number of countable sets is countable.
4) The union of a countable number of countable sets is countable.

THEOREM 1 If A and B are countable sets, then $A \cup B$ is also countable.

2.5.3 Uncountable sets

【*Theorem*】The set of real numbers (between 0 and 1) is **uncountable**. 实数集不可数

Solution: To show that the set of real numbers is uncountable, we suppose that the set of real numbers is countable and arrive at a contradiction. Then, the subset of all real numbers that fall between 0 and 1 would also be countable (because any subset of a countable set is also countable; see Exercise 16). Under this assumption, the real numbers between 0 and 1 can be listed in some order, say, $r_1, r_2, r_3, \ldots$. Let the decimal representation of these real numbers be

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\ldots \\ r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\ldots \\ &\vdots \end{aligned}$$

where $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. (For example, if $r_1 = 0.23794102\ldots$, we have $d_{11} = 2$, $d_{12} = 3$, $d_{13} = 7$, and so on.) Then, form a new real number with decimal expansion $r = 0.d_1d_2d_3d_4\ldots$, where the decimal digits are determined by the following rule:

$$d_i = \begin{cases} 4 \text{ if } d_{ii} \neq 4 \\ 5 \text{ if } d_{ii} = 4. \end{cases}$$

(As an example, suppose that $r_1 = 0.23794102\ldots$, $r_2 = 0.44590138\ldots$, $r_3 = 0.09118764\ldots$, $r_4 = 0.80553900\ldots$, and so on. Then we have $r = 0.d_1d_2d_3d_4\ldots = 0.4544\ldots$, where $d_1 = 4$ because $d_{11} \neq 4$, $d_2 = 5$ because $d_{22} = 4$, $d_3 = 4$ because $d_{33} \neq 4$, $d_4 = 4$ because $d_{44} \neq 4$, and so on.)

(Un)Computable

A function is **computable** 不可计算 if there is a computer program in some programming language that **finds the values of this function**. If a function is not computable we say it is uncomputable.

Continuum Hypothesis 连续性假设

The cardinality of the power set of an arbitrary set has a greater cardinality than the original arbitrary set.

The power set of Z^+ and the set of real numbers R have the same cardinality.

$$|P(Z^+)| = |R| = c$$

- 任意集合其所有子集的基数大于原来集合的基数
- 正整数集的所有子集和实数集的所有子集有相同的基数

The continuum hypothesis (CH) asserts that there is no cardinal number a such that $\aleph_0 < a < \aleph$.

3 Algorithms

3.1 Algorithms

Definition 1 An *algorithm* is a finite sequence of precise instructions for performing a computation or for solving a problem.

Searching Algorithms; Sorting; String Matching; Greedy Algorithms

3.2 The Growth of Functions

f(x) is O(g(x)) : the fact that $|f(x)| \leq C|g(x)|$ for all $x > k$ for some constants C and k
f(x) is Ω(g(x)) : the fact that $|f(x)| \geq C|g(x)|$ for all $x > k$ for some positive constants C and k
f(x) is Θ(g(x)) :the fact that f(x) is both _O(g(x)) and Ω(g(x))

Big-O

$log(n!) = O(nlogn)$

Definition 1 Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $O(g(x))$ if there are constants C and k such that

$$|f(x)| \leq C|g(x)|$$

whenever $x > k$. [This is read as "$f(x)$ is big-oh of $g(x)$."]

THEOREM 1 Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_{n-1}, a_n$ are real numbers. Then $f(x)$ is $O(x^n)$.

THEOREM 2 Suppose that $f_1(x)$ is $O(g_1(x))$ and that $f_2(x)$ is $O(g_2(x))$. Then $(f_1 + f_2)(x)$ is $O(g(x))$, where $g(x) = (\max(|g_1(x)|, |g_2(x)|)$ for all x.

COROLLARY 1 Suppose that $f_1(x)$ and $f_2(x)$ are both $O(g(x))$. Then $(f_1 + f_2)(x)$ is $O(g(x))$.

THEOREM 3 Suppose that $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. Then $(f_1 f_2)(x)$ is $O(g_1(x)g_2(x))$.

例 9 试给出 $f(n)=3n\log(n!)+(n^2+3)\log n$ 的大 O 估算，其中 n 是一个正整数。

解 首先估算乘积 $3n\log(n!)$。从例 6 知道 $\log(n!)$ 是 $O(n\log n)$ 的。由这一估算及 $3n$ 是 $O(n)$ 的事实，定理 3 给出的估算为 $3n\log(n!)$ 是 $O(n^2\log n)$ 的。

下一步估算乘积 $(n^2+3)\log n$。因为当 $n>2$ 时 $(n^2+3)<2n^2$ 成立，则有 n^2+3 是 $O(n^2)$ 的。因此，由定理 3 可知 $(n^2+3)\log n$ 是 $O(n^2\log n)$ 的。用定理 2 把两个乘积的大 O 估算组合起来得 $f(n)=3n\log(n!)+(n^2+3)\log n$ 是 $O(n^2\log n)$ 的。 ◀

Big-Omega and Big-Theta Notation

Definition 2 Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $\Omega(g(x))$ if there are constants C and k with C positive such that

$$|f(x)| \geq C|g(x)|$$

whenever $x > k$. [This is read as "$f(x)$ is big-Omega of $g(x)$."]

Definition 3 Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $\Theta(g(x))$ if $f(x)$ is $O(g(x))$ and $f(x)$ is $\Omega(g(x))$. When $f(x)$ is $\Theta(g(x))$, we say that f is big-Theta of $g(x)$, that $f(x)$ is of *order* $g(x)$, and that $f(x)$ and $g(x)$ are of the *same order*.

THEOREM 4 Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_n$ are real numbers with $a_n \neq 0$. Then $f(x)$ is of order x^n.

通常，当采用大 Θ 记号时，$\Theta(g(x))$ 中的函数 $g(x)$ 是一个相对简单的参照函数，诸如 x^n、c^x、$\log x$ 等，而 $f(x)$ 则相对复杂。

例 13 证明 $3x^2+8x\log x$ 是 $\Theta(x^2)$。

解 因为 $0\leqslant 8x\log x\leqslant 8x^2$，所以对 $x>1$ 有 $3x^2+8x\log x\leqslant 11x^2$。因此，$3x^2+8x\log x$ 是 $O(x^2)$ 的。显然，x^2 是 $O(3x^2+8x\log x)$ 的。因此，$3x^2+8x\log x$ 是 $\Theta(x^2)$ 的。 ◀

example

We can easily show that $(n- i)(i + 1) \geq n$ for $i = 0,1, \ldots, n - 1$. Hence, $(n!)^2 = (n \cdot 1)((n - 1) \cdot 2)((n - 2) \cdot 3) \ldots (2 \cdot (n - 1)) \cdot (1 \cdot n) \geq n^n$. Therefore, $2 \log n! \geq n \log n$.

3.3 Complexity of Algorithms

TABLE 1 Commonly Used Terminology for the Complexity of Algorithms.

Complexity	*Terminology*
$\Theta(1)$	Constant complexity
$\Theta(\log n)$	Logarithmic complexity
$\Theta(n)$	Linear complexity
$\Theta(n \log n)$	Linearithmic complexity
$\Theta(n^b)$	Polynomial complexity
$\Theta(b^n)$, where $b > 1$	Exponential complexity
$\Theta(n!)$	Factorial complexity

THEOREM 1 Let a, b, and c be integers, where $a \neq 0$. Then

(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(*ii*) if $a \mid b$, then $a \mid bc$ for all integers c;
(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$ (proved in Section 5.2).

- d is called the divisor.
- a is called the dividend.
- q is called the quotient.
- r is called the remainder.

Definitions of Functions div and mod
$q = a \text{ div } d$
$r = a \bmod d$

Examples:

4 Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

Definition 1 If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$ (or equivalently, if $\frac{b}{a}$ is an integer). When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

a | b：a divides b, b是大的被除数

THEOREM 1 Let a, b, and c be integers, where $a \neq 0$. Then

(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(*ii*) if $a \mid b$, then $a \mid bc$ for all integers c;
(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

COROLLARY 1 If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

THEOREM 2 **THE DIVISION ALGORITHM** Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition 2 In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

a div d: a 整除d为q

THEOREM 3 Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \textbf{ mod } m = b \textbf{ mod } m$.

同余定理

定理四 a ≡ b (mod m)，则a=b+km

THEOREM 5 Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

COROLLARY 2 Let m be a positive integer and let a and b be integers. Then

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Proof: By the definitions of **mod** m and of congruence modulo m, we know that $a \equiv (a \bmod m) \pmod m$ and $b \equiv (b \bmod m) \pmod m$. Hence, Theorem 5 tells us that

$$a + b \equiv (a \bmod m) + (b \bmod m) \pmod m$$

and

$$ab \equiv (a \bmod m)(b \bmod m) \pmod m.$$

The equalities in this corollary follow from these last two congruences by Theorem 3. ◁

We can define arithmetic operations on $\mathbf{Z}_m$, the set of nonnegative integers less than m, that is, the set $\{0, 1, \ldots, m - 1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

$$a +_m b = (a + b) \bmod m,$$

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by $\cdot_m$ by

$$a \cdot_m b = (a \cdot b) \bmod m,$$

where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers. The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo m and when we use these operations, we are said to be doing **arithmetic modulo** m.

模m算术：满足

封闭性：如果 a 和 b 属于 $\mathbf{Z}_m$，则 $a+_m b$ 和 $a \cdot_m b$ 也属于 $\mathbf{Z}_m$。

结合律：如果 a，b 和 c 属于 $\mathbf{Z}_m$，则有 $(a+_m b)+_m c=a+_m(b+_m c)$ 和 $(a \cdot_m b) \cdot_m c=a \cdot_m(b \cdot_m c)$。

交换律：如果 a 和 b 属于 $\mathbf{Z}_m$，则 $a+_m b=b+_m a$ 和 $a \cdot_m b=b \cdot_m a$。

单位元：元素 0 和 1 分别是模 m 加法和乘法的单位元。即，如果 a 属于 $\mathbf{Z}_m$，则 $a+_m 0=0+_m a=a$ 和 $a \cdot_m 1=1 \cdot_m a=a$。

加法逆元：如果 $a \neq 0$ 属于 $\mathbf{Z}_m$，则 $m-a$ 是 a 的模 m 加法逆元，而 0 是其自身的加法逆元。即 $a+_m(m-a)=0$ 且 $0+_m 0=0$。

分配律：如果 a，b 和 c 属于 $\mathbf{Z}_m$，则 $a \cdot_m(b+_m c)=(a \cdot_m b)+_m(a \cdot_m c)$ 和 $(a+_m b) \cdot_m c=(a \cdot_m c)+_m(b \cdot_m c)$。

4.2 Integer Representations and Algorithms

THEOREM 1 Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

n的b进制展开式

EXAMPLE 5 Find the hexadecimal expansion of $(177130)_{10}$.

Solution: First divide 177130 by 16 to obtain

$$177130 = 16 \cdot 11070 + 10.$$

Successively dividing quotients by 16 gives

$$\begin{aligned} 11070 &= 16 \cdot 691 + 14, \\ 691 &= 16 \cdot 43 + 3, \\ 43 &= 16 \cdot 2 + 11, \\ 2 &= 16 \cdot 0 + 2. \end{aligned}$$

The successive remainders that we have found, 10, 14, 3, 11, 2, give us the digits from the right to the left of 177130 in the hexadecimal (base 16) expansion of $(177130)_{10}$. It follows that

$$(177130)_{10} = (2B3EA)_{16}.$$

4.3 Primes and Greatest Common Divisors

relatively prime互素
prime：素数
composite:合数
Mersenne prime 梅森素数**:** a prime of the form 2p _− 1, where p is prime
Trial Division 试除法

THEOREM 2 If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

The Sieve of Eratosthenes 埃拉托斯特尼筛法

100内筛2、3、5、7整除的数

THEOREM 4 **THE PRIME NUMBER THEOREM** The ratio of $\pi(x)$, the number of primes not exceeding x, and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

Definition 2 Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

gcd：最大公约数

Definition 5 The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

lcm：最小公倍数

THEOREM 5 Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

LEMMA 1 Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

The Euclidean Algorithm 欧几里得算法

EXAMPLE 16 Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41. \end{aligned}$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

贝祖定理

THEOREM 6 **BÉZOUT'S THEOREM** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Bezout coefficients of a and b: sa + tb = gcd(a, b)

LEMMA 2 If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

LEMMA 3 If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

THEOREM 7 Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

a ≡ b (mod m) (a is congruent to b modulo m): a − b is divisible by m，即a-b能被m整除

4.4 Solving Congruences 求解同余方程

sa + **tm** = 1 → s是a mod m的逆

1. 用欧几里得算法算模的逆s
2. 左右两边同 ✕s
3. 得到x的解即为等式右边

Once we have an inverse $\overline{a}$ of a modulo m, we can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides of the linear congruence by $\overline{a}$, as Example 3 illustrates.

EXAMPLE 3 What are the solutions of the linear congruence $3x \equiv 4 \pmod{7}$?

Solution: By Example 1 we know that -2 is an inverse of 3 modulo 7. Multiplying both sides of the congruence by -2 shows that

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$.

We need to determine whether every x with $x \equiv 6 \pmod{7}$ is a solution. Assume that $x \equiv 6 \pmod{7}$. Then, by Theorem 5 of Section 4.1, it follows that

$$3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7},$$

which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are the integers x such that $x \equiv 6 \pmod{7}$, namely, $6, 13, 20, \ldots$ and $-1, -8, -15, \ldots$. ◀

解法一 因 $(a, m) = 1$，则存在二数 s, t 使 $as + mt = 1$，即 $as \equiv 1 \pmod{m}$，由此有 $asx \equiv bs \pmod{m}$，于是 $x \equiv bs \pmod{m}$ 为 (1) 的解.

例如, 方程 $2x = 3 \pmod{5}$，由于 $2 \times 13 - 5 \times 4 \equiv 1 \pmod{5}$，则 $x = 3 \times 13 = 39 \equiv 4 \pmod{5}$ 为其解.

该解法a，m要求互素

Chinese remainder theorem 中国剩余定理

THEOREM 2 **THE CHINESE REMAINDER THEOREM** Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1},\\
x &\equiv a_2 \pmod{m_2},\\
&\cdot\\
&\cdot\\
&\cdot\\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo m to this solution.)

$$M_k = m/m_k$$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

例 4 在公元 1 世纪，中国数学家孙子问道："有物不知其数，三分之余二，五分之余三，七分之余二，此物几何？"

这个谜题可以翻译成下面的问题：下列同余方程组的解什么？

$$
\begin{aligned}
x &\equiv 2 \pmod 3\\
x &\equiv 3 \pmod 5\\
x &\equiv 2 \pmod 7
\end{aligned}
$$

例 5 要求解例 4 中的同余方程组，首先令 $m = 3 \cdot 5 \cdot 7 = 105$，$M_1 = m/3 = 35$，$M_2 = m/5 = 21$，$M_3 = m/7 = 15$。可以看出 2 是 $M_1 = 35$ 模 3 的逆，因为 $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$；1 是 $M_2 = 21$ 模 5 的逆，因为 $21 \equiv 1 \pmod 5$；1 也是 $M_3 = 15$ 的模 7 逆，因为 $15 \equiv 1 \pmod 7$。该方程组的解是那些满足下列式子的 x：

$$
\begin{aligned}
x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1\\
&= 233 \equiv 23 \pmod{105}
\end{aligned}
$$

从而得出 23 是方程组的最小正整数解。我们的结论是 23 是最小的正整数满足除以 3 时余 2，除以 5 时余 3，除以 7 时余 2。 ◀

尽管定理 2 的构造法提供了一个通用方法来求解模数两两互素的同余方程组，但还可以用不同的方法更容易地求解方程组。例 6 解释了利用一种称为是**反向替换的方法**。

Back substitution 反向替换 → 翻译成一个同余式

同余方程重写为

例 6 利用反向替换方法找出所有整数 x 使得 $x\equiv1(\mathrm{mod}\ 5)$，$x\equiv2(\mathrm{mod}\ 6)$，和 $x\equiv3(\mathrm{mod}\ 7)$ 成立。

解 由 4.1 节定理 4 可知，第一个同余方程可以重写为一个等式 $x=5t+1$，这里 t 是一个整数。用这个表达式替换第二个同余方程中的 x，可得

$$5t+1\equiv2(\mathrm{mod}\ 6)$$

这容易解得 $t\equiv5(\mathrm{mod}\ 6)$(读者应该能验证)。再次应用 4.1 节定理 4，可得 $t=6u+5$，这里 u 是一个整数。用这个表达式反向替换等式 $x=5t+1$ 中的 t 可得 $x=5(6u+5)+1=30u+26$。再用这个替换第三个同余方程，得到

$$30u+26\equiv3(\mathrm{mod}\ 7)$$

解该同余方程可得 $u\equiv6(\mathrm{mod}\ 7)$(读者应该能验证)。故，4.1 节定理 4 告诉我们 $u=7v+6$，这里 v 是一个整数。用这个表达式替换等式 $x=30u+26$ 中的 u 可得 $x=30(7v+6)+26=210u+206$。将这个翻译成一个同余式，就找到了同余方程组的解，

$$x\equiv206(\mathrm{mod}\ 210)$$

◀

pseudo prime to the base b 以b为基底的伪素数: a composite integer n such that $bn-1\equiv1(\mathrm{mod}\ n)$

费马小定理

THEOREM 3 **FERMAT'S LITTLE THEOREM** If p is prime and a is an integer not divisible by p, then

$$a^{p-1}\equiv1\ (\mathrm{mod}\ p).$$

Furthermore, for every integer a we have

$$a^{p}\equiv a\ (\mathrm{mod}\ p).$$

例 9 计算 $7^{222}\ \mathbf{mod}\ 11$。

解 我们利用费马小定理来计算 $7^{222}\ \mathbf{mod}\ 11$ 而不采用快速模指数算法。由费马小定理可知 $7^{10}\equiv1(\mathrm{mod}\ 11)$，所以对每个正整数 k 有 $(7^{10})^k\equiv1(\mathrm{mod}\ 11)$。为了利用这最后一个同余式，我们将指数 222 除以 10，得 $222=22\cdot10+2$。可以看出

$$7^{222}=7^{22\cdot10+2}=(7^{10})^{22}7^2\equiv(1)^{22}\cdot49\equiv5(\mathrm{mod}\ 11)$$

从而得 $7^{222}\ \mathbf{mod}\ 11=5$。

◀

Definition 2 A composite integer n that satisfies the congruence $b^{n-1}\equiv1\ (\mathrm{mod}\ n)$ for all positive integers b with $\gcd(b,n)=1$ is called a *Carmichael number*. (These numbers are named after Robert Carmichael, who studied them in the early twentieth century.)

卡米切尔数

例 11 整数 561 是卡米切尔数。为了说明这一点，首先注意 561 是合数，因为 $561=3\cdot 11\cdot 17$。其次，注意到如果 $\gcd(b, 561)=1$，则 $\gcd(b, 3)=\gcd(b, 11)=\gcd(b, 17)=1$。

利用费马小定理可得到

$$b^2 \equiv 1 \pmod 3, \quad b^{10} \equiv 1 \pmod{11}, \quad b^{16} \equiv 1 \pmod{17}$$

从而有

$$b^{560} = (b^2)^{280} \equiv 1 \pmod 3$$
$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$$
$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$$

根据练习 29 可得，对于所有满足 $\gcd(b, 561)=1$ 的正整数 b 都有 $b^{560}\equiv 1 \pmod{561}$。因此，561 是卡米切尔数。 ◀

5 Induction and Recursion

5.1 Mathematical Induction

Mathematical Induction 数学归纳法

PRINCIPLE OF MATHEMATICAL INDUCTION To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

inductive hypothesis 归纳假设

Template for Proofs by Mathematical Induction

1. Express the statement that is to be proved in the form "for all $n \geq b$, $P(n)$" for a fixed integer b. For statements of the form "$P(n)$ for all positive integers n," let $b = 1$, and for statements of the form "$P(n)$ for all nonnegative integers n," let $b = 0$. For some statements of the form $P(n)$, such as inequalities, you may need to determine the appropriate value of b by checking the truth values of $P(n)$ for small values of n, as is done in Example 6.
2. Write out the words "Basis Step." Then show that $P(b)$ is true, taking care that the correct value of b is used. This completes the first part of the proof.
3. Write out the words "Inductive Step" and state, and clearly identify, the inductive hypothesis, in the form "Assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$."
4. State what needs to be proved under the assumption that the inductive hypothesis is true. That is, write out what $P(k + 1)$ says.
5. Prove the statement $P(k + 1)$ making use of the assumption $P(k)$. (Generally, this is the most difficult part of a mathematical induction proof. Decide on the most promising proof strategy and look ahead to see how to use the induction hypothesis to build your proof of the inductive step. Also, be sure that your proof is valid for all integers k with $k \geq b$, taking care that the proof works for small values of k, including $k = b$.)
6. Clearly identify the conclusion of the inductive step, such as by saying "This completes the inductive step."
7. After completing the basis step and the inductive step, state the conclusion, namely, "By mathematical induction, $P(n)$ is true for all integers n with $n \geq b$".

EXAMPLE 8 Use mathematical induction to prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer. (Note that this is the statement with $p = 3$ of Fermat's little theorem, which is Theorem 3 of Section 4.4.)

Extra Examples

Solution: To construct the proof, let $P(n)$ denote the proposition: "$n^3 - n$ is divisible by 3."

BASIS STEP: The statement $P(1)$ is true because $1^3 - 1 = 0$ is divisible by 3. This completes the basis step.

INDUCTIVE STEP: For the inductive hypothesis we assume that $P(k)$ is true; that is, we assume that $k^3 - k$ is divisible by 3 for an arbitrary positive integer k. To complete the inductive step, we must show that when we assume the inductive hypothesis, it follows that $P(k + 1)$, the statement that $(k + 1)^3 - (k + 1)$ is divisible by 3, is also true. That is, we must show that $(k + 1)^3 - (k + 1)$ is divisible by 3. Note that

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k).\end{aligned}$$

Using the inductive hypothesis, we conclude that the first term $k^3 - k$ is divisible by 3. The second term is divisible by 3 because it is 3 times an integer. So, by part (i) of Theorem 1 in Section 4.1, we know that $(k + 1)^3 - (k + 1)$ is also divisible by 3. This completes the inductive step.

Because we have completed both the basis step and the inductive step, by the principle of mathematical induction we know that $n^3 - n$ is divisible by 3 whenever n is a positive integer. ◀

5.2 Strong Induction and Well-Ordering

强归纳法（第二归纳法）和良序性

STRONG INDUCTION To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that the proposition $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.

良序性：Every *nonempty* set of *nonnegative* integers has the smallest element.
每个非空的自然数集都有最小的元素。

利用良序原理证明结论的模板：

证明$\forall \mathrm{n} \in \mathrm{N}, \mathrm{P}(\mathrm{n})$成立：

- 令$\mathrm{C} = \{\mathrm{n} | \mathrm{P}(\mathrm{n})$不成立$\}$。
- 假设C非空。
- 根据良序原理，$\exists \mathrm{n}_0 \in \mathrm{C}$为C中最小的元素。
- 推出矛盾——一般通过说明$\mathrm{P}(\mathrm{n}_0)$为真或者C中有比n_0更小的元素。
- 得出结论：C一定是空集，就是说，没有反例存在。

BASIS STEP: We verify that the propositions $P(b), P(b+1), \ldots, P(b+j)$ are true.

INDUCTIVE STEP: We show that $[P(b) \wedge P(b+1) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for every integer $k \geq b+j$.

That this alternative form is equivalent to strong induction is left as Exercise 28.

We begin with one of the most prominent uses of strong induction, the part of the fundamental theorem of arithmetic that tells us that every positive integer can be written as the product of primes.

EXAMPLE 2 Show that if n is an integer greater than 1, then n can be written as the product of primes.

Extra Examples

Solution: Let $P(n)$ be the proposition that n can be written as the product of primes.

BASIS STEP: $P(2)$ is true, because 2 can be written as the product of one prime, itself. (Note that $P(2)$ is the first case we need to establish.)

INDUCTIVE STEP: The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k. To complete the inductive step, it must be shown that $P(k+1)$ is true under this assumption, that is, that $k+1$ is the product of primes.

There are two cases to consider, namely, when $k+1$ is prime and when $k+1$ is composite. If $k+1$ is prime, we immediately see that $P(k+1)$ is true. Otherwise, $k+1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k+1$. Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if $k+1$ is composite, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b. ◀

5.3 Recursive Definitions and Structural Induction

递归定义和结构归纳法

We use two steps to define a function with the set of nonnegative integers as its domain:

BASIS STEP: Specify the value of the function at zero.

RECURSIVE STEP: Give a rule for finding its value at an integer from its values at smaller integers.

记$f_n = n!$

EXAMPLE 4 Show that whenever $n \geq 3$, $f_n > \alpha^{n-2}$, where $\alpha = (1 + \sqrt{5})/2$.

Extra Examples

Solution: We can use strong induction to prove this inequality. Let $P(n)$ be the statement $f_n > \alpha^{n-2}$. We want to show that $P(n)$ is true whenever n is an integer greater than or equal to 3.

BASIS STEP: First, note that

$$\alpha < 2 = f_3, \qquad \alpha^2 = (3 + \sqrt{5})/2 < 3 = f_4,$$

so $P(3)$ and $P(4)$ are true.

INDUCTIVE STEP: Assume that $P(j)$ is true, namely, that $f_j > \alpha^{j-2}$, for all integers j with $3 \leq j \leq k$, where $k \geq 4$. We must show that $P(k + 1)$ is true, that is, that $f_{k+1} > \alpha^{k-1}$. Because α is a solution of $x^2 - x - 1 = 0$ (as the quadratic formula shows), it follows that $\alpha^2 = \alpha + 1$. Therefore,

$$\alpha^{k-1} = \alpha^2 \cdot \alpha^{k-3} = (\alpha + 1)\alpha^{k-3} = \alpha \cdot \alpha^{k-3} + 1 \cdot \alpha^{k-3} = \alpha^{k-2} + \alpha^{k-3}.$$

By the inductive hypothesis, because $k \geq 4$, we have

$$f_{k-1} > \alpha^{k-3}, \qquad f_k > \alpha^{k-2}.$$

Therefore, it follows that

$$f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}.$$

Hence, $P(k + 1)$ is true. This completes the proof. ◀

THEOREM 1

LAMÉ'S THEOREM Let a and b be positive integers with $a \geq b$. Then the number of divisions used by the Euclidean algorithm to find $\gcd(a, b)$ is less than or equal to five times the number of decimal digits in b.

定理 1 拉梅定理 设 a 和 b 是满足 $a \geqslant b$ 的正整数。则欧几里得算法为了求出 $\gcd(a, b)$ 而使用的除法的次数小于或等于 b 的十进制位数的 5 倍。

Definition 1

The set Σ^* of *strings* over the alphabet Σ is defined recursively by

BASIS STEP: $\lambda \in \Sigma^*$ (where λ is the empty string containing no symbols).

RECURSIVE STEP: If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$.

Definition 3

The set of *rooted trees*, where a rooted tree consists of a set of vertices containing a distinguished vertex called the *root*, and edges connecting these vertices, can be defined recursively by these steps:

BASIS STEP: A single vertex r is a rooted tree.

RECURSIVE STEP: Suppose that $T_1, T_2, \ldots, T_n$ are disjoint rooted trees with roots $r_1, r_2, \ldots, r_n$, respectively. Then the graph formed by starting with a root r, which is not in any of the rooted trees $T_1, T_2, \ldots, T_n$, and adding an edge from r to each of the vertices $r_1, r_2, \ldots, r_n$, is also a rooted tree.

定义 3 以下这些步骤可以递归地定义根树的集合，其中根树是由一个顶点集合和连接这些顶点的边组成的，顶点集合包含的一个特殊顶点，称为树根。

基础步骤：单个顶点 r 是根树。

递归步骤：假设 T_1，T_2，…，T_n 是根树，分别带有树根 r_1，r_2，…，r_n。则如下形成的图也是根树：从树根 r 开始，r 不属于根树 T_1，T_2，…，T_n 中的任何一个，从 r 到顶点 r_1，r_2，…，r_n 中的每个都加入一条边。

Definition 6 We define the height $h(T)$ of a full binary tree T recursively.

BASIS STEP: The height of the full binary tree T consisting of only a root r is $h(T) = 0$.

RECURSIVE STEP: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1 + \max(h(T_1), h(T_2))$.

定义 6 递归地定义满二叉树 T 的高度 $h(T)$。

基础步骤：只含有树根 r 的满二叉树 T 的高度是 $h(T)=0$。

递归步骤：如果 T_1 和 T_2 都是满二叉树，则满二叉树 $T=T_1 \cdot T_2$ 有高度 $h(T)=1+\max(h(T_1), h(T_2))$。

If we let $n(T)$ denote the number of vertices in a full binary tree, we observe that $n(T)$ satisfies the following recursive formula:

BASIS STEP: The number of vertices $n(T)$ of the full binary tree T consisting of only a root r is $n(T) = 1$.

RECURSIVE STEP: If T_1 and T_2 are full binary trees, then the number of vertices of the full binary tree $T = T_1 \cdot T_2$ is $n(T) = 1 + n(T_1) + n(T_2)$.

如果设 $n(T)$ 表示满二叉树 T 的顶点个数，则 $n(T)$ 满足下面的递归定义：

基础步骤：只含有树根 r 的满二叉树 T 的顶点数 $n(T)$ 是 $n(T)=1$。

递归步骤：如果 T_1 和 T_2 都是满二叉树，则满二叉树 $T=T_1 \cdot T_2$ 的顶点数是 $n(T)=1+n(T_1)+n(T_2)$。

THEOREM 2 If T is a full binary tree T, then $n(T) \leq 2^{h(T)+1} - 1$.

定理 2 如果 T 是满二叉树，则 $n(T) \leqslant 2^{h(T)+1}-1$。

Proof: We prove this inequality using structural induction.

BASIS STEP: For the full binary tree consisting of just the root r the result is true because $n(T) = 1$ and $h(T) = 0$, so that $n(T) = 1 \leq 2^{0+1} - 1 = 1$.

RECURSIVE STEP: For the inductive hypothesis we assume that $n(T_1) \leq 2^{h(T_1)+1} - 1$ and $n(T_2) \leq 2^{h(T_2)+1} - 1$ whenever T_1 and T_2 are full binary trees. By the recursive formulae for $n(T)$ and $h(T)$ we have $n(T) = 1 + n(T_1) + n(T_2)$ and $h(T) = 1 + \max(h(T_1), h(T_2))$.

We find that

$$
\begin{aligned}
n(T) &= 1 + n(T_1) + n(T_2) && \text{by the recursive formula for } n(T) \\
&\overset{\text{IH}}{\leq} 1 + (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1) && \text{by the inductive hypothesis} \\
&\leq 2 \cdot \max(2^{h(T_1)+1}, 2^{h(T_2)+1}) - 1 && \text{because the sum of two terms is at most 2 times the larger} \\
&= 2 \cdot 2^{\max(h(T_1),h(T_2))+1} - 1 && \text{because } \max(2^x, 2^y) = 2^{\max(x,y)} \\
&= 2 \cdot 2^{h(T)} - 1 && \text{by the recursive definition of } h(T) \\
&= 2^{h(T)+1} - 1.
\end{aligned}
$$

This completes the recursive step. ◁

Generalized Induction 广义归纳法

EXAMPLE 13 Suppose that $a_{m,n}$ is defined recursively for $(m, n) \in \mathbf{N} \times \mathbf{N}$ by $a_{0,0} = 0$ and

$$a_{m,n} = \begin{cases} a_{m-1,n} + 1 & \text{if } n = 0 \text{ and } m > 0 \\ a_{m,n-1} + n & \text{if } n > 0. \end{cases}$$

Show that $a_{m,n} = m + n(n + 1)/2$ for all $(m, n) \in \mathbf{N} \times \mathbf{N}$, that is, for all pairs of nonnegative integers.

Solution: We can prove that $a_{m,n} = m + n(n + 1)/2$ using a generalized version of mathematical induction. The basis step requires that we show that this formula is valid when $(m, n) = (0, 0)$. The induction step requires that we show that if the formula holds for all pairs smaller than (m, n) in the lexicographic ordering of $\mathbf{N} \times \mathbf{N}$, then it also holds for (m, n).

BASIS STEP: Let $(m, n) = (0, 0)$. Then by the basis case of the recursive definition of $a_{m,n}$ we have $a_{0,0} = 0$. Furthermore, when $m = n = 0$, $m + n(n + 1)/2 = 0 + (0 \cdot 1)/2 = 0$. This completes the basis step.

INDUCTIVE STEP: Suppose that $a_{m',n'} = m' + n'(n' + 1)/2$ whenever (m', n') is less than (m, n) in the lexicographic ordering of $\mathbf{N} \times \mathbf{N}$. By the recursive definition, if $n = 0$, then $a_{m,n} = a_{m-1,n} + 1$. Because $(m - 1, n)$ is smaller than (m, n), the inductive hypothesis tells us that $a_{m-1,n} = m - 1 + n(n + 1)/2$, so that $a_{m,n} = m - 1 + n(n + 1)/2 + 1 = m + n(n + 1)/2$, giving us the desired equality. Now suppose that $n > 0$, so $a_{m,n} = a_{m,n-1} + n$. Because $(m, n - 1)$ is smaller than (m, n), the inductive hypothesis tells us that $a_{m,n-1} = m + (n - 1)n/2$, so $a_{m,n} = m + (n - 1)n/2 + n = m + (n^2 - n + 2n)/2 = m + n(n + 1)/2$. This finishes the inductive step. ◀

As mentioned, we will justify this proof technique in Section 9.6.

lexicographic ordering 字典序

5.4 Recursive Algorithms

递归算法

EXAMPLE 3 Give a recursive algorithm for computing the greatest common divisor of two nonnegative integers a and b with $a < b$.

Solution: We can base a recursive algorithm on the reduction $\gcd(a, b) = \gcd(b \bmod a, a)$ and the condition $\gcd(0, b) = b$ when $b > 0$. This produces the procedure in Algorithm 3, which is a recursive version of the Euclidean algorithm.

We illustrate the workings of Algorithm 3 with a trace when the input is $a = 5$, $b = 8$. With this input, the algorithm uses the "else" clause to find that $\gcd(5, 8) = \gcd(8 \bmod 5, 5) = \gcd(3, 5)$. It uses this clause again to find that $\gcd(3, 5) = \gcd(5 \bmod 3, 3) = \gcd(2, 3)$, then to get $\gcd(2, 3) = \gcd(3 \bmod 2, 2) = \gcd(1, 2)$, then to get $\gcd(1, 2) = \gcd(2 \bmod 1, 1) = \gcd(0, 1)$. Finally, to find $\gcd(0, 1)$ it uses the first step with $a = 0$ to find that $\gcd(0, 1) = 1$. Consequently, the algorithm finds that $\gcd(5, 8) = 1$. ◀

ALGORITHM 3 A Recursive Algorithm for Computing gcd(a, b).

procedure *gcd*(a, b: nonnegative integers with $a < b$)
if $a = 0$ **then return** b
else return *gcd*(b **mod** a, a)
{output is gcd(a, b)}

例 3 给出求满足 $a<b$ 的两个非负整数 a 和 b 的最大公因子的递归算法。

解 可以基于 $\gcd(a, b)=\gcd(b \bmod a, a)$ 和当 $b>0$ 时 $\gcd(0, b)=b$ 找出递归算法中的过程。这产生了欧几里得算法的递归版本——算法 3。

当输入为 $a=5$、$b=8$ 时，跟踪算法 3 以说明它是如何工作的。对该输入，算法执行 "else" 语句，得到 $\gcd(5, 8)=\gcd(8 \bmod 5, 5)=\gcd(3, 5)$。再执行此语句，得到 $\gcd(3, 5)=\gcd(5 \bmod 3, 3)=\gcd(2, 3)$，然后得到 $\gcd(2, 3)=\gcd(3 \bmod 2, 2)=\gcd(1, 2)$，再得到 $\gcd(1, 2)=\gcd(2 \bmod 1, 1)=\gcd(0, 1)$。最后，算法执行第一步，由 $a=0$ 得到 $\gcd(0, 1)=1$。因此，算法的执行结果是 $\gcd(5, 8)=1$。 ◀

算法 3 计算 $\gcd(a, b)$的递归算法
procedure $\gcd(a, b$：非负整数且 $a<b)$
if $a=0$ **then return** b
else return $\gcd(b \bmod a, a)$
{输出是 $\gcd(a, b)$}

geometric progression:几何数列（等比）

arithmetic progression:等差

6 Counting

6.1 The Basics of Counting

THE PRODUCT RULE Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

乘积原则

THE SUM RULE If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

求和原则

THE SUBTRACTION RULE If a task can be done in either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.

The subtraction rule is also known as the **principle of inclusion–exclusion**

减法原则又称容斥原理

THE DIVISION RULE There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.

除法原则

除法法则 如果一个任务能由一个可以用 n 种方式完成的过程实现，而对于每种完成任务的方式 w，在 n 种方式中正好有 d 种与之对应，那么完成这个任务的方法数为 n/d。

6.2 The Pigeonhole Principle

鸽巢原理

COROLLARY 1 A function f from a set with $k + 1$ or more elements to a set with k elements is not one-to-one.

THEOREM 2 **THE GENERALIZED PIGEONHOLE PRINCIPLE** If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

把N个物品放到k个箱子中，至少有一个箱子中包含$\lceil N/k \rceil$ 个物品（向上取整）

EXAMPLE 10 During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

Solution: Let a_j be the number of games played on or before the jth day of the month. Then $a_1, a_2, \ldots, a_{30}$ is an increasing sequence of distinct positive integers, with $1 \le a_j \le 45$. Moreover, $a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$ is also an increasing sequence of distinct positive integers, with $15 \le a_j + 14 \le 59$.

The 60 positive integers $a_1, a_2, \ldots, a_{30}, a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$ are all less than or equal to 59. Hence, by the pigeonhole principle two of these integers are equal. Because the integers $a_j, j = 1, 2, \ldots, 30$ are all distinct and the integers $a_j + 14, j = 1, 2, \ldots, 30$ are all distinct, there must be indices i and j with $a_i = a_j + 14$. This means that exactly 14 games were played from day $j + 1$ to day i. ◀

例 10 在 30 天的一个月里，某棒球队一天至少打一场比赛，但至多打 45 场。证明一定有连续的若干天内这个队恰好打了 14 场。

解 令 a_j 是在这个月的第 j 天或第 j 天之前所打的场数。则 a_1，a_2，…，a_{30} 是不同正整数的一个递增序列，其中 $1 \leqslant a_j \leqslant 45$。而且 a_1+14，a_2+14，…，$a_{30}+14$ 也是不同正整数的一个递增序列，其中 $15 \leqslant a_j+14 \leqslant 59$。

60 个正整数 a_1，a_2，…，a_{30}，a_1+14，a_2+14，…，$a_{30}+14$ 全都小于等于 59。因此，由鸽巢原理，有两个正整数相等。因为整数 $a_j(j=1, 2, \cdots, 30)$ 都不相同，并且 $a_j+14(j=1, 2, \cdots, 30)$ 也不相同，所以一定存在下标 i 和 j 满足 $a_i = a_j+14$。这意味着从第 $j+1$ 天到第 i 天恰好打了 14 场比赛。 ◀

定理 3 每个由 n^2+1 个不同实数构成的序列都包含一个长为 $n+1$ 的严格递增子序列或严格递减子序列。

THEOREM 3 Every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of length $n + 1$ that is either strictly increasing or strictly decreasing.

6.3 Permutations and Combinations

排序与组合

THEOREM 1 If n is a positive integer and r is an integer with $1 \leq r \leq n$, then there are

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

r-permutations of a set with n distinct elements.

COROLLARY 1 If n and r are integers with $0 \leq r \leq n$, then $P(n, r) = \dfrac{n!}{(n-r)!}$.

THEOREM 2 The number of r-combinations of a set with n elements, where n is a nonnegative integer and r is an integer with $0 \leq r \leq n$, equals

$$C(n, r) = \frac{n!}{r!\,(n-r)!}.$$

Definition 1

A *combinatorial proof* of an identity is a proof that uses counting arguments to prove that both sides of the identity count the same objects but in different ways or a proof that is based on showing that there is a bijection between the sets of objects counted by the two sides of the identity. These two types of proofs are called *double counting proofs* and *bijective proofs*, respectively.

6.4 Binomial Coefficients

THEOREM 1 **THE BINOMIAL THEOREM** Let x and y be variables, and let n be a nonnegative integer. Then

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

二项式定理

COROLLARY 1 Let n be a nonnegative integer. Then

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

COROLLARY 2 Let n be a positive integer. Then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

COROLLARY 3 Let n be a nonnegative integer. Then

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n.$$

帕斯卡恒等式 **pascal's identity**

THEOREM 2 **PASCAL'S IDENTITY** Let n and k be positive integers with $n \geq k$. Then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Proof: We will use a combinatorial proof. Suppose that T is a set containing $n+1$ elements. Let a be an element in T, and let $S = T - \{a\}$. Note that there are $\binom{n+1}{k}$ subsets of T containing k elements. However, a subset of T with k elements either contains a together with $k-1$ elements of S, or contains k elements of S and does not contain a. Because there are $\binom{n}{k-1}$ subsets of $k-1$ elements of S, there are $\binom{n}{k-1}$ subsets of k elements of T that contain a. And there are $\binom{n}{k}$ subsets of k elements of T that do not contain a, because there are $\binom{n}{k}$ subsets of k elements of S. Consequently,

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

◁

证明 我们将采用组合证明方法。假定 T 是包含 $n+1$ 个元素的集合。令 a 是 T 的一个元素且 $S=T-\{a\}$。注意，T 的包含 k 个元素的子集有 $\binom{n+1}{k}$ 个。然而 T 的包含 k 个元素的子集或者包含 a 和 S 中的 $k-1$ 个元素，或者不包含 a 但包含 S 中的 k 个元素。由于 S 的 $k-1$ 元子集有 $\binom{n}{k-1}$ 个，所以 T 含 a 在内的 k 元子集有 $\binom{n}{k-1}$ 个。又由于 S 的 k 元子集有 $\binom{n}{k}$ 个，所以 T 的不含 a 的 k 元子集有 $\binom{n}{k}$ 个。从而得到

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

◀

THEOREM 3 **VANDERMONDE'S IDENTITY** Let m, n, and r be nonnegative integers with r not exceeding either m or n. Then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}.$$

范德蒙德恒等式

证明 假定在第一个集合中有 m 项，第二个集合中有 n 项。从这两个集合的并集中取 r 个元素的方式数是 $\binom{m+n}{r}$。

从并集中取 r 个元素的另一种方式是先从第一个集合中取 k 个元素，接着从第二个集合中取 $r-k$ 个元素，其中 k 是满足 $0 \leqslant k \leqslant r$ 的整数。因为从第二个集合中选取 k 个元素的方法是 $\binom{n}{k}$，从第一个集合中选取 $r-k$ 个元素的方法是 $\binom{m}{r-k}$，所以由乘积法则，这可以用 $\binom{m}{r-k}\binom{n}{k}$ 种方式完成。所以，从这个并集中选取 r 个元素的总方式数等于 $\sum_{k=0}^{r}\binom{m}{r-k}\binom{n}{k}$。◀

我们已经找到从一个 m 个元素集合和一个 n 元素集合并集中取 r 个元素的方法数的两种表达式。这就证明了范德蒙德恒等式。

COROLLARY 4 If n is a nonnegative integer, then

$$\binom{2n}{n} = \sum_{k=0}^{n}\binom{n}{k}^2.$$

THEOREM 4 Let n and r be nonnegative integers with $r \leq n$. Then

$$\binom{n+1}{r+1} = \sum_{j=r}^{n}\binom{j}{r}.$$

证明：长度为n+1的位串里有r+1个1，最后一个1在第k位。那么前k-1位必须有r个1，即有C(k-1, r)种情况，同时对于最后一个1，k最小为r+1，最大为n+1，则把所有情况相加，

$$\sum_{k=r+1}^{n+1}\binom{k-1}{r} = \sum_{j=r}^{n}\binom{j}{r}$$

6.5 Generalized Permutations and Combinations

permutation 排列

THEOREM 2 There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set with n elements when repetition of elements is allowed.

定理 2 n 个元素的集合中允许重复的 r 组合有 $C(n+r-1, r)=C(n+r-1, n-1)$ 个。

Combination with repetition n个元素集合中允许重复的r组合个数:

$$H_n^r = C_{n-1+r}^{r} = C_{n-1+r}^{n-1}$$

表 1　允许和不允许重复的组合与排列

类　型	是否允许重复	公　式
r 排列	否	$\frac{n!}{(n-r)!}$
r 组合	否	$\frac{n!}{r!\,(n-r)!}$
r 排列	是	n^r
r 组合	是	$\frac{(n+r-1)!}{r!\,(n-1)!}$

Example

〖Example 3〗How many solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 = 16$$

where $x_i (i = 1,2,3,4)$ **is nonnegative integer?**

Question:

(1) $x_i > 1$, for $i = 1,2,3,4$ ⇨ $x_i \geq 2$

$$H_4^8 = C(4\text{-}1+8, 8) = C(11, 8) = C(11, 3)$$

(2) $x_1 + x_2 + x_3 + x_4 \leq 16$

We can introduce an auxiliary variable x_5 so that

$$x_1 + x_2 + x_3 + x_4 + x_5 = 16$$

$$H_5^{16} = C(5\text{-}1+16, 16) = C(20, 16) = C(20, 4)$$

THEOREM 3

The number of different permutations of n objects, where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, … , and n_k indistinguishable objects of type k, is

$$\frac{n!}{n_1!\, n_2! \cdots n_k!}.$$

1. Indistinguishable objects and distinguishable boxes

EXAMPLE 9 How many ways are there to place 10 indistinguishable balls into eight distinguishable bins?

Solution: The number of ways to place 10 indistinguishable balls into eight bins equals the number of 10-combinations from a set with eight elements when repetition is allowed. Consequently, there are

$$C(8 + 10 - 1, 10) = C(17, 10) = \frac{17!}{10!7!} = 19{,}448.$$

◀

This means that there are $C(n + r - 1, n - 1)$ ways to place r indistinguishable objects into n distinguishable boxes.

这意味着有 $C(n+r-1,\ n-1)$ 种方法将 r 个不可辨别的球放入 n 个可辨别的盒子。

2. **Distinguishable objects and indistinguishable boxes**

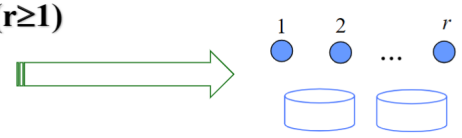
$\sum_{j=1}^{k} S(n,j) = \sum_{j=1}^{k} \frac{1}{j!} \sum_{i=0}^{j-1} (-1)^i \binom{j}{i} (j-i)^n.$ ：将n个不同的物品放进k个相同的箱子的总方法数

$S(n,j)$：将n个不同的物品放进j个相同的箱子（没有箱子是空的）

$S(n,j)j!$：将n个不同的物品房间j个不同的箱子（没有箱子是空的）

(1) $S(r,1)=S(r,r)=1$ $(r\geq 1)$

(2) $S(r,2)=2^{r-1}-1$



(3) $S(r,r-1)=C(r,2)$

(4) $S(r+1,n)=S(r,n-1)+nS(r,n)$

8 Advanced Counting Techniques

8.1 Applications of Recurrence Relations

递推关系

令 H_n 表示解 n 个盘子的汉诺塔问题所需要的移动次数。建立一个关于序列$\{H_n\}$的递推关系。

解 开始时 n 个盘子在柱 1。按照游戏规则，我们可以用 H_{n-1} 次移动将上边的 $n-1$ 个盘子移到柱 3(图 3 说明了此刻的柱子和盘子)。在这些移动中保留最大的盘子不动。然后，我们用一次移动将最大的盘子移到第二根柱子上。我们可以再使用 H_{n-1} 次移动将柱 3 上的 $n-1$ 个

盘子移到柱 2，把它们放到最大的盘子上面，这个最大的盘子一直放在柱 2 的底部。这表示解 n 个盘子的汉诺塔问题所需要的移动次数为 $2H_{n-1}+1$ 次。

令 H_n 表示解 n 个盘子的汉诺塔问题所需要的移动次数。建立一个关于序列$\{H_n\}$的递推关系。

解 开始时 n 个盘子在柱 1。按照游戏规则，我们可以用 H_{n-1} 次移动将上边的 $n-1$ 个盘子移到柱 3(图 3 说明了此刻的柱子和盘子)。在这些移动中保留最大的盘子不动。然后，我们用一次移动将最大的盘子移到第二根柱子上。我们可以再使用 H_{n-1} 次移动将柱 3 上的 $n-1$ 个

盘子移到柱 2，把它们放到最大的盘子上面，这个最大的盘子一直放在柱 2 的底部。这表示解 n 个盘子的汉诺塔问题所需要的移动次数为 $2H_{n-1}+1$ 次。

EXAMPLE 3 Find a recurrence relation and give initial conditions for the number of bit strings of length n that do not have two consecutive 0s. How many such bit strings are there of length five?

例 3 对于不含 2 个连续 0 的 n 位比特串的个数，找出递推关系和初始条件。有多少个这样的 5 位比特串？

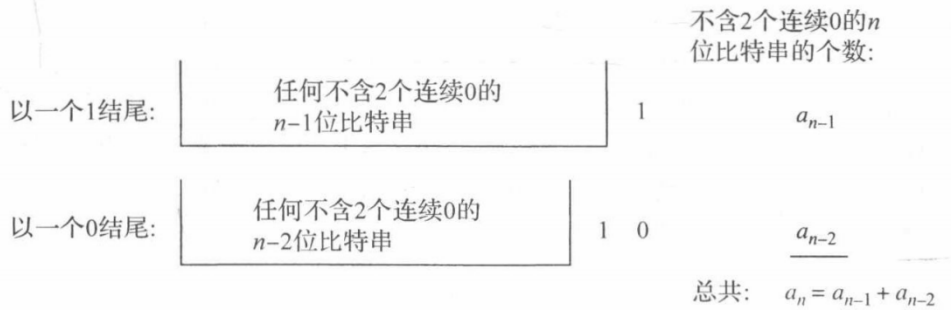
解 设 a_n 表示不含 2 个连续 0 的 n 位比特串的个数。我们将假定 $n\geqslant 3$，比特串至少有 3 位。n 位比特串可以分为以 1 结尾的和以 0 结尾的。

精确地说，不含 2 个连续 0 并以 1 结尾的 n 位比特串就是在不含 2 个连续 0 的 $n-1$ 位比特串的尾部加上一个 1。因此存在 a_{n-1} 个这样的比特串。

不含 2 个连续 0 并以 0 结尾的 n 位比特串的 $n-1$ 位必须是 1，否则就将以 2 个 0 结尾。因而，精确地说，不含 2 个连续 0 并以 0 结尾的 n 位比特串就是在不含 2 个连续 0 的 $n-2$ 位比特串的尾部加上 10。因此存在 a_{n-2} 个这样的比特串。

如图 4 所示，可以断言对于 $n\geqslant 3$，有

$$a_n = a_{n-1} + a_{n-2}$$



8.2 Solving Linear Recurrence Relations

求解线性递推关系

Definition 1 A *linear homogeneous recurrence relation of degree k with constant coefficients* is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

THEOREM 1 Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0, 1, 2, \ldots$, where α_1 and α_2 are constants.

定理 1　设 c_1 和 c_2 是实数。假设 $r^2 - c_1 r - c_2 = 0$ 有两个不相等的根 r_1 和 r_2，那么序列 $\{a_n\}$ 是递推关系 $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ 的解，当且仅当 $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ $(n = 0, 1, 2, \cdots)$，其中 α_1 和 α_2 是常数。

Fibonacci numbers: $f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

linear线性：右边是a_k*c之和+F(n)

homogeneous同类：都是形如$s_j * s$的项

constant coefficients常系数：对每个a_k前的系数都是常数

degree k：右边追溯到前k项，k=a-(n-k)

(1) $a_n = (1.02)a_{n-1}$
linear; constant coefficients; homogeneous; degree 1

(2) $a_n = (1.02)\, a_{n-1} + 2^{n-1}$
linear; constant coefficients; nonhomogeneous; degree 1

(3) $a_n = a_{n-1} + a_{n-2} + a_{n-3} + 2^{n-3}$
linear; constant coefficients; nonhomogeneous; degree 3

(4) $a_n = n\, a_{n-1} + n^2\, a_{n-2} + a_{n-1}\, a_{n-2}$
nonlinear; coefficients are not constants; homogeneous; degree 2

THEOREM 2

Let c_1 and c_2 be real numbers with $c_2 \neq 0$. Suppose that $r^2 - c_1 r - c_2 = 0$ has only one root r_0. A sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$, for $n = 0, 1, 2, \ldots$, where α_1 and α_2 are constants.

定理 2 设 c_1 和 c_2 是实数，$c_2 \neq 0$。假设 $r^2 - c_1 r - c_2 = 0$ 只有一个根 r_0。序列 $\{a_n\}$ 是递推关系 $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ 的解，当且仅当 $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$，$n = 0, 1, 2, \cdots$，其中 α_1 和 α_2 是常数。

定理 3 设 c_1，c_2，$\cdots$，c_k 是实数。假设特征方程

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

有 k 个不相等的根 r_1，r_2，$\cdots$，r_k。那么序列 $\{a_n\}$ 是递推关系

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

的解，当且仅当

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

$n = 0, 1, 2, \cdots$，其中 α_1，α_2，$\cdots$，α_k 是常数。

递推关系 $a_n = 3a_{n-1} + 2n$ 是一个**常系数线性非齐次递推关系**，即形如

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

THEOREM 4

Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has t distinct roots $r_1, r_2, \ldots, r_t$ with multiplicities $m_1, m_2, \ldots, m_t$, respectively, so that $m_i \geq 1$ for $i = 1, 2, \ldots, t$ and $m_1 + m_2 + \cdots + m_t = k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$\begin{aligned} a_n = {} & (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n \\ & + \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n \end{aligned}$$

for $n = 0, 1, 2, \ldots$, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

例 7 假设线性齐次递推关系的特征方程的根是 2、2、2、5、5 和 9（即有 3 个根，根 2 的重数为 3，根 5 的重数为 2，根 9 的重数为 1）。那么通解形式是什么？

解 由定理 4，解的一般形式是

$$(\alpha_{1,0} + \alpha_{1,1} n + \alpha_{1,2} n^2) 2^n + (\alpha_{2,0} + \alpha_{2,1} n) 5^n + \alpha_{3,0} 9^n$$

◀

定理 5 如果$\{a_n^{(p)}\}$是常系数非齐次线性递推关系

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

的一个特解，那么每个解都是$\{a_n^{(p)} + a_n^{(h)}\}$的形式，其中$\{a_n^{(h)}\}$是相伴的齐次递推关系

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

的一个解。

例 10 求递推关系 $a_n = 3a_{n-1} + 2n$ 的所有解。具有 $a_1 = 3$ 的解是什么？

解 为求解这个常系数线性非齐次递推关系，我们需要求解与它相伴的线性齐次方程并且找到一个关于给定非齐次方程的特解。相伴的线性齐次方程是 $a_n = 3a_{n-1}$。它的解是 $a_n^{(h)} = \alpha 3^n$，其中 α 是常数。

我们现在找一个特解。因为 $F(n) = 2n$ 是 n 的 1 次多项式，所以解的一个合理的尝试就是 n 的线性函数，比如说 $p_n = cn + d$，其中 c 和 d 是常数。为确定是否存在这种形式的解，假设 $p_n = cn + d$是一个这样的解。那么方程 $a_n = 3a_{n-1} + 2n$ 就变成 $cn + d = 3(c(n-1) + d) + 2n$。简化和归并同类项得$(2 + 2c)n + (2d - 3c) = 0$。从而，$cn + d$ 是一个解当且仅当 $2 + 2c = 0$ 和$2d - 3c = 0$。这说明 $cn + d$ 是一个解当且仅当 $c = -1$ 和 $d = -3/2$。因此，$a_n^{(p)} = -n - 3/2$ 是一个特解。

例 11 求出下述递推关系

$$a_n = 5a_{n-1} - 6a_{n-2} + 7^n$$

的所有的解。

解 这是一个线性非齐次递推关系。它的相伴的齐次递推关系

$$a_n = 5a_{n-1} - 6a_{n-2}$$

的解是 $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$，其中 α_1 和 α_2 是常数。因为 $F(n) = 7^n$，所以一个合理的解是 $a_n^{(p)} = C \cdot 7^n$，其中 C 是常数。把这些项代入递推关系得 $C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n$。提出公因子 7^{n-2}，这个等式变成 $49C = 35C - 6C + 49$，从而推出 $20C = 49$ 或 $C = 49/20$。于是，$a_n^{(p)} = (49/20)7^n$ 是特解。由定理 5，所有的解都有下述形式

$$a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n$$

◀

定理6是特解的形式

THEOREM 6 Suppose that $\{a_n\}$ satisfies the linear nonhomogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and

$$F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n,$$

where $b_0, b_1, \ldots, b_t$ and s are real numbers. When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

$$(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

When s is a root of this characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

最后a_n要把通解和特解相加

8.4 Generating Functions

生成函数

定义 1 实数序列 a_0，a_1，…，a_k，…的生成函数是无穷级数

$$G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k$$

THEOREM 1

Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$. Then

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k \quad \text{and} \quad f(x)g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k.$$

Extended Binomial Theorem 拓展二项式系数

THEOREM 2 **THE EXTENDED BINOMIAL THEOREM** Let x be a real number with $|x| < 1$ and let u be a real number. Then

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k.$$

TABLE 1 Useful Generating Functions.

$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k = 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k)$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^k x^k = 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	$C(n,k)a^k$
$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk} = 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	$C(n,k/r)$ if $r \mid k$; 0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if $k \le n$; 0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2x^2 + \cdots$	a^k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if $r \mid k$; 0 otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k = 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k) = C(n+k-1,n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k = 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n+k-1,k) = (-1)^k C(n+k-1,n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^k x^k = 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)a^k = C(n+k-1,n-1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$1/k!$
$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k$

〖Example 3〗 (3) What is the generating function for the sequence $a_k = k^2$?

Solution:

$$a_k = 1 \longleftrightarrow \frac{1}{1-x}$$

$$a_k = k \longleftrightarrow \frac{x}{(1-x)^2}$$

$$a_k = k^2 \longleftrightarrow x\left(\frac{x}{(1-x)^2}\right)' = \frac{x(1+x)}{(1-x)^3}$$

利用公式

$$\begin{aligned}\sum_{k=0}^{\infty} k a_k x^k &= \sum_{k=0}^{\infty} a_k \cdot x \cdot k x^{k-1} \\ &= x\sum_{k=0}^{\infty} a_k (x^k)' \\ &= x\left(\sum_{k=0}^{\infty} a_k x^k\right)' \\ &= xf'(x)\end{aligned}$$

，其中$a_k = 1$

〖Example 3〗 (4) What is the generating function for the sequence $a_k = \sum_{i=1}^{k} i^2$?

Solution:

$$a_k = k^2 \longleftrightarrow x\left(\frac{x}{(1-x)^2}\right)' = \frac{x(1+x)}{(1-x)^3}$$

$$a_k = \sum_{i=1}^{k} i^2 \longleftrightarrow \frac{x(1+x)}{(1-x)^4}$$

$a_k \leftrightarrow G(x), \quad b_k \leftrightarrow F(x)$

利用公式

$$c_k = 1$$

$$\begin{aligned} b_k &= \sum_{i=0}^{k} a_i \\ &= \sum_{i=0}^{k} a_i \times c_{k-i} \end{aligned}$$

$$F(x) = G(x) \cdot \frac{1}{1-x}$$

，其中c_k全为1的生成函数为$\frac{1}{1-x}$

Sequence	Generating function
(1) $C(n,k)$	$\sum_{k=0}^{\infty} C(n,k)x^k = (1+x)^n$
(2) $C(n,k)a^k$	$(1+ax)^n$
(3) 1,1,...,1	$1+x+x^2+\ldots+x^n = \frac{1-x^{n+1}}{1-x}$
(4) 1,1,1,...	$\frac{1}{1-x}$
(5) a^k	$\frac{1}{1-ax}$
(6) $k+1$	$\frac{1}{(1-x)^2}$

Sequence	Generating function
(7) $C(n+k-1,k)$	$(1-x)^{-n}$
(8) $(-1)^k C(n+k-1,k)$	$(1+x)^{-n}$
(9) $C(n+k-1,k)a^k$	$(1-ax)^{-n}$
(10) $\frac{1}{k!}$	e^x
(11) $\frac{(-1)^{k+1}}{k}$	$\ln(1+x)$

Solve Recurrence Relations

EXAMPLE 16 Solve the recurrence relation $a_k = 3a_{k-1}$ for $k = 1, 2, 3, \ldots$ and initial condition $a_0 = 2$.

Extra Examples

Solution: Let $G(x)$ be the generating function for the sequence $\{a_k\}$, that is, $G(x) = \sum_{k=0}^{\infty} a_k x^k$. First note that

$$xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1} x^k.$$

Using the recurrence relation, we see that

$$\begin{aligned} G(x) - 3xG(x) &= \sum_{k=0}^{\infty} a_k x^k - 3 \sum_{k=1}^{\infty} a_{k-1} x^k \\ &= a_0 + \sum_{k=1}^{\infty} (a_k - 3a_{k-1}) x^k \\ &= 2, \end{aligned}$$

because $a_0 = 2$ and $a_k = 3a_{k-1}$. Thus,

$$G(x) - 3xG(x) = (1 - 3x)G(x) = 2.$$

Solving for $G(x)$ shows that $G(x) = 2/(1 - 3x)$. Using the identity $1/(1 - ax) = \sum_{k=0}^{\infty} a^k x^k$, from Table 1, we have

$$G(x) = 2 \sum_{k=0}^{\infty} 3^k x^k = \sum_{k=0}^{\infty} 2 \cdot 3^k x^k.$$

Consequently, $a_k = 2 \cdot 3^k$. ◀

例 17 设一个有效的码字是一个包含偶数个 0 的十进制数字串。令 a_n 表示 n 位有效码字的个数。在 8.1 节的例 4 中我们证明了序列$\{a_n\}$满足递推关系

$$a_n=8a_{n-1}+10^{n-1}$$

且初始条件 $a_1=9$。使用生成函数找出关于 a_n 的显式公式。

解 为了简化关于生成函数的推导，我们通过设置 $a_0=1$ 将序列扩充，当把这个值赋给 a_0 并使用递推关系，就得到 $a_1=8a_0+10^0=8+1=9$，这与初始条件一致。(由于存在一个长为 0 的码字——空串，所以这也是有意义的。)

用 x^n 乘以递推关系的两边得

$$a_nx^n=8a_{n-1}x^n+10^{n-1}x^n$$

设 $G(x)=\sum_{n=0}^{\infty}a_nx^n$ 是序列 a_0，a_1，a_2，…的生成函数。从 $n=1$ 开始对上面的等式两边求和，得到

$$\begin{aligned}G(x)-1&=\sum_{n=1}^{\infty}a_nx^n=\sum_{n=1}^{\infty}(8a_{n-1}x^n+10^{n-1}x^n)\\&=8\sum_{n=1}^{\infty}a_{n-1}x^n+\sum_{n=1}^{\infty}10^{n-1}x^n\\&=8x\sum_{n=1}^{\infty}a_{n-1}x^{n-1}+x\sum_{n=1}^{\infty}10^{n-1}x^{n-1}\\&=8x\sum_{n=0}^{\infty}a_nx^n+x\sum_{n=0}^{\infty}10^nx^n\\&=8xG(x)+x/(1-10x)\end{aligned}$$

其中我们已经使用了例 5 对第二个和进行求值。因此有

$$G(x)-1=8xG(x)+x/(1-10x)$$

求解 $G(x)$得

$$G(x)=\frac{1-9x}{(1-8x)(1-10x)}$$

把等式的右边展开成部分分式(正如在微积分中研究有理函数的积分时所做的)得到

$$G(x)=\frac{1}{2}\left(\frac{1}{1-8x}+\frac{1}{1-10x}\right)$$

两次使用例 5(一次设 $a=8$，一次设 $a=10$)得

$$\begin{aligned}G(x)&=\frac{1}{2}\left(\sum_{n=0}^{\infty}8^nx^n+\sum_{n=0}^{\infty}10^nx^n\right)\\&=\sum_{n=0}^{\infty}\frac{1}{2}(8^n+10^n)x^n\end{aligned}$$

于是，证明了

$$a_n=\frac{1}{2}(8^n+10^n)$$

Counting Problems

$$G(x)=(1+x+x^2+x^3+\dots)^n=\frac{1}{(1-x)^n}$$

例 15 使用生成函数求出从 n 类不同的物体中选择 r 个物体并且每类物体至少选 1 个的方式数。

解 因为我们需要每类物体至少选 1 个，所以这 n 个类中的每类物体都对序列 $\{a_r\}$ 的生成函数 $G(x)$ 贡献了因子 $(x+x^2+x^3+\cdots)$，其中 a_r 是从 n 类不同的物体中选择 r 个物体并且每类物体至少选 1 个的方式数。因此，

$$G(x)=(x+x^2+x^3+\cdots)^n=x^n(1+x+x^2+\cdots)^n=x^n/(1-x)^n$$

使用广义二项式定理和例 8，有

$$\begin{aligned}
G(x) &= x^n/(1-x)^n \\
&= x^n \cdot (1-x)^{-n} \\
&= x^n \sum_{r=0}^{\infty} \binom{-n}{r} (-x)^r \\
&= x^n \sum_{r=0}^{\infty} (-1)^r C(n+r-1,r)(-1)^r x^r \\
&= \sum_{r=0}^{\infty} C(n+r-1,r)x^{n+r} \\
&= \sum_{t=n}^{\infty} C(t-1,t-n)x^t \\
&= \sum_{r=n}^{\infty} C(r-1,r-n)x^r
\end{aligned}$$

8.5 Inclusion–Exclusion

容斥原理

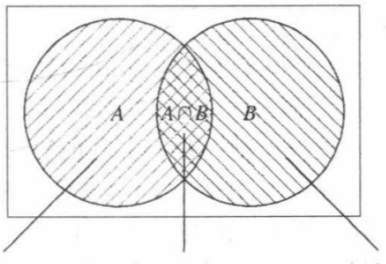
例 2 有多少个不超过 1000 的正整数可以被 7 或 11 整除？

解 设 A 是不超过 1000 且可被 7 整除的正整数的集合，B 是不超过 1000 且可被 11 整除的正整数的集合，那么 $A \cup B$ 是不超过 1000 且可被 7 或 11 整除的正整数的集合，$A \cap B$ 是不超过 1000 且可被 7 和 11 同时整除的正整数的集合。由 4.1 节的例 2，我们知道在不超过 1000 的正整数中有 $\lfloor 1000/7 \rfloor$ 个整数可被 7 整除，并且有 $\lfloor 1000/11 \rfloor$ 个整数可被 11 整除。由于 7 和 11 是互素的，所以被 7 和 11 同时整除的整数就是被 $7 \cdot 11$ 整除的整数。因此，有 $\lfloor 1000/(11 \cdot 7) \rfloor$ 个不超过 1000 的正整数可被 7 和 11 同时整除。于是有

$$\begin{aligned}
|A \cup B| &= |A| + |B| - |A \cap B| \\
&= \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{11} \right\rfloor - \left\lfloor \frac{1000}{7 \cdot 11} \right\rfloor \\
&= 142 + 90 - 12 \\
&= 220
\end{aligned}$$

个正整数不超过 1000 且可被 7 或 11 整除。如图 2 所示。 ◀

$|A \cup B| = |A| + |B| - |A \cap B| = 142 + 90 - 12 = 220$



$|A| = 142$　　$|A \cap B| = 12$　　$|B| = 90$

图 2　不超过 1000 的可被 7 或 11 整除的正整数的集合

向下取整

THEOREM 1 **THE PRINCIPLE OF INCLUSION–EXCLUSION** Let $A_1, A_2, \ldots, A_n$ be finite sets. Then

$$\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup A_n| = &\sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\
&+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.
\end{aligned}$$

8.6 Applications of Inclusion–Exclusion

例 1 $x_1+x_2+x_3=11$ 有多少个整数解？其中 x_1、x_2 和 x_3 是非负整数，且 $x_1\leqslant 3$，$x_2\leqslant 4$，$x_3\leqslant 6$。

解 为了使用容斥原理，令解的性质 P_1 为 $x_1>3$，性质 P_2 为 $x_2>4$，性质 P_3 为 $x_3>6$。满足不等式 $x_1\leqslant 3$、$x_2\leqslant 4$ 以及 $x_3\leqslant 6$ 的解的个数是

$$N(P_1'P_2'P_3') = N - N(P_1) - N(P_2) - N(P_3) + N(P_1P_2) + N(P_1P_3) + N(P_2P_3) - N(P_1P_2P_3)$$

使用与 6.5 节例 5 相同的技术，得到

$$N = \text{解的总数} = C(3+11-1,11) = 78$$
$$N(P_1) = (\text{具有 } x_1 \geqslant 4 \text{ 的解数}) = C(3+7-1,7) = C(9,7) = 36$$
$$N(P_2) = (\text{具有 } x_2 \geqslant 5 \text{ 的解数}) = C(3+6-1,6) = C(8,6) = 28$$
$$N(P_3) = (\text{具有 } x_3 \geqslant 7 \text{ 的解数}) = C(3+4-1,4) = C(6,4) = 15$$
$$N(P_1P_2) = (\text{具有 } x_1 \geqslant 4 \text{ 且 } x_2 \geqslant 5 \text{ 的解数}) = C(3+2-1,2) = C(4,2) = 6$$
$$N(P_1P_3) = (\text{具有 } x_1 \geqslant 4 \text{ 且 } x_3 \geqslant 7 \text{ 的解数}) = C(3+0-1,0) = 1$$
$$N(P_2P_3) = (\text{具有 } x_2 \geqslant 5 \text{ 且 } x_3 \geqslant 7 \text{ 的解数}) = 0$$
$$N(P_1P_2P_3) = (\text{具有 } x_1 \geqslant 4, x_2 \geqslant 5 \text{ 且 } x_3 \geqslant 7 \text{ 的解数}) = 0$$

把这些等式代入关于 $N(P_1'P_2'P_3')$ 的公式，说明满足 $x_1\leqslant 3$、$x_2\leqslant 4$ 以及 $x_3\leqslant 6$ 的解的个数等于

$$N(P_1'P_2'P_3') = 78-36-28-15+6+1+0-0=6$$ ◀

例 2 从 6 元素集合到 3 元素集合有多少个映上函数？

解 假定在陪域中的元素是 b_1，b_2，b_3。设 P_1，P_2，P_3 分别是 b_1，b_2，b_3 不在函数值域中的性质。注意，一个函数是映上的当且仅当它没有性质 P_1、P_2 和 P_3。根据容斥原理得到 6 元素集合到 3 元素集合的映上函数的个数是

$$N(P_1'P_2'P_3') = N - [N(P_1) + N(P_2) + N(P_3)] + [N(P_1P_2) + N(P_1P_3) + N(P_2P_3)] - N(P_1P_2P_3)$$

其中 N 是从 6 元素集合到 3 元素集合的函数总数。我们将对等式右边的每一项求值。

由 6.1 节的例 6 得出 $N=3^6$。注意 $N(P_i)$ 是值域中不含 b_i 的函数的个数。所以，对于定义域中的每个元素的函数值有 2 种选择，从而得到 $N(P_i)=2^6$。此外，这种项有 $C(3,1)$ 个。注意 $N(P_iP_j)$ 是值域中不含 b_i 和 b_j 的函数个数。所以，对于定义域中的每个元素的函数值只有 1 种选择。从而得到 $N(P_iP_j)=1^6=1$。此外，这种项有 $C(3,2)$ 个。还有，注意 $N(P_1P_2P_3)=0$，因为这个项是值域中不含 b_1、b_2 和 b_3 的函数的个数。显然，没有这样的函数。于是，从 6 元素集合到 3 元素集合的映上函数的个数是

$$3^6 - C(3,1)2^6 + C(3,2)1^6 = 729-192+3=540$$ ◀

m个东西分配给n个人，每个人至少有一件东西的方法总数：

THEOREM 1 Let m and n be positive integers with $m \geq n$. Then, there are

$$n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - \cdots + (-1)^{n-1}C(n,n-1)\cdot 1^m$$

onto functions from a set with m elements to a set with n elements.

即映上函数onto function m →n（每个y至少有一个x与之对应）

derangement 错排

THEOREM 2 The number of derangements of a set with n elements is

$$D_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right].$$

即 $\approx n!/e$最接近的整数

9 Relations

9.1 Relations and Their Properties

Definition 1 Let A and B be sets. A *binary relation from A to B* is a subset of $A \times B$.

binary relation from A to B 二元关系

定义 1 设 A 和 B 是集合，一个从 A 到 B 的二元关系是 $A \times B$ 的子集。

换句话说，一个从 A 到 B 的二元关系是集合 R，其中每个有序对的第一个元素取自 A 而第二个元素取自 B。我们使用记号 aRb 表示 $(a, b) \in R$，$a\not{R}b$ 表示 $(a, b) \notin R$。当 (a, b) 属于 R 时，称 a 与 b 有**关系** R。

- 二元关系是一个集合， R包含于A✕B
- n元关系就是A1✕A2✕···✕An的子集

Definition 2 A *relation on a set A* is a relation from A to A.

Properties of binary relations

reflexive 自反性

Definition 3 A relation R on a set A is called *reflexive* if $(a, a) \in R$ for every element $a \in A$.

矩阵主对角线都是1；有向图每个顶点都有环

irreflexive 反自反性

矩阵主对角线都是0；存在既不是自反也不是反自反的关系

symmetric & antisymmetric 对称性和反对称性

Definition 4 A relation R on a set A is called *symmetric* if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$. A relation R on a set A such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called *antisymmetric*.

对称性：矩阵主对角线为对称轴；反对称性，主对角线随意，以主对角线为轴的一边如果是1，另一边必须是0

对称性和反对称性不是互斥的

transitive 传递性

Definition 5 A relation R on a set A is called *transitive* if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

Definition 6 Let R be a relation from a set A to a set B and S a relation from B to a set C. The *composite* of R and S is the relation consisting of ordered pairs (a, c), where $a \in A$, $c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. We denote the composite of R and S by $S \circ R$.

$$\overline{(m_{ij} \wedge m_{jk})} \vee m_{ik} = 1$$

R的n次幂

定义6 设R是从集合A到集合B的关系，S是从集合B到集合C的关系。R与S的合成是由有序对(a, c)的集合构成的关系，其中$a \in A$，$c \in C$，并且存在一个$b \in B$的元素，使得$(a, b) \in R$且$(b, c) \in S$。我们用$S \circ R$表示R与S的合成。

Definition 7 Let R be a relation on the set A. The powers R^n, $n = 1, 2, 3, \ldots$, are defined recursively by

$$R^1 = R \quad \text{and} \quad R^{n+1} = R^n \circ R.$$

定义7 设R是集合A上的关系。R的n次幂R^n($n=1, 2, 3, \cdots$)递归地定义为
$R^1 = R$和$R^{n+1} = R^n \circ R$

THEOREM 1 The relation R on a set A is transitive if and only if $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$.

定理1 集合A上的关系R是传递的，当且仅当对$n=1, 2, 3, \cdots$有$R^n \subseteq R$。

对于n个元素的集合，以下关系有多少种？

REFLEXIVE 自反	IRREFLEXIVE 反自反	SYMMETRIC AND REFLEXIVE 对称+自反
2^{n^2-n}	2^{n^2-n}	$2^{n(n-1)/2}$

SYMMETRIC 对称	ANTISYMMETRIC 反对称	ASYMMETRIC 非对称
$2^{C(n+1,2)} = 2^{n(n+1)/2}$	$2^n * 3^{C(n,2)}$	$3^{C(n,2)}$

$$C(n,2) = n(n-1)/2$$

例 16 n 元素集合上有多少个自反的关系？

解 A 上的关系 R 是 $A\times A$ 的子集。因此，要通过指定 $A\times A$ 中 n^2 个有序对中的每一个是否在 R 中来确定关系。然而，如果 R 是自反的，对于任意 $a\in A$，n 个有序对 (a, a) 中的每一个都必须在 R 中。其他 $n(n-1)$ 个形如 (a, b) 的有序对，$a\neq b$，可能在也可能不在 R 中。因此，由计数的乘积法则可知，存在 $2^{n(n-1)}$ 个自反的关系。[这就是选择具有 $a\neq b$ 的每个元素 (a, b) 是否属于 R 的方式数。]

n个元素的集合A上共有2^{n^2}种二元关系

Example

正整数的整除关系是：reflexive, symmetric, transitive

从m个元素的集合到n个元素的集合的不同关系有2^{mn}个

9.3 Representing Relations

A relation between finite sets can be represented using a zero–one matrix. Suppose that R is a relation from $A = \{a_1, a_2, \ldots, a_m\}$ to $B = \{b_1, b_2, \ldots, b_n\}$. (Here the elements of the sets A and B have been listed in a particular, but arbitrary, order. Furthermore, when $A = B$ we use the same ordering for A and B.) The relation R can be represented by the matrix $\mathbf{M}_R = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 \text{ if } (a_i, b_j) \in R, \\ 0 \text{ if } (a_i, b_j) \notin R. \end{cases}$$

例 2 设 $A=\{a_1, a_2, a_3\}$，$B=\{b_1, b_2, b_3, b_4, b_5\}$。哪些有序对在下面的矩阵所表示的关系 R 中？

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

解 因为 R 是由 $m_{ij}=1$ 的有序对(a_i, b_j)构成的，所以

$$R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}$$ ◀

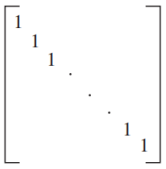
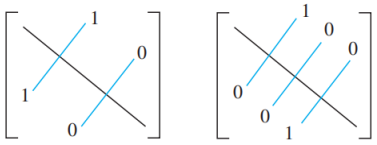


FIGURE 1 **The zero–one matrix for a reflexive relation. (Off diagonal elements can be 0 or 1.)**



(a) Symmetric (b) Antisymmetric

FIGURE 2 **The zero–one matrices for symmetric and antisymmetric relations.**

关系的并和交的矩阵表示是

$$\mathbf{M}_{R_1 \cup R_2} = \mathbf{M}_{R_1} \vee \mathbf{M}_{R_2}, \quad \mathbf{M}_{R_1 \cap R_2} = \mathbf{M}_{R_1} \wedge \mathbf{M}_{R_2}$$

例 4 假设集合 A 上的关系 R_1 和 R_2 由下述矩阵表示，$R_1 \cup R_2$ 和 $R_1 \cap R_2$ 的矩阵表示是什么？

$$\mathbf{M}_{R_1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{M}_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

解 这两个关系的矩阵是

$$\mathbf{M}_{R_1 \cup R_2} = \mathbf{M}_{R_1} \vee \mathbf{M}_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$\mathbf{M}_{R_1 \cap R_2} = \mathbf{M}_{R_1} \wedge \mathbf{M}_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$ ◀

现在我们来考虑怎样确定关系合成的矩阵。这个矩阵可以通过关系矩阵的布尔积(见 2.6 节)得到。特别地，假设 R 是从集合 A 到集合 B 的关系且 S 是从集合 B 到集合 C 的关系。又假设 A、B 和 C 分别有 m、n 和 p 个元素。令 $S \circ R$、R 和 S 的 0-1 矩阵分别为 $\mathbf{M}_{S \circ R}=[t_{ij}]$、$\mathbf{M}_R=[r_{ij}]$、$\mathbf{M}_S=[s_{ij}]$(这些矩阵的大小分别为 $m \times p$、$m \times n$ 和 $n \times p$)。有序对(a_i, c_j)属于 $S \circ R$当且仅当存在元素 b_k 使得(a_i, b_k)属于 R 并且(b_k, c_j)属于 S。由此得出 $t_{ij}=1$，当且仅当存在某个 k 满足 $r_{ik}=s_{kj}=1$。根据布尔积的定义，可得

$$\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S$$

Combining relations

R^{-1}：R的逆，R^{-1} ={(y,x)丨(x,y)∈R}

$$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$$

$$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$$

$$(\overline{R})^{-1} = \overline{R^{-1}}$$

$$(R - S)^{-1} = R^{-1} - S^{-1}$$

$$(A \times B)^{-1} = B \times A$$

A⊙B，两个矩阵的布尔乘积

Boolean product

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

For square zero-one matrices, we can extend Boolean product to *Boolean power*. Denote by $A^{[n]}$ the Boolean product of A with itself n times. Since Boolean products are associative, the order of operations does not matter for a Boolean power.

$$A^{[2]} = A \odot A, \qquad A^{[3]} = A^{[2]} \odot A = A \odot A^{[2]} = A \odot A \odot A, \qquad \text{etc.}$$

$$c_{i,j} = \begin{bmatrix} a_{i,1} & a_{i,2} & a_{i,3} & \cdots & a_{i,n} \end{bmatrix} \odot \begin{bmatrix} b_{1,j} \\ b_{2,j} \\ b_{3,j} \\ \vdots \\ b_{n,j} \end{bmatrix}$$

$$= (a_{i,1} \wedge b_{1,j}) \vee (a_{i,2} \wedge b_{2,j}) \vee \cdots \vee (a_{i,n} \wedge b_{n,j})$$

A⊕B，异或，不一样就出1

$M_{S \circ R} = M_R \cdot M_S = M_R \bigodot M_S$

$R^{n+1} = R^n \circ R$——关系R的幂集

Using the connection matrix

$$\mathbf{M}_R=[r_{ij}]_{m\times n},\mathbf{M}_S=[s_{jk}]_{n\times l}$$

$$\mathbf{M}_{S\circ R}=\mathbf{M}_R\cdot\mathbf{M}_S=[w_{ik}]_{m\times l},\quad w_{ik}=\bigvee_{j=1}^{n}(r_{ij}\wedge s_{jk})$$

$$A=\{a,b\},B=\{1,2,3,4\},C=\{5,6,7\}$$

$$R=\{(a,1),(a,2),(b,3)\},S=\{(2,6),(3,7),(4,5)\}$$

$$\therefore\mathbf{M}_R=\begin{bmatrix}1&1&0&0\\0&0&1&0\end{bmatrix}\qquad\mathbf{M}_s=\begin{bmatrix}0&0&0\\0&1&0\\0&0&1\\1&0&0\end{bmatrix}$$

$$\mathbf{M}_{S\circ R}=\mathbf{M}_R\cdot\mathbf{M}_S=\begin{bmatrix}0&1&0\\0&0&1\end{bmatrix}$$

$$\therefore S\circ R=\{(a,6),(b,7)\}$$

【集合论】关系幂运算 (关系幂运算 | 关系幂运算示例 | 关系幂运算性质)_关系的幂运算-CSDN博客

定义 1　一个有向图由顶点(或结点)集 V 和边(或弧)集 E 组成，其中边集是 V 中元素的有序对的集合。顶点 a 叫作边$(a,\ b)$的始点，而顶点 b 叫作这条边的终点。

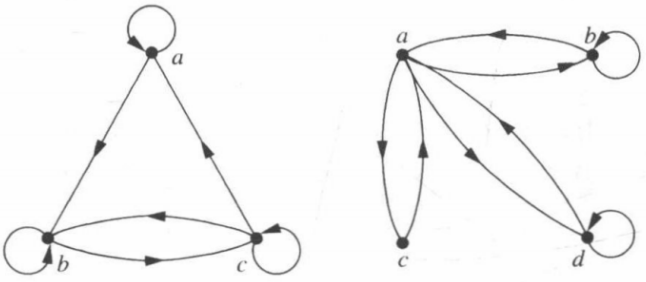
形如$(a,\ a)$的边用一条从顶点 a 到自身的弧表示。这种边叫作**环**。

Definition 1

A *directed graph*, or *digraph*, consists of a set V of *vertices* (or *nodes*) together with a set E of ordered pairs of elements of V called *edges* (or *arcs*). The vertex a is called the *initial vertex* of the edge (a, b), and the vertex b is called the *terminal vertex* of this edge.

An edge of the form (a, a) is represented using an arc from the vertex a back to itself. Such an edge is called a **loop**.

例 10　判断图 6 中的有向图表示的关系，是否为自反的、对称的、反对称的和/或传递的。



a）S_1的有向图　　b）S_2的有向图

图 6　关系 R 和 S 的有向图

解　因为关系 S_1 的有向图的每个顶点都有环，所以它是自反的。S_1 既不是对称的也不是反对称的，因为存在一条从 a 到 b 的边，但没有从 b 到 a 的边，并且 b 和 c 两个方向都有边。最后，S_1 不是传递的，因为从 a 到 b 有边，从 b 到 c 有边，但是从 a 到 c 没有边。

因为在有向图 S_2 中，不是所有的顶点都有环，所以关系 S_2 不是自反的。关系 S_2 是对称的，不是反对称的，因为在不同顶点之间的每条边都伴随着一条方向相反的边。从有向图中不难看出，S_2 不是传递的，因为$(c,\ a)$和$(a,\ b)$属于 S_2，但$(c,\ b)$不属于 S_2。◀

9.4 Closures of Relations

定义 1　设 R 是集合 A 上的关系，若存在关系 R 的具有性质 P 的**闭包**，则此闭包是集合 A 上包含 R 的具有性质 P 的关系 S，并且 S 是每一个包含 R 的具有性质 P 的 $A\times A$ 的子集。

Definition 1 If R is a relation on a set A, then the **closure** of R with respect to **P**, if it exists, is the relation S on A with property **P** that contains R and is a subset of every subset of $A \times A$ containing R with property **P**.

集合 $A=\{1, 2, 3\}$ 上的关系 $R=\{(1, 1), (1, 2), (2, 1), (3, 2)\}$ 不是自反的。我们怎样才能得到一个包含关系 R 的尽可能小的自反关系呢？这可以通过把 $(2, 2)$ 和 $(3, 3)$ 加到 R 中来做到，因为只有它们是不在 R 中的形如 (a, a) 的有序对。这个新关系包含了关系 R。此外，任何包含关系 R 的自反关系一定包含 $(2, 2)$ 和 $(3, 3)$。因为这个关系包含了 R，所以是自反的，并且包含于每一个包含关系 R 的自反关系中，因此它就是关系 R 的**自反闭包**。

Reflective Closures 自反闭包 $r(R)$

【 Corollary 】$R = R \cap I_A$ ⇔ R is a reflexive relation

$\Delta=\{(a, a) \mid a\in A\}$ 是 A 上的**对角关系**。

例 1　整数集上的关系 $R=\{(a, b) \mid a<b\}$ 的自反闭包是什么？

解　R 的自反闭包是

$$R \cup \Delta = \{(a,b) \mid a < b\} \cup \{(a,a) \mid a \in \mathbf{Z}\} = \{(a,b) \mid a \leqslant b\}$$ ◀

$\{1, 2, 3\}$ 上的关系 $\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$ 不是对称的。如何产生一个包含关系 R 的尽可能小的对称关系呢？只需增加 $(2, 1)$ 和 $(1, 3)$，因为只有它们是具有 $(a, b)\in R$ 而 (b, a) 不在 R 中的 (b, a) 对。这个新关系是对称的，且包含了关系 R。此外，任何包含了关系 R 的对称关系一定包含这个新关系，因为任何一个包含关系 R 的对称关系一定包含 $(2, 1)$ 和 $(1, 3)$。因此，这个新关系叫作关系 R 的**对称闭包**。

Symmetric Closures 对称闭包 $s(R)$

【 Corollary 】$R = R \cup R^{-1}$ ⇔ R is a symmetric relation

S 是包含关系 R 的最小的传递关系。这个关系称为 R 的**传递闭包**。

Transitive Closures 传递闭包

定义 2　在有向图 G 中，从 a 到 b 的一条路径是图 G 中一条或多条边的序列 (x_0, x_1)，(x_1, x_2)，(x_2, x_3)，…，(x_{n-1}, x_n)，其中 n 是一个非负整数，$x_0 = a$，$x_n = b$。即一个边的序列，其中一条边的终点和路径中下一条边的始点相同。这条路径记为 x_0，x_1，…，x_{n-1}，x_n，长度为 n。我们把一个为空的边的集合看作从 a 到 a 的长度为 0 的路径。在同一顶点开始和结束的长度 $n \geqslant 1$ 的路径，称为回路或圈。

THEOREM 1

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

定义 3　设 R 是集合 A 上的关系。连通性关系 R^* 由形如 (a, b) 的有序对构成，使得在关系 R 中，从顶点 a 到 b 之间存在一条长度至少为 1 的路径。

Definition 3

Let R be a relation on a set A. The *connectivity relation* R^* consists of the pairs (a, b) such that there is a path of length at least one from a to b in R.

R^* (connectivity relation 连通性关系): the relation consisting of those ordered pairs (a, b) such that there is a path from a to b

THEOREM 2

The transitive closure of a relation R equals the connectivity relation R^*.

传递闭包等于连通性关系 $t(R)=R^*$

LEMMA 1

Let A be a set with n elements, and let R be a relation on A. If there is a path of length at least one in R from a to b, then there is such a path with length not exceeding n. Moreover, when $a \neq b$, if there is a path of length at least one in R from a to b, then there is such a path with length not exceeding $n - 1$.

引理 1　设 A 是含有 n 个元素的集合，R 是集合 A 上的关系。如果 R 中存在一条从 a 到 b 的长度至少为 1 的路径，那么这两点间存在一条长度不超过 n 的路径。此外，当 $a \neq b$ 时，如果在 R 中存在一条从 a 到 b 的长度至少为 1 的路径，那么这两点间存在一条长度不超过 $n-1$ 的路径。

【Theorem】 If $|A| = n$, R is a relation on A, then

$$\exists k, k \leq n, R^* = R \cup R^2 \cup \ldots \cup R^k$$

【Corollary】 If $|A| = n$, then $t(R) = R^* = R \cup R^2 \cup \ldots \cup R^n$

传递闭包的0-1矩阵（矩阵并

定理 3　设 M_R 是定义在 n 个元素集合上的关系 R 的 0-1 矩阵。那么传递闭包 R^* 的 0-1 矩阵是

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}$$

THEOREM 3

Let $\mathbf{M}_R$ be the zero–one matrix of the relation R on a set with n elements. Then the zero–one matrix of the transitive closure R^* is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]} \vee \cdots \vee \mathbf{M}_R^{[n]}.$$

EXAMPLE 7 Find the zero–one matrix of the transitive closure of the relation R where

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Solution: By Theorem 3, it follows that the zero–one matrix of R^* is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]}.$$

Because

$$\mathbf{M}_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

it follows that

$$\mathbf{M}_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

我们可以容易地求出用算法 1 求关系的传递闭包所使用的比特运算次数。计算布尔幂 M_R，$M_R^{[2]}$，…，$M_R^{[n]}$ 需要求出 $n-1$ 个 $n \times n$ 的 0-1 矩阵的布尔积。计算每个布尔积使用 $n^2(2n-1)$ 次比特运算。因此，计算这些乘积使用 $n^2(2n-1)(n-1)$ 次比特运算。

为从 n 个 M_R 的布尔幂求 M_{R^*}，需要求 $n-1$ 个 0-1 矩阵的并。计算每一个并运算使用 n^2 次比特运算。因此，在这部分计算中使用 $(n-1)n^2$ 次比特运算。所以，当使用算法 1 计算定义在 n 个元素的集合上的关系的传递闭包的矩阵时，需要用 $n^2(2n-1)(n-1)+(n-1)n^2 = 2n^3(n-1)$ 次比特运算，即该算法复杂度为 $O(n^4)$。本节后面部分将要描述一个更有效的求传递闭包的算法。

Warshall's algorithm 沃舍尔算法

use the concept of the **interior vertices** of a path 用到了一条路径内部顶点的概念

内部顶点：一条路径去掉起点和终点，如acdafbj的内部顶点cdafb

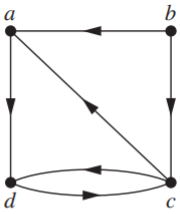


FIGURE 3
The directed graph of the relation *R*.

例 8 设 R 是一个关系，它的有向图如图 3 所示。设 a，b，c，d 是集合元素的排列。求矩阵 $\boldsymbol{W}_0$，$\boldsymbol{W}_1$，$\boldsymbol{W}_2$，$\boldsymbol{W}_3$，$\boldsymbol{W}_4$。矩阵 $\boldsymbol{W}_4$ 是关系 R 的传递闭包。

解 令 $v_1=a$，$v_2=b$，$v_3=c$，$v_4=d$。$\boldsymbol{W}_0$ 是这个关系的矩阵，于是

$$\boldsymbol{W}_0=\begin{bmatrix}0&0&0&1\\1&0&1&0\\1&0&0&1\\0&0&1&0\end{bmatrix}$$

<矩阵中

$a_{ij}=0,1$表示有从i到j的路径

$\mathbf{W}_1$ has 1 as its (i, j)th entry if there is a path from v_i to v_j that has only $v_1 = a$ as an interior vertex. Note that all paths of length one can still be used because they have no interior vertices. Also, there is now an allowable path from b to d, namely, b, a, d. Hence,

$$\mathbf{W}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

$\mathbf{W}_2$ has 1 as its (i, j)th entry if there is a path from v_i to v_j that has only $v_1 = a$ and/or $v_2 = b$ as its interior vertices, if any. Because there are no edges that have b as a terminal vertex, no new paths are obtained when we permit b to be an interior vertex. Hence, $\mathbf{W}_2 = \mathbf{W}_1$.

$\mathbf{W}_3$ has 1 as its (i, j)th entry if there is a path from v_i to v_j that has only $v_1 = a$, $v_2 = b$, and/or $v_3 = c$ as its interior vertices, if any. We now have paths from d to a, namely, d, c, a, and from d to d, namely, d, c, d. Hence,

$$\mathbf{W}_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

Finally, $\mathbf{W}_4$ has 1 as its (i, j)th entry if there is a path from v_i to v_j that has $v_1 = a$, $v_2 = b$, $v_3 = c$, and/or $v_4 = d$ as interior vertices, if any. Because these are all the vertices of the graph, this entry is 1 if and only if there is a path from v_i to v_j. Hence,

$$\mathbf{W}_4 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

This last matrix, $\mathbf{W}_4$, is the matrix of the transitive closure. ◀

LEMMA 2 Let $\mathbf{W}_k = [w_{ij}^{[k]}]$ be the zero–one matrix that has a 1 in its (i, j)th position if and only if there is a path from v_i to v_j with interior vertices from the set $\{v_1, v_2, \ldots, v_k\}$. Then

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]}),$$

whenever i, j, and k are positive integers not exceeding n.

引理 2　设 $\boldsymbol{W}_k = [w_{ij}^{[k]}]$ 是 0-1 矩阵，它的 (i, j) 位置为 1 当且仅当存在一条从 v_i 到 v_j 的路径，其内部顶点取自集合 $\{v_1, v_2, \cdots, v_k\}$，那么

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]})$$

那么其中 i，j 和 k 是不超过 n 的正整数。

k确定的情况下，原先矩阵是1的还是1，只要检查第k列是1的行中的0有没有变化

total number of bit operations（时间复杂度

沃舍尔算法的计算复杂度可以很容易地以比特运算的次数进行计算。使用引理 2，从项 $w_{ij}^{[k-1]}$、$w_{ik}^{[k-1]}$ 和 $w_{kj}^{[k-1]}$ 求出项 $w_{ij}^{[k]}$ 需要 2 次比特运算。从 $\boldsymbol{W}_{k-1}$ 求出 $\boldsymbol{W}_k$ 的所有 n^2 个项需要 $2n^2$ 次比特运算。因为沃舍尔算法从 $\boldsymbol{W}_0 = \boldsymbol{M}_R$ 开始，所以计算 n 个 0-1 矩阵的序列 $\boldsymbol{W}_1$，$\boldsymbol{W}_2$，$\cdots$，$\boldsymbol{W}_n = \boldsymbol{M}_{R^*}$，使用的比特运算总次数是 $n \cdot 2n^2 = 2n^3$。

9.5 Equivalence Relations

Equivalence Relations 等价关系

equivalent 等价: if R is an equivalence relation, a is equivalent to b if `aRb`

Definition 1 A relation on a set A is called an *equivalence relation* if it is reflexive, symmetric, and transitive.

等价关系：自反+对称+传递

Definition 2 Two elements a and b that are related by an equivalence relation are called *equivalent*. The notation $a \sim b$ is often used to denote that a and b are equivalent elements with respect to a particular equivalence relation.

例 2 设 R 是定义在实数集上的关系，满足 aRb 当且仅当 $a-b$ 是整数。R 是等价关系吗？

解 因为对所有的实数 a，$a-a=0$ 是整数，即对所有的实数 a，有 aRa，因此 R 是自反的。假设 aRb，那么 $a-b$ 是整数，所以 $b-a$ 也是整数。因此有 bRa。由此，R 是对称的。如果 aRb 且 bRc，那么 $a-b$ 和 $b-c$ 是整数，所以 $a-c=(a-b)+(b-c)$ 也是整数。因此 aRc。所以，R 是传递的。综上所述，R 是等价关系。 ◀

- 模m同余是等价关系 R={(a,b) | a≡b(mod m), a,b∈Z}

EXAMPLE 3 **Congruence Modulo m** Let m be an integer with $m > 1$. Show that the relation

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

is an equivalence relation on the set of integers.

Solution: Recall from Section 4.1 that $a \equiv b \pmod{m}$ if and only if m divides $a - b$. Note that $a - a = 0$ is divisible by m, because $0 = 0 \cdot m$. Hence, $a \equiv a \pmod{m}$, so congruence modulo m is reflexive. Now suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m, so $a - b = km$, where k is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$. Hence, congruence modulo m is symmetric. Next, suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then m divides both $a - b$ and $b - c$. Therefore, there are integers k and l with $a - b = km$ and $b - c = lm$. Adding these two equations shows that $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Thus, $a \equiv c \pmod{m}$. Therefore, congruence modulo m is transitive. It follows that congruence modulo m is an equivalence relation. ◀

Equivalence Classes 等价类

定义 3 设 R 是定义在集合 A 上的等价关系。与 A 中的一个元素 a 有关系的所有元素的集合叫作 a 的等价类。A 的关于 R 的等价类记作 $[a]_R$。当只考虑一个关系时，我们将省去下标 R 并把这个等价类写作 $[a]$。

换句话说，如果 R 是定义在集合 A 上的等价关系，则元素 a 的等价类是

$$[a]_R = \{s \mid (a,s) \in R\}$$

如果 $b \in [a]_R$，b 叫作这个等价类的**代表元**。一个等价类的任何元素都可以作为这个类的代表元。也就是说，选择特定元素作为一个类的代表元没有特殊要求。

representative代表元

$[a]_R$ **(equivalence class of a with respect to R)** 等价类**:** the set of all elements of A that are equivalent to a

例 9 对于模 4 同余关系，0 和 1 的等价类是什么？

解 0 的等价类包含使得 $a \equiv 0 \pmod 4$ 的所有整数 a。这个类中的整数是能被 4 整除的那些整数。因此，对于这个关系，0 的等价类是

$$[0] = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$$

1 的等价类包含使得 $a \equiv 1 \pmod 4$ 的所有整数 a。这个类中的整数是被 4 除时余数为 1 的那些整数。因此，对于这个关系，1 的等价类是

$$[1] = \{\cdots, -7, -3, 1, 5, 9, \cdots\}$$

2 的等价类包含使得 $a \equiv 2 \pmod 4$ 的所有整数 a。这个类中的整数是被 4 除时余数为 2 的那些整数。因此，对于这个关系，2 的等价类是

$$[2] = \{\cdots, -6, -2, 2, 6, 10, \cdots\}$$

3 的等价类包含使得 $a \equiv 3 \pmod 4$ 的所有整数 a。这个类中的整数是被 4 除时余数为 3 的那些整数。因此，对于这个关系，3 的等价类是

$$[3] = \{\cdots, -5, -1, 3, 7, 11, \cdots\}$$

注意，每一个整数都恰好在四个等价类的一个中，并且整数 n 在包含 n **mod** 4 的类中。◀

在例 9 中找到了 0，1，2 和 3 关于模 4 同余的等价类。用任何正整数 m 代替 4，很容易把例 9 加以推广。模 m 同余关系的等价类叫作**模 *m* 同余类**。整数 a 模 m 的同余类记作 $[a]_m$，满足 $[a]_m = \{\cdots, a-2m, a-m, a, a+m, a+2m, \cdots\}$。例如，从例 9 得出 $[0]_4 = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$ 和 $[1]_4 = \{\cdots, -7, -3, 1, 5, 9, \cdots\}$。

[a]m (congruence class modulo m)模m的同余类

THEOREM 1 Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:

(*i*) aRb (*ii*) $[a] = [b]$ (*iii*) $[a] \cap [b] \neq \emptyset$

THEOREM 2 Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set S, there is an equivalence relation R that has the sets A_i, $i \in I$, as its equivalence classes.

定理 2 设 R 是定义在集合 S 上的等价关系。那么 R 的等价类构成 S 的划分。反过来，给定集合 S 的划分 $\{A_i \mid i \in I\}$，则存在一个等价关系 R，它以集合 $A_i (i \in I)$ 作为它的等价类。

例 13 说明了怎样从一个划分构造一个等价关系。

例 13 $A_1=\{1, 2, 3\}$，$A_2=\{4, 5\}$，$A_3=\{6\}$ 是例 12 给出的集合 $S=\{1, 2, 3, 4, 5, 6\}$ 的划分，列出这个划分所产生的等价关系 R 中的有序对。

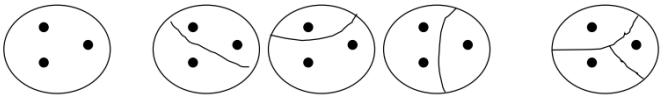
解 划分中的子集是 R 的等价类。有序对 $(a, b) \in R$，当且仅当 a 和 b 在划分的同一个子集中。由于 $A_1=\{1, 2, 3\}$ 是一个等价类，所以有序对 $(1, 1)$，$(1, 2)$，$(1, 3)$，$(2, 1)$，$(2, 2)$，$(2, 3)$，$(3, 1)$，$(3, 2)$，$(3, 3)$ 属于 R；由于 $A_2=\{4, 5\}$ 是一个等价类，所以有序对 $(4, 4)$，$(4, 5)$，$(5, 4)$，$(5, 5)$ 也属于 R；最后，由于 $\{6\}$ 是一个等价类，所以有序对 $(6, 6)$ 属于 R。此外没有其他的有序对属于 R。 ◀

等价关系的数量：partition of a set 有一个分化就有一个等价关系

|A|=3. How many different equivalence relations on the set A are there?

Solution:

an equivalence relation on a set A $\leftrightarrow$ a partition of A



- 5个（3个元素集合的等价关系有5个）

【 Theorem 3】 If R_1, R_2 are equivalence relations on A, then $R_1 \cap R_2$ is equivalence relations on A.

【 Theorem 4】 If R_1, R_2 are equivalence relations on A, then $R_1 \cup R_2$ is reflexive and symmetric relation on A.

【 Theorem 】 If R_1, R_2 are equivalence relations on A, then $(R_1 \cup R_2)^*$ is an equivalence relation on A.

Questions

1 R={(a,b) | a≡b(mod m), a,b∈Z}, $pr(Z) = [0]_m, [1]_m, \cdots, [m-1]_m$

2 If |A|=n, the p(n)=?

p(n): the number of different equivalence relations on a set with n elements

> $p(n) = B_n = \sum_{k=0}^{n} C(n,k)$

9.6 Partial Orderings

Partial Orderings

poset (S, R)偏序集: a set S and a partial ordering R on this set

Definition 1 A relation R on a set S is called a *partial ordering* or *partial order* if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a *partially ordered set*, or *poset*, and is denoted by (S, R). Members of S are called *elements* of the poset.

偏序：自反+反对称+传递

例 3 证明：包含关系⊆是定义在集合 S 的幂集上的偏序。

解 因为只要 A 是 S 的子集，就有 $A\subseteq A$，所以⊆是自反的。因为 $A\subseteq B$ 和 $B\subseteq A$ 蕴含 $A=B$，所以它是反对称的。最后，因为 $A\subseteq B$ 和 $B\subseteq C$ 蕴含 $A\subseteq C$，所以⊆是传递的。因此，⊆是 $P(S)$ 上的偏序，且 $(P(S), \subseteq)$ 是偏序集。 ◀

在不同的偏序集中，会使用不同的符号表示偏序，如≤、⊆和|。然而，我们需要一个符号用来表示任意一个偏序集中的序关系。通常，在一个偏序集 (S, R) 中，记号 $a\leqslant b$ 表示 $(a, b)\in R$。使用这个记号是由于“小于或等于”关系是偏序关系的范例，而且符号≤和≤很相似。(注意符号≤用来表示任意偏序集中的关系，并不仅仅是“小于或等于”关系。)记号 $a<b$ 表示 $a\leqslant b$，但 $a\neq b$。如果 $a<b$，我们说“a 小于 b”或“b 大于 a”。

当 a 与 b 是偏序集 $(S, \leqslant)$ 的元素时，不一定有 $a\leqslant b$ 或 $b\leqslant a$。例如，在 $(\mathcal{P}(\mathbf{Z}), \subseteq)$ 中，{1，2}与{1，3}没有关系，反之亦然，因为没有一个集合被另一个集合包含。类似地，在 $(\mathbf{Z}^+, |)$ 中，2 与 3 没有关系，3 与 2 也没有关系，因为 $2\nmid 3$ 且 $3\nmid 2$。由此得到定义 2。

Example:

(1) $R_1 = \{(a,b) \mid a \le b, a,b \in Z\}$ $(Z, \le)$

(2) $R_2 = \{(a,b) \mid a \mid b, a,b \in Z^+\}$ $(Z^+, |)$

(3) $R_3 = \{(s_1,s_2) \mid s_1 \subseteq s_2, s_1,s_2 \in P(S)\}$ $(P(S), \subseteq)$

Definition 2 The elements a and b of a poset $(S, \preccurlyeq)$ are called *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$. When a and b are elements of S such that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, a and b are called *incomparable*.

定义 2 偏序集 $(S, \leqslant)$ 中的元素 a 和 b 称为可比的，如果 $a\leqslant b$ 或 $b\leqslant a$。当 a 和 b 是 S 中的元素并且既没有 $a\leqslant b$，也没有 $b\leqslant a$，则称 a 与 b 是不可比的。

≤: less than or equal to

EXAMPLE 5 In the poset $(\mathbf{Z}^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?

Solution: The integers 3 and 9 are comparable, because $3 \mid 9$. The integers 5 and 7 are incomparable, because $5 \nmid 7$ and $7 \nmid 5$. ◀

The adjective "partial" is used to describe partial orderings because pairs of elements may be incomparable. When every two elements in the set are comparable, the relation is called a **total ordering**.

totally (or linearly) ordered set 全序（线序）集：一个偏序集中每对元素都是可比的

Definition 3 If $(S, \preccurlyeq)$ is a poset and every two elements of S are comparable, S is called a *totally ordered* or *linearly ordered set*, and $\preccurlyeq$ is called a *total order* or a *linear order*. A totally ordered set is also called a *chain*.

例 6 偏序集$(\mathbf{Z}, \leqslant)$是全序集，因为只要 a 和 b 是整数，就有 $a \leqslant b$ 或 $b \leqslant a$。 ◀

Well-ordered良序

Definition 4 $(S, \preccurlyeq)$ is a *well-ordered set* if it is a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of S has a least element.

良序归纳定理

THEOREM 1 **THE PRINCIPLE OF WELL-ORDERED INDUCTION** Suppose that S is a well-ordered set. Then $P(x)$ is true for all $x \in S$, if

INDUCTIVE STEP: For every $y \in S$, if $P(x)$ is true for all $x \in S$ with $x \prec y$, then $P(y)$ is true.

证明 假设 $P(x)$不对所有的 $x \in S$ 为真。那么存在一个元素 $y \in S$ 使得 $P(y)$为假。于是集合 $A = \{x \in S \mid P(x)$为假$\}$是非空的。因为 S 是良序的，所以集合 A 有最小元素 a。根据 a 是选自 A 的最小元素，我们知道对所有的 $x \in S$ 且 $x \prec a$ 都有 $P(x)$为真。由归纳步骤可以推出 $P(a)$为真。这个矛盾就证明了 $P(x)$必须对所有 $x \in S$ 为真。 ◀

评注 使用良序归纳法进行证明时，不需要基础步骤。因为若 x_0 是良序集的最小元素，由归纳步骤可知 $P(x_0)$为真。因为不存在 $x \in S$ 且 $x \prec x_0$，所以(使用空证明)$P(x)$对所有 $x \in S$ 且 $x \prec x_0$ 为真。

Lexicographic ordering 字典顺序

Hasse diagram 哈塞图

表示的是偏序

例 12 画出表示{1，2，3，4，6，8，12}上的偏序{(a，b)|a 整除 b}的哈塞图。

解 从这个偏序的有向图开始，如图 3a 所示。移走所有的环，如图 3b 所示。然后删除所有由传递性可以得到的边。这些边是(1，4)、(1，6)、(1，8)、(1，12)、(2，8)、(2，12)和(3，12)。排列所有的边使得方向向上，并且删除所有的箭头得到哈塞图。结果如图 3c 所示。 ◀

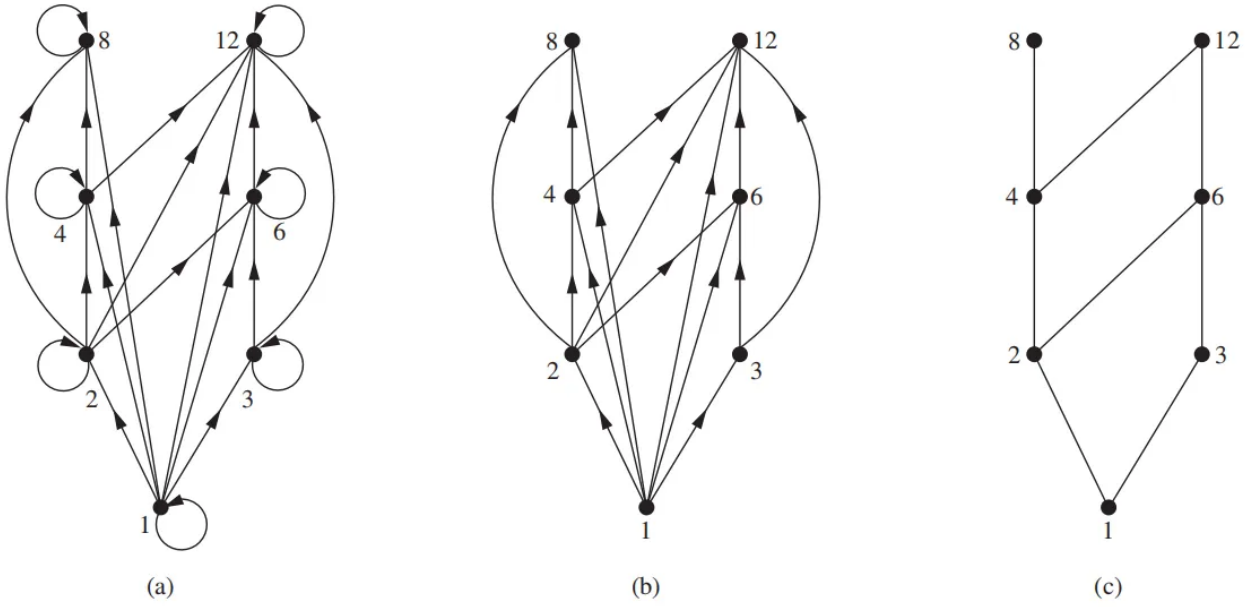


FIGURE 3 **Constructing the Hasse diagram of ({1, 2, 3, 4, 6, 8, 12}, |).**

EXAMPLE 13 Draw the Hasse diagram for the partial ordering $\{(A, B) \mid A \subseteq B\}$ on the power set $P(S)$, where $S = \{a, b, c\}$.

Solution: The Hasse diagram for this partial ordering is obtained from the associated digraph by deleting all the loops and all the edges that occur from transitivity, namely, $(\emptyset, \{a, b\})$, $(\emptyset, \{a, c\})$, $(\emptyset, \{b, c\})$, $(\emptyset, \{a, b, c\})$, $(\{a\}, \{a, b, c\})$, $(\{b\}, \{a, b, c\})$, and $(\{c\}, \{a, b, c\})$. Finally, all edges point upward, and arrows are deleted. The resulting Hasse diagram is illustrated in Figure 4. ◀

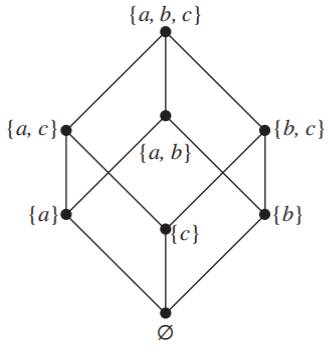


FIGURE 4 **The Hasse diagram of (P({a, b, c}), ⊆).**

Chain and antichain

【Definition】$(A,\leq)$ is a poset. $B \subseteq A$, if $(B,\leq)$ is a totally ordered set, the B is called a *chain* of $(A,\leq)$.

The length of chain: |B|, B is a definite set,

$B \subseteq A$, if $\forall a,b \in B(a \neq b),(a,b) \notin R,(b,a) \notin R$ the *B* is called a ***antichain*** of $(A,\leq)$.

Maximal and Minimal Elements 极大元与极小元

Elements of posets that have certain extremal properties are important for many applications. An element of a poset is called maximal if it is not less than any element of the poset. That is, a is **maximal** in the poset $(S, \preccurlyeq)$ if there is no $b \in S$ such that $a \prec b$. Similarly, an element of a poset is called minimal if it is not greater than any element of the poset. That is, a is **minimal** if there is no element $b \in S$ such that $b \prec a$. Maximal and minimal elements are easy to spot using a Hasse diagram. They are the "top" and "bottom" elements in the diagram.

Sometimes there is an element in a poset that is greater than every other element. Such an element is called the greatest element. That is, a is the **greatest element** of the poset $(S, \preccurlyeq)$ if $b \preccurlyeq a$ for all $b \in S$. The greatest element is unique when it exists [see Exercise 40(a)]. Likewise, an element is called the least element if it is less than all the other elements in the poset. That is, a is the **least element** of $(S, \preccurlyeq)$ if $a \preccurlyeq b$ for all $b \in S$. The least element is unique when it exists [see Exercise 40(b)].

EXAMPLE 15 Determine whether the posets represented by each of the Hasse diagrams in Figure 6 have a greatest element and a least element.

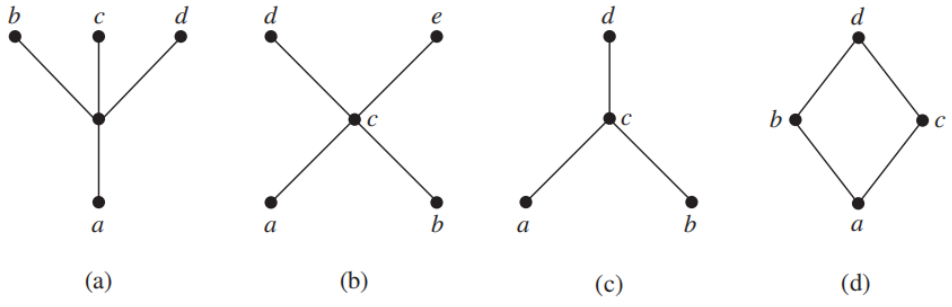


FIGURE 6 **Hasse diagrams of four posets.**

Solution: The least element of the poset with Hasse diagram (a) is a. This poset has no greatest element. The poset with Hasse diagram (b) has neither a least nor a greatest element. The poset with Hasse diagram (c) has no least element. Its greatest element is d. The poset with Hasse diagram (d) has least element a and greatest element d. ◀

例 16 设 S 是集合。确定偏序集 $(\mathcal{P}(S), \subseteq)$ 中是否存在最大元与最小元。

解 最小元是空集，因为对于 S 的任何子集 T，有 $\varnothing \subseteq T$。集合 S 是这个偏序集的最大元，因为只要 T 是 S 的子集，就有 $T \subseteq S$。◀

例 17 在偏序集 $(\mathbf{Z}^+, |)$ 中是否存在最大元和最小元？

解 1 是最小元，因为只要 n 是正整数，就有 $1 | n$。因为没有被所有正整数整除的整数，所以不存在最大元。◀

上界和下界（可以有多个）

Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset A of a poset $(S, \preccurlyeq)$. If u is an element of S such that $a \preccurlyeq u$ for all elements $a \in A$, then u is called an **upper bound** of A. Likewise, there may be an element less than or equal to all the elements in A. If l is an element of S such that $l \preccurlyeq a$ for all elements $a \in A$, then l is called a **lower bound** of A.

最小上界&最大下界（最多只能有1个）

EXAMPLE 18 Find the lower and upper bounds of the subsets $\{a, b, c\}$, $\{j, h\}$, and $\{a, c, d, f\}$ in the poset with the Hasse diagram shown in Figure 7.

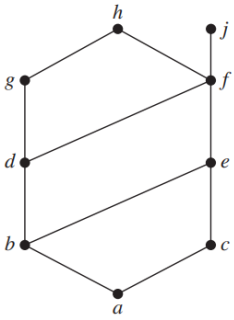


FIGURE 7 The Hasse diagram of a poset.

Solution: The upper bounds of $\{a, b, c\}$ are e, f, j, and h, and its only lower bound is a. There are no upper bounds of $\{j, h\}$, and its lower bounds are a, b, c, d, e, and f. The upper bounds of $\{a, c, d, f\}$ are f, h, and j, and its lower bound is a. ◀

The element x is called the **least upper bound** of the subset A if x is an upper bound that is less than every other upper bound of A. Because there is only one such element, if it exists, it makes sense to call this element *the* least upper bound [see Exercise 42(a)]. That is, x is the least upper bound of A if $a \preccurlyeq x$ whenever $a \in A$, and $x \preccurlyeq z$ whenever z is an upper bound of A. Similarly, the element y is called the **greatest lower bound** of A if y is a lower bound of A and $z \preccurlyeq y$ whenever z is a lower bound of A. The greatest lower bound of A is unique if it exists [see Exercise 42(b)]. The greatest lower bound and least upper bound of a subset A are denoted by $\text{glb}(A)$ and $\text{lub}(A)$, respectively.

lattice 格

Definition: A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**.

如果一个偏序集的每对元素都有最小上界和最大下界，就称这个偏序集为**格**。

例 21 确定图 8 中的每个哈塞图表示的偏序集是否是格。

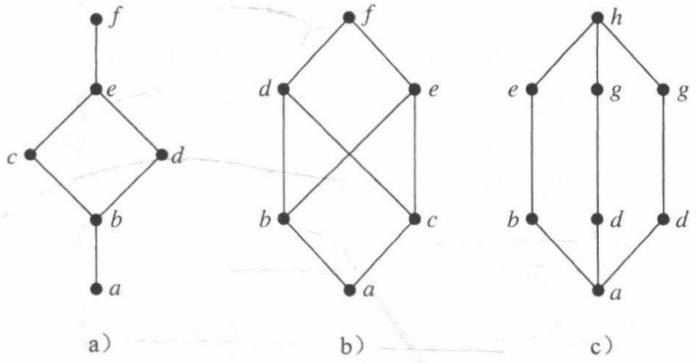


图 8　三个偏序集的哈塞图

解　在图 8a 和图 8c 中的哈塞图表示的偏序集是格，因为在每个偏序集中每对元素都有最小上界和最大下界，读者可自行验证。另一方面，图 8b 所示的哈斯图表示的偏序集不是格，因为元素 b 和 c 没有最小上界。注意，虽然 d、e 和 f 都是上界，但这 3 个元素中的任何一个在这个偏序集中的顺序都不出现在其他 2 个之前。 ◀

- 图b中d和e同为b、c最小上界，不唯一，最小上界最多只能有1个

例 22 偏序集$(\mathbf{Z}^+, |)$是格吗？

解　设 a 和 b 是两个正整数。这两个整数的最小上界和最大下界分别是它们的最小公倍数和最大公约数，读者应自行验证。因此这个偏序集是格。 ◀

例 23 确定偏序集$(\{1, 2, 3, 4, 5\}, |)$和$(\{1, 2, 4, 8, 16\}, |)$是否为格。

解　因为 2 和 3 在$(\{1, 2, 3, 4, 5\}, |)$中没有上界，所以它们当然没有最小上界。因此第一个偏序集不是格。

第二个偏序集中的每两个元素都有最小上界和最大下界。在这个偏序集中两个元素的最小上界是它们中间较大的元素，而两个元素的最大下界是它们中间较小的元素。读者应自行验证。因此第二个偏序集是格。 ◀

- 每一个全序集（totally ordered set）都是格
- $(Z^+, |)$ & $(P(s), \subseteq)$ 是格

Topological Sorting 拓扑排序

我们从定义开始。如果只要 aRb 就有 $a \preccurlyeq b$，则称一个全序 $\preccurlyeq$ 与偏序 R 是**相容的**。从一个偏序构造一个相容的全序称为**拓扑排序**[⊖]。我们需要使用引理 1。

引理 1　每个有穷非空偏序集$(S, \preccurlyeq)$至少有一个极小元。

LEMMA 1　Every finite nonempty poset $(S, \preccurlyeq)$ has at least one minimal element.

例 26 找出与偏序集$(\{1, 2, 4, 5, 12, 20\}, |)$相容的一个全序。

解 第一步是选择一个极小元。这个元素一定是 1，因为它是唯一的极小元。下一步选择$(\{2, 4, 5, 12, 20\}, |)$的一个极小元。在这个偏序集中有两个极小元，即 2 和 5。我们选择 5。剩下的元素是{2，4，12，20}。在这一步，唯一的极小元是 2。下一步选择 4，因为它是$(\{4, 12, 20\}, |)$的唯一极小元。因为 12 和 20 都是$(\{12, 20\}, |)$的极小元，下一步选哪一个都可以。我们选 20，只剩下 12 作为最后的元素。这产生了全序

$$1 \prec 5 \prec 2 \prec 4 \prec 20 \prec 12$$

这个排序算法所使用的步骤在图 9 中给出。 ◀

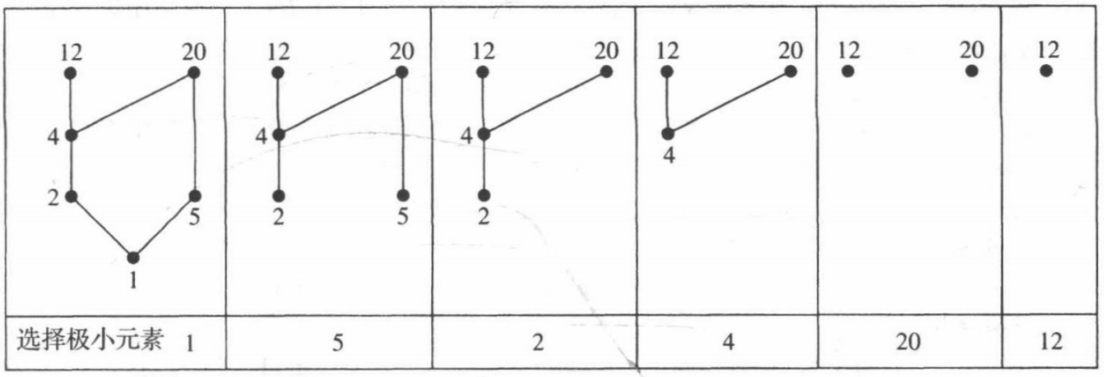


图 9 $(\{1, 2, 4, 5, 12, 20\}, |)$的拓扑排序

例 27 一个计算机公司的开发项目需要完成 7 个任务。其中某些任务只能在其他任务结束后才能开始。考虑如下建立任务上的偏序，如果任务 Y 在 X 结束后才能开始，则任务 $X \prec$ 任务 Y。这 7 个任务对应于这个偏序的哈塞图如图 10 所示。求一个任务的执行顺序，使得能够完成这个项目。

解 可以通过执行一个拓扑排序得到 7 个任务的排序。排序的步骤显示在图 11 中。这个排序的结果，$A \prec C \prec B \prec E \prec F \prec D \prec G$，给出了一种可行的任务次序。 ◀

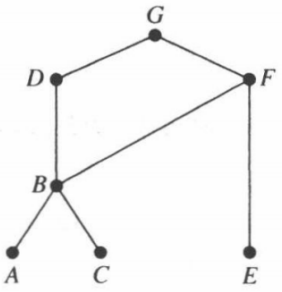


图 10 关于 7 个任务的哈塞图

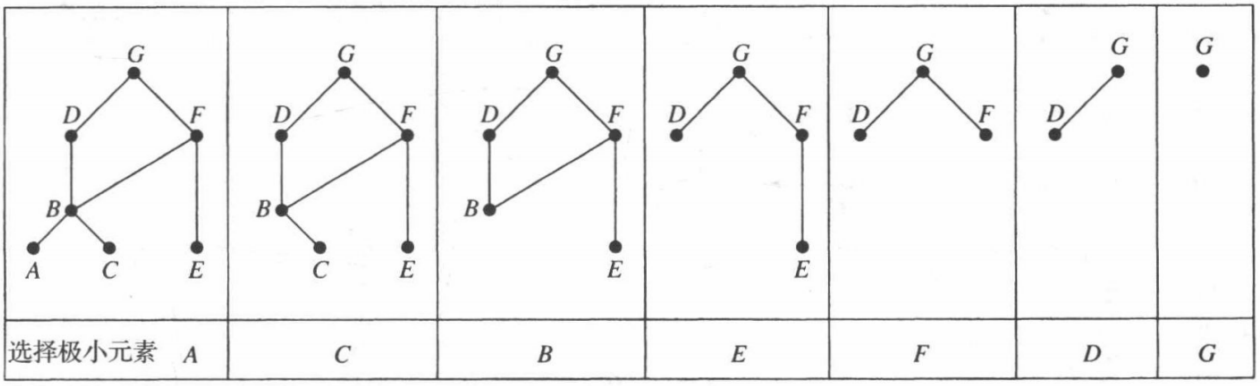


图 11 任务的拓扑排序

10 Graphs

10.1 Graphs and Graph Models

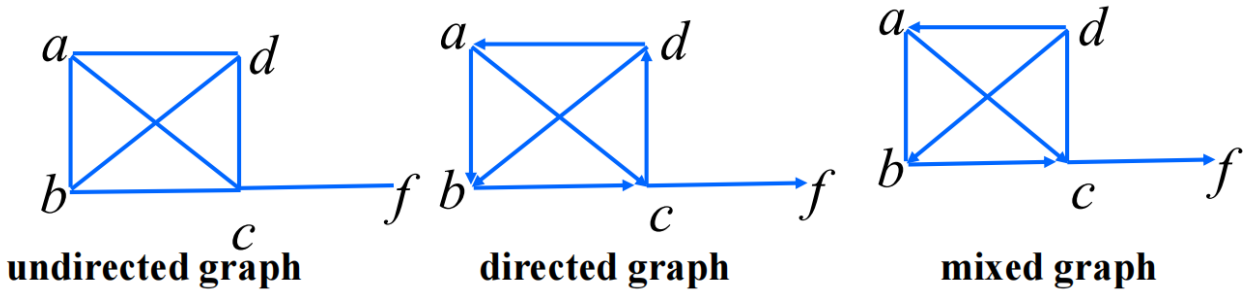
Definition 1 A *graph* $G = (V, E)$ consists of V, a nonempty set of *vertices* (or *nodes*) and E, a set of *edges*. Each edge has either one or two vertices associated with it, called its *endpoints*. An edge is said to *connect* its endpoints.

finite graph 有限图
A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices is called a **simple graph**.
简单图没有环，无多重边，无向

Graphs that may have **multiple edges** connecting the same vertices are called **multigraphs**. 可能会有**多重边**连接同一对顶点的图称为**多重图**。

loops: edges that connect a vertex to itself

undirected graphs 无向图: a graph with undirected edges.
directed graph 有向图 : a graph with directed edges.
mixed graph: a graph with both directed and undirected edges.



undirected graph can be classified into:
Simple graph 简单图: A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices.
Multigraph 多重图: Graphs that may have multiple edges connecting the same vertices.
Pseudograph 伪图: Graphs that may include loops, and possibly multiple edges connecting the same pair of vertices.

Definition 2

A *directed graph* (or *digraph*) (V, E) consists of a nonempty set of vertices V and a set of *directed edges* (or *arcs*) E. Each directed edge is associated with an ordered pair of vertices. The directed edge associated with the ordered pair (u, v) is said to *start* at u and *end* at v.

定义 2　有向图(V, E)由一个非空顶点集 V 和一个有向边(或弧)集 E 组成。每条有向边与一个顶点有序对相关联。我们称与有序对(u, v)相关联的有向边开始于 u、结束于 v。

When a directed graph has no loops and has no multiple directed edges, it is called a **simple directed graph.**

TABLE 1 Graph Terminology.

Type	*Edges*	*Multiple Edges Allowed?*	*Loops Allowed?*
Simple graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes
Simple directed graph	Directed	No	No
Directed multigraph	Directed	Yes	Yes
Mixed graph	Directed and undirected	Yes	Yes

10.2 Graph Terminology and Special Types of Graphs

Basic Terminology

Definition 1 Two vertices u and v in an undirected graph G are called *adjacent* (or *neighbors*) in G if u and v are endpoints of an edge e of G. Such an edge e is called *incident with* the vertices u and v and e is said to *connect* u and v.

为了描述和图中某个特定的顶点相邻接的顶点的集合，会使用下面的术语。

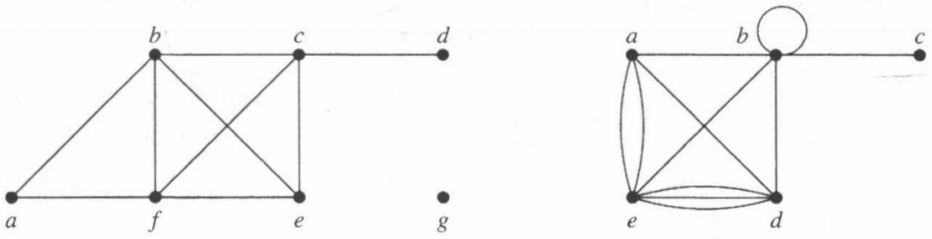
Definition 2 The set of all neighbors of a vertex v of $G = (V, E)$, denoted by $N(v)$, is called the *neighborhood* of v. If A is a subset of V, we denote by $N(A)$ the set of all vertices in G that are adjacent to at least one vertex in A. So, $N(A) = \bigcup_{v \in A} N(v)$.

为了反映有多少条边和一个顶点相关联，有下述的定义。

Definition 3 The *degree of a vertex in an undirected graph* is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. The degree of the vertex v is denoted by $\deg(v)$.

例 1 如图 1 所示，图 G 和图 H 的顶点的度和顶点的邻居是什么？

解 在 G 中，$\deg(a)=2$，$\deg(b)=\deg(c)=\deg(f)=4$，$\deg(d)=1$，$\deg(e)=3$，$\deg(g)=0$。这些顶点的邻居是 $N(a)=\{b, f\}$，$N(b)=\{a, c, e, f\}$，$N(c)=\{b, d, e, f\}$，$N(d)=\{c\}$，$N(e)=\{b, c, f\}$，$N(f)=\{a, b, c, e\}$和 $N(g)=\varnothing$。在 H 中，$\deg(a)=4$，$\deg(b)=\deg(e)=6$，$\deg(c)=1$，$\deg(d)=5$。这些顶点的邻居是 $N(a)=\{b, d, e\}$，$N(b)=\{a, b, c, d, e\}$，$N(c)=\{b\}$，$N(d)=\{a, b, e\}$和 $N(e)=\{a, b, d\}$。 ◀



G H

把度为 0 的顶点称为**孤立的**。因此孤立点不与任何顶点相邻。例 1 中图 G 的顶点 g 是孤立的。顶点是**悬挂的**，当且仅当它的度是 1。因此悬挂点恰与 1 个其他顶点相邻。例 1 中图 G 的顶点 d 是悬挂的。

A vertex of degree zero is called **isolated**. It follows that an isolated vertex is not adjacent to any vertex. Vertex g in graph G in Example 1 is isolated. A vertex is **pendant** if and only if it has degree one. Consequently, a pendant vertex is adjacent to exactly one other vertex. Vertex d in graph G in Example 1 is pendant.

THEOREM 1 **THE HANDSHAKING THEOREM** Let $G = (V, E)$ be an undirected graph with m edges. Then

$$2m = \sum_{v \in V} \deg(v).$$

(Note that this applies even if multiple edges and loops are present.)

定理 1 握手定理 设 $G=(V, E)$ 是有 m 条边的无向图，则

$$2m = \sum_{v \in V} \deg(v)$$

（注意即使出现多重边和环，这个式子也仍然成立。）

- 握手定理说明无向图顶点度数之和为偶数

THEOREM 2 An undirected graph has an even number of vertices of odd degree.

定理 2 无向图有偶数个度为奇数的顶点。

Definition 4 When (u, v) is an edge of the graph G with directed edges, u is said to be *adjacent to* v and v is said to be *adjacent from* u. The vertex u is called the *initial vertex* of (u, v), and v is called the *terminal* or *end vertex* of (u, v). The initial vertex and terminal vertex of a loop are the same.

Definition 5 In a graph with directed edges the *in-degree of a vertex* v, denoted by $\deg^-(v)$, is the number of edges with v as their terminal vertex. The *out-degree of* v, denoted by $\deg^+(v)$, is the number of edges with v as their initial vertex. (Note that a loop at a vertex contributes 1 to both the in-degree and the out-degree of this vertex.)

因为带有有向边的图的边是有序对，所以这时顶点度的定义细化成把这个顶点作为起点和作为终点的不同的边数。

THEOREM 3 Let $G = (V, E)$ be a graph with directed edges. Then

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|.$$

The undirected graph that results from ignoring the directions of edges is called the **underlying undirected graph.** 基本无向图忽略边的方向

Some Special Simple Graphs

Complete Graphs 完全图

每对顶点间都有一条边的简单图 Kn

EXAMPLE 5 **Complete Graphs** A **complete graph on n vertices**, denoted by K_n, is a simple graph that contains exactly one edge between each pair of distinct vertices. The graphs K_n, for $n = 1, 2, 3, 4, 5, 6$, are displayed in Figure 3. A simple graph for which there is at least one pair of distinct vertex not connected by an edge is called **noncomplete**. ◀

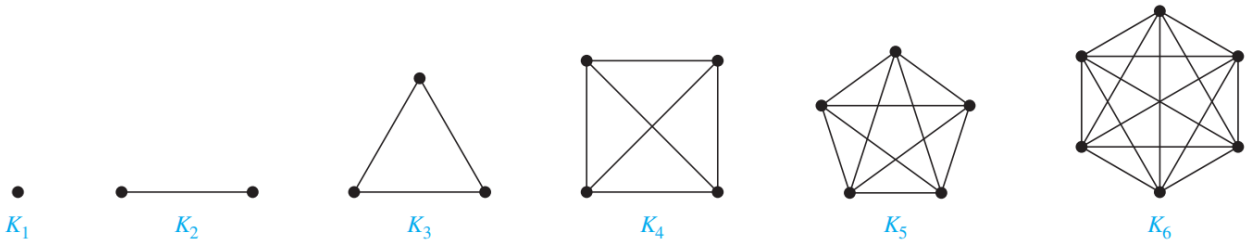


FIGURE 3 **The graphs K_n for $1 \leq n \leq 6$.**

圆圈 Cn

EXAMPLE 6 **Cycles** A **cycle C_n**, $n \geq 3$, consists of n vertices $v_1, v_2, \ldots, v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}$, and $\{v_n, v_1\}$. The cycles C_3, C_4, C_5, and C_6 are displayed in Figure 4. ◀

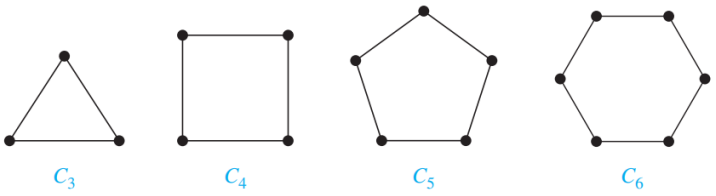


FIGURE 4 **The cycles C_3, C_4, C_5, and C_6.**

车轮 Wn

相同n，比Cycles多一个点放中间和周围的点连

EXAMPLE 7 **Wheels** We obtain a **wheel W_n** when we add an additional vertex to a cycle C_n, for $n \geq 3$, and connect this new vertex to each of the n vertices in C_n, by new edges. The wheels W_3, W_4, W_5, and W_6 are displayed in Figure 5. ◀

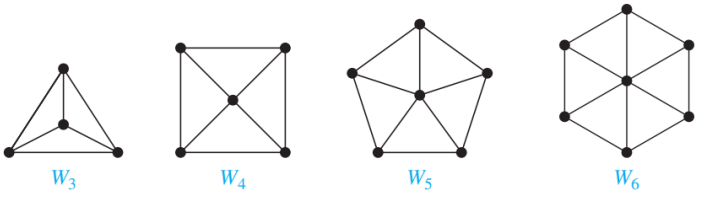


FIGURE 5 **The wheels W_3, W_4, W_5, and W_6.**

立方体 Qn

EXAMPLE 8 ***n*-Cubes** An ***n*-dimensional hypercube**, or ***n*-cube**, denoted by Q_n, is a graph that has vertices representing the 2^n bit strings of length n. Two vertices are adjacent if and only if the bit strings that they represent differ in exactly one bit position. We display Q_1, Q_2, and Q_3 in Figure 6.

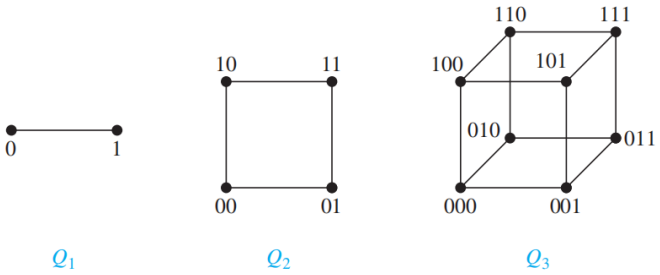


FIGURE 6 **The *n*-cube Q_n, $n = 1, 2, 3$.**

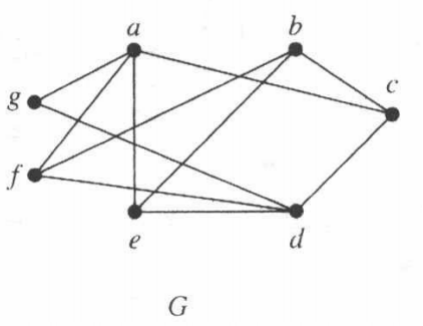
Bipartite Graphs 二分图

Definition 6

A simple graph G is called *bipartite* if its vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2). When this condition holds, we call the pair (V_1, V_2) a *bipartition* of the vertex set V of G.

定义 6　若把简单图 G 的顶点集分成两个不相交的非空集合 V_1 和 V_2，使得图中的每一条边都连接 V_1 中的一个顶点与 V_2 中的一个顶点（因此 G 中没有边连接 V_1 中的两个顶点或 V_2 中的两个顶点），则 G 称为二分图。当此条件成立时，称 (V_1, V_2) 为 G 的顶点集的一个二部划分。

- 树是二分图



G

解　图 G 是二分图，因为它的顶点集是两个不相交集合 $\{a, b, d\}$ 和 $\{c, e, f, g\}$ 的并集，每条边都连接一个子集中的一个顶点与另一个子集中的一个顶点。（注意，对二分图 G 来说，不必让 $\{a, b, d\}$ 里每一个顶点与 $\{c, e, f, g\}$ 里每一个顶点都相邻。例如 b 与 g 就不相邻。）

判断二分图的条件（当且仅当可以用两个颜色着色相邻顶点不重复）

THEOREM 4 A simple graph is bipartite if and only if it is possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color.

EXAMPLE 13 **Complete Bipartite Graphs** A **complete bipartite graph** $K_{m,n}$ is a graph that has its vertex set partitioned into two subsets of m and n vertices, respectively with an edge between two vertices if and only if one vertex is in the first subset and the other vertex is in the second subset. The complete bipartite graphs $K_{2,3}$, $K_{3,3}$, $K_{3,5}$, and $K_{2,6}$ are displayed in Figure 9. ◀

完全二分图

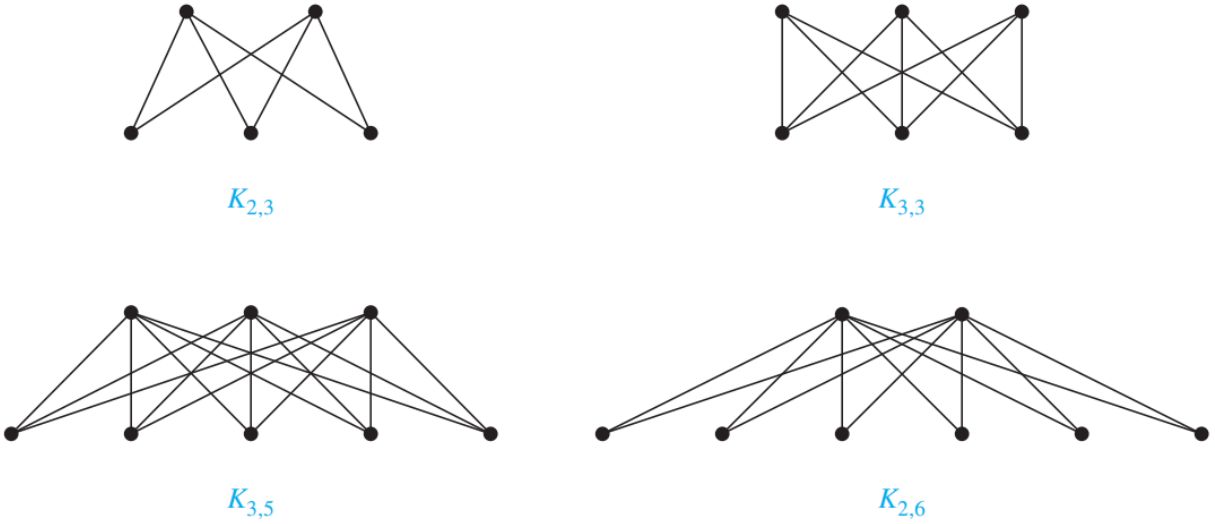


FIGURE 9 **Some complete bipartite graphs.**

New Graphs from Old

subgraph 子图：

Definition 7 A *subgraph of a graph* $G = (V, E)$ is a graph $H = (W, F)$, where $W \subseteq V$ and $F \subseteq E$. A subgraph H of G is a *proper subgraph* of G if $H \neq G$.

Definition 8 Let $G = (V, E)$ be a simple graph. The **subgraph induced** by a subset W of the vertex set V is the graph (W, F), where the edge set F contains an edge in E if and only if both endpoints of this edge are in W.

导出的子图

- **Removing edges of a graph**

  $G-e = (V, E-\{e\})$

- **Adding edges to a graph**

  $G+e = (V, E \cup \{e\})$

- **Edge contration**

  Remove an edge e with endpoints u and v, merge u and v into a new single vertex w, and for each edge with u or v as an endpoint replaces the edge with one with w as endpoint in place of u and v and with the same second endpoint.

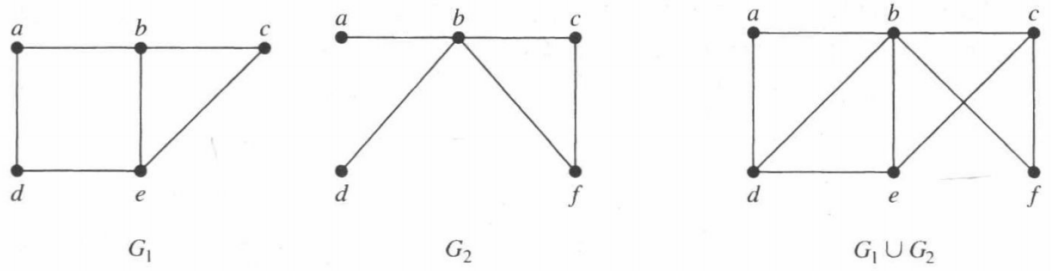
- **Removing vertices from a graph**

  $G-v = (V-v, E')$, where E' is the set of edges of G not incident to v

GRAPH UNIONS

Definition 9 The *union* of two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the simple graph with vertex set $V_1 \cup V_2$ and edge set $E_1 \cup E_2$. The union of G_1 and G_2 is denoted by $G_1 \cup G_2$.

例 20 求图 17a 所示的图 G_1 和 G_2 的并图。



a）简单图G_1和G_2　　b）它们的并$G_1 \cup G_2$

图 17　并图的产生过程

解　并图 $G_1 \cup G_2$ 的顶点集是两个顶点集的并，即$\{a, b, c, d, e, f\}$。并图的边集是两个边集的并。并图显示在图 17b 中。 ◀

10.3 Representing Graphs and Graph Isomorphism

同构

adjacency lists

EXAMPLE 1 Use adjacency lists to describe the simple graph given in Figure 1.

Solution: Table 1 lists those vertices adjacent to each of the vertices of the graph. ◀

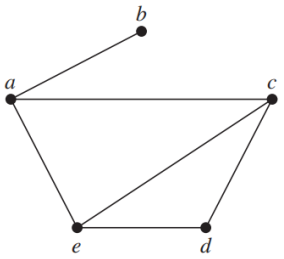


FIGURE 1 **A simple graph.**

TABLE 1 An Adjacency List for a Simple Graph.

Vertex	*Adjacent Vertices*
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

EXAMPLE 2 Represent the directed graph shown in Figure 2 by listing all the vertices that are the terminal vertices of edges starting at each vertex of the graph.

Solution: Table 2 represents the directed graph shown in Figure 2. ◀

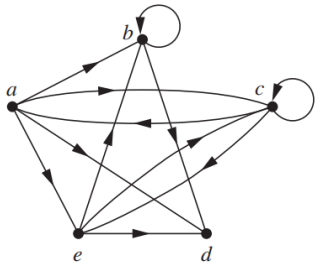


FIGURE 2 **A directed graph.**

TABLE 2 An Adjacency List for a Directed Graph.

Initial Vertex	*Terminal Vertices*
a	b, c, d, e
b	b, d
c	a, c, e
d	
e	b, c, d

Adjacency Matrices 邻接矩阵

邻接矩阵 $A = [a_{ij}]$, $a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \text{ is an edge of } G, \\ 0 & \text{otherwise.} \end{cases}$

EXAMPLE 3 Use an adjacency matrix to represent the graph shown in Figure 3.

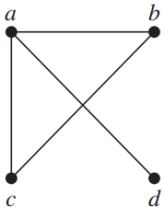


FIGURE 3
A simple graph.

Solution: We order the vertices as a, b, c, d. The matrix representing this graph is

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

The adjacency matrix of a simple graph is symmetric, that is, $a_{ij} = a_{ji}$. All undirected graphs, including multigraphs and pseudographs, have **symmetric adjacency matrices**..
多重图、伪图、简单图的邻接矩阵都对称

注意，图的邻接矩阵依赖于所选择的顶点的顺序。因此带 n 个顶点的图有 $n!$ 个不同的邻接矩阵，因为 n 个顶点有 $n!$ 个不同的顺序。

EXAMPLE 5

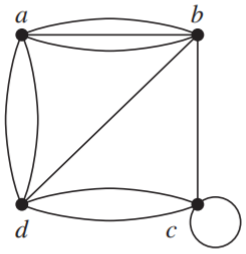


FIGURE 5
A pseudograph.

Use an adjacency matrix to represent the pseudograph shown in Figure 5.

Solution: The adjacency matrix using the ordering of vertices *a, b, c, d* is

$$\begin{bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{bmatrix}.$$

The adjacency matrix for a directed graph does not have to be symmetric.
有向图的邻接矩阵不一定对称

Incidence Matrices 关联矩阵

n × m matrix $M = [m_{ij}]$, $m_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident with } v_i, \\ 0 & \text{otherwise.} \end{cases}$

EXAMPLE 6 Represent the graph shown in Figure 6 with an incidence matrix.

Solution: The incidence matrix is

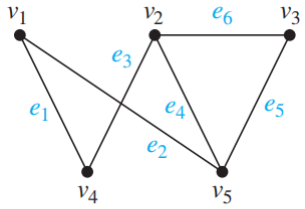


FIGURE 6 **An undirected graph.**

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}.$$

EXAMPLE 7 Represent the pseudograph shown in Figure 7 using an incidence matrix.

Solution: The incidence matrix for this graph is

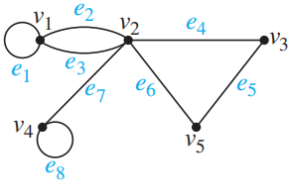


FIGURE 7 **A pseudograph.**

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}.$$

Isomorphism of Graphs 同构

Definition 1 The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are *isomorphic* if there exists a one-to-one and onto function f from V_1 to V_2 with the property that a and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2, for all a and b in V_1. Such a function f is called an *isomorphism*.* Two simple graphs that are not isomorphic are called *nonisomorphic*.

定义 1　设 $G_1=(V_1, E_1)$ 和 $G_2=(V_2, E_2)$ 是简单图，若存在一对一的和映上的从 V_1 到 V_2 的函数 f，且 f 具有这样的性质：对 V_1 中所有的 a 和 b 来说，a 和 b 在 G_1 中相邻当且仅当 $f(a)$ 和 $f(b)$ 在 G_2 中相邻，则称 G_1 与 G_2 是同构的。这样的函数 f 称为同构[⊖]。两个不同构的简单图称为非同构的。

例 8　证明：图 8 所示的图 $G=(V, E)$ 和 $H=(W, F)$ 同构。

解　函数 f 定义为 $f(u_1)=v_1$，$f(u_2)=v_4$，$f(u_3)=v_3$，$f(u_4)=v_2$，它是 V 和 W 之间的一一对应。为了看出这个对应保持相邻关系，注意 G 中相邻的顶点是 u_1 和 u_2、u_1 和 u_3、u_2 和 u_4，以及 u_3 和 u_4，由 $f(u_1)=v_1$ 和 $f(u_2)=v_4$、$f(u_1)=v_1$ 和 $f(u_3)=v_3$、$f(u_2)=v_4$ 和 $f(u_4)=v_2$，以及 $f(u_3)=v_3$ 和 $f(u_4)=v_2$ 所组成的每一对顶点都是在 H 中相邻的。◀

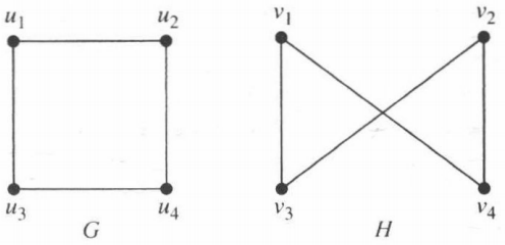


图 8　图 G 和 H

graph invariant 图形不变量

顶点数、边数、顶点的度数

9个顶点不同构的有根树有9个

10.4 Connectivity

simple path 简单通路：a path that does not contain an edge more than once 只包含一条边一次

定义 1　设 n 是非负整数且 G 是无向图。在 G 中从 u 到 v 的长度为 n 的通路是 G 的 n 条边 e_1，…，e_n 的序列，其中存在 $x_0=u$，x_1，…，$x_n=v$ 的顶点序列，使得对于 $i=1$，…，n，e_i 以 x_{i-1} 和 x_i 作为端点。当这个图是简单图时，就用顶点序列 x_0，x_1，…，x_n 表示这条通路（因为列出这些顶点就唯一地确定了通路）。若一条通路在相同的顶点开始和结束，即 $u=v$ 且长度大于 0，则它是一条回路。把通路或回路说成是经过顶点 x_1，x_2，…，x_{n-1} 或遍历边 e_1，e_2，…，e_n。若通路或回路不重复地包含相同的边，则它是简单的。

Definition 1

Let n be a nonnegative integer and G an undirected graph. A *path* of *length* n from u to v in G is a sequence of n edges $e_1, \ldots, e_n$ of G for which there exists a sequence $x_0 = u, x_1, \ldots, x_{n-1}, x_n = v$ of vertices such that e_i has, for $i = 1, \ldots, n$, the endpoints x_{i-1} and x_i. When the graph is simple, we denote this path by its vertex sequence $x_0, x_1, \ldots, x_n$ (because listing these vertices uniquely determines the path). The path is a *circuit* if it begins and ends at the same vertex, that is, if $u = v$, and has length greater than zero. The path or circuit is said to *pass through* the vertices $x_1, x_2, \ldots, x_{n-1}$ or *traverse* the edges $e_1, e_2, \ldots, e_n$. A path or circuit is *simple* if it does not contain the same edge more than once.

例 1　如图 1 所示，a，d，c，f，e 是长度为 4 的简单通路，因为 $\{a, d\}$、$\{d, c\}$、$\{c, f\}$ 和 $\{f, e\}$ 都是边。但是 d，e，c，a 不是通路，因为 $\{e, c\}$ 不是边。注意 b，c，f，e，b 是长度为 4 的回路，因为 $\{b, c\}$、$\{c, f\}$、$\{f, e\}$ 和 $\{e, b\}$ 都是边，且这条通路在 b 上开始和结束。长度为 5 的通路 a，b，e，d，a，b 不是简单的，因为它包含边 $\{a, b\}$ 两次。 ◀

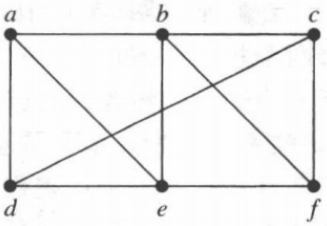


图 1　简单图

定义 2　设 n 是非负整数且 G 是有向图。在 G 中从 u 到 v 的长度为 n 的通路是 G 的边的序列 e_1，e_2，…，e_n，使得 $f(e_1)=(x_0, x_1)$，$f(e_2)=(x_1, x_2)$，…，$f(e_n)=(x_{n-1}, x_n)$，其中 $x_0=u$，$x_n=v$。当有向图中没有多重边时，就用顶点序列 x_0，x_1，…，x_n 表示这条通路。把在相同的顶点上开始和结束的长度大于 0 的通路称为回路或圈。若一条通路或回路不重复地包含相同的边，则把它称为简单的。

Definition 2

Let n be a nonnegative integer and G a directed graph. A *path* of length n from u to v in G is a sequence of edges $e_1, e_2, \ldots, e_n$ of G such that e_1 is associated with (x_0, x_1), e_2 is associated with (x_1, x_2), and so on, with e_n associated with (x_{n-1}, x_n), where $x_0 = u$ and $x_n = v$. When there are no multiple edges in the directed graph, this path is denoted by its vertex sequence $x_0, x_1, x_2, \ldots, x_n$. A path of length greater than zero that begins and ends at the same vertex is called a *circuit* or *cycle*. A path or circuit is called *simple* if it does not contain the same edge more than once.

connected graph: an undirected graph with the property that there is a path between every pair of vertices

Paths in Acquaintanceship Graphs 无向图的连通性

Definition 3 An undirected graph is called *connected* if there is a path between every pair of distinct vertices of the graph. An undirected graph that is not *connected* is called *disconnected*. We say that we *disconnect* a graph when we remove vertices or edges, or both, to produce a disconnected subgraph.

THEOREM 1 There is a simple path between every pair of distinct vertices of a connected undirected graph.

connected component 连通分支

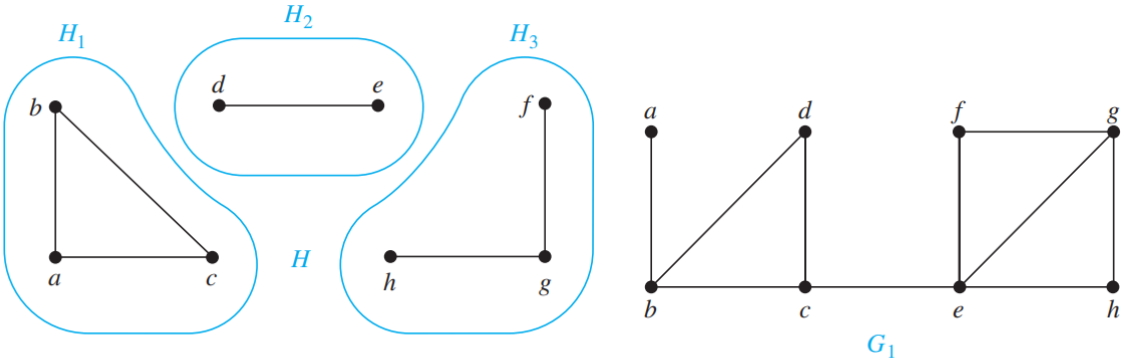


FIGURE 3 **The graph H and its connected components H_1, H_2, and H_3.**

cut vertices(or **articulation points**) 割点：a vertex *v such that _G _− _v _is disconnected*

cut edge *or* ***bridge***：*an edge _e _such that _G _- _e _is disconnected*

EXAMPLE 7 Find the cut vertices and cut edges in the graph G_1 shown in Figure 4.

Solution: The cut vertices of G_1 are b, c, and e. The removal of one of these vertices (and its adjacent edges) disconnects the graph. The cut edges are $\{a, b\}$ and $\{c, e\}$. Removing either one of these edges disconnects G_1. ◀

VERTEX CONNECTIVITY

点连通性 并不是所有的图都有割点。例如，完全图 K_n，其中 $n \geqslant 3$，就没有割点。当从 K_n 中删除一个顶点及其相关联的边时，得到的子图是一个连通的完全图 K_{n-1}。不含割点的连通图称为**不可分割图**，它比有割点的连通图具有更好的连通性。我们可以扩展这个概念，基于使一个图不连通需要删除的最小的顶点数，定义一个与图的连通性相关的更大粒度的方法。

若 $G-V'$ 是不连通的，则称 $G=(V, E)$ 的顶点集 V 的子集 V' 是点割集，或分割集。例如，在图 1 中，集合 $\{b, c, e\}$ 是一个含有 3 个顶点的点割集，读者可自行验证。我们留给读者证明（练习 51），除了完全图以外，每一个连通图都有一个点割集。我们定义非完全图的点连通度为点割集中最小的顶点数，记作 $\kappa(G)$。

当 G 是完全图时，它没有点割集，因为删除它顶点集合的任意子集及其所有相关联的边后它仍然是一个完全图。同时，当 G 是完全图时，我们不能把 $\kappa(G)$ 定义为点割集的最小顶点数。我们用 $\kappa(K_n)=n-1$ 来替代，这是需要删除的顶点数，以便得到只含有一个顶点的图。

A subset _V′ of the vertex set *V _of _G _= (*V, E*) is a* ***vertex cut,*** *or* ***separating set,*** *if _G _− _V _′ is disconnected.*

因此，对于每一个图 G，$\kappa(G)$是使 G 变成不连通的图或只含有一个顶点的图所需删除的最小的顶点数。若 G 含有 n 个顶点，则 $0 \leqslant \kappa(G) \leqslant n-1$，$\kappa(G)=0$ 当且仅当 G 是不连通的或 $G=K_1$，$\kappa(G)=n-1$ 当且仅当 G 是完全图[参见练习 52a]。

$\kappa(G)$越大，我们认为 G 的连通性越好。不连通的图和 K_1 具有 $\kappa(G)=0$，含有点割集的连通图和 K_2 具有 $\kappa(G)=1$，不含点割集的需要删除两个顶点才变成不连通的图和 K_3 具有 $\kappa(G)=2$，以此类推。若 $\kappa(G) \geqslant k$，我们称图为 **k 连通的**(或 **k 顶点-连通的**)。若图是连通的且不是只含 1 个顶点的图，则称该图是 1 连通的；若图是不可分割的且至少含有 3 个顶点，则称该图为 2 连通的或**双连通的**。注意若 G 是一个 k 连通图，则对所有的 j，$0 \leqslant j \leqslant k$，$G$ 是一个 j 连通图。

κ(G) *(the vertex connectivity of _G)*: **the size of a smallest vertex cut of *G*

EDGE CONNECTIVITY

边连通度 我们可以通过把连通图 $G=(V, E)$变成不连通的所需要删除的最小边数，来度量连通图 G 的连通性。若一个图含有割边，那么我们只需删除该边就可以使 G 变成不连通的。如果 G 不含有割边，那么我们寻找需要删除的最小的边割集，以使 G 变成不连通的。如果$G-E'$是不连通的，则称边集 E'是图 G 的**边割集**。图 G 的**边连通度**，记作 $\lambda(G)$，是图 G 的边割集中的最小的边数。这给出了顶点数大于 1 的所有连通图的 $\lambda(G)$的定义，因为把所有与图中某个顶点相关联的边都删除，就可以使该图变成不连通的。注意，若 G 是不连通的，则 $\lambda(G)=0$。若 G 是只含有 1 个顶点的图，我们也定义 $\lambda(G)=0$。由此可得，若 G 是含有 n 个顶点的图，则 $0 \leqslant \lambda(G) \leqslant n-1$。我们留给读者[练习 52b]证明，$G$ 是含有 n 个顶点的图，$\lambda(G)=n-1$当且仅当 $G=K_n$，这等价于命题，若 G 不是完全图，则 $\lambda(G) \leqslant n-2$。

AN INEQUALITY FOR VERTEX CONNECTIVITY AND EDGE CONNECTIVITY

一个与点连通度和边连通度相关的不等式 当 $G=(V, E)$是一个至少含有 3 个顶点的非完全连通图时，图 G 中顶点的最小度是图 G 的点连通度和图 G 的边连通度的上界。即 $\kappa(G) \leqslant \min_{v \in V} \deg(v)$ 和 $\lambda(G) \leqslant \min_{v \in V} \deg(v)$。为了明白这一点，注意删除度最小的顶点的所有邻居，就使 G 变成不连通的；而且删除所有以度最小的顶点为端点的边，就使 G 变成不连通的。

在练习 55 中，我们要求读者证明，若 G 是一个连通的非完全图，则$\kappa(G) \leqslant \lambda(G)$。还要注意，若 n 是正整数，则$\kappa(K_n)=\lambda(K_n)=\min_{v \in V} \deg(v)=n-1$，而且，若 G 是不连通的图，则$\kappa(G)=\lambda(G)=0$。将这些事实结合起来，对所有的图 G 有

λ(G) (the edge connectivity of *G*): the size of a smallest edge cut of *G*

$$\kappa(G) \leq \lambda(G) \leq \min_{v \in V} \deg(v).$$

Connectedness in Directed Graphs 有向图的连通性

Definition 4 A directed graph is *strongly connected* if there is a path from *a* to *b* and from *b* to *a* whenever *a* and *b* are vertices in the graph.

强连通：有一条路从a到b，从b到a（a, b是图中的顶点）

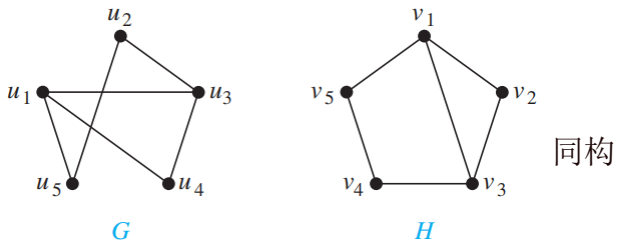
Definition 5 A directed graph is *weakly connected* if there is a path between every two vertices in the underlying undirected graph.

STRONG COMPONENTS OF A DIRECTED GRAPH

有向图的强连通分支 有向图 G 的子图是强连通的，但不包含在更大的强连通子图中，即极大强连通子图，可称为 G 的**强连通分支**或**强分支**。注意，若 a 和 b 是有向图中的两个顶点，它们的强连通分支或者相同或者不相交。（我们把这个事实的证明留在练习 17 中。）

也就是说，有向图是弱连通的，当且仅当在忽略边的方向时，任何两个顶点之间总是存在通路。显然，任何强连通有向图也是弱连通的。

Paths and Isomorphism



同构

FIGURE 7 **The graphs *G* and *H*.**

Counting Paths Between Vertices

THEOREM 2 Let G be a graph with adjacency matrix $\mathbf{A}$ with respect to the ordering $v_1, v_2, \ldots, v_n$ of the vertices of the graph (with directed or undirected edges, with multiple edges and loops allowed). The number of different paths of length r from v_i to v_j, where r is a positive integer, equals the (i, j)th entry of $\mathbf{A}^r$.

定理2 设G是一个图，该图的邻接矩阵$\boldsymbol{A}$相对于图中的顶点顺序v_1，v_2，…，v_n（允许带有无向或有向边、带有多重边和环）。从v_i到v_j长度为r的不同通路的数目等于$\boldsymbol{A}^r$的第(i, j)项，其中r是正整数。

例15 在图8所示的简单图G中，从a到d长度为4的通路有多少条？

解 G的邻接矩阵（顶点顺序为a，b，c，d）是

$$\boldsymbol{A} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

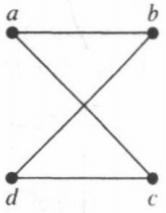


图8 图G

因此从a到d长度为4的通路数是$\mathbf{A}^4$的第$(1, 4)$项。因为

$$\boldsymbol{A}^4 = \begin{bmatrix} 8 & 0 & 0 & 8 \\ 0 & 8 & 8 & 0 \\ 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \end{bmatrix}$$

所以恰好有8条从a到d长度为4的通路。通过观察这个图，我们看出a，b，a，b，d；a，b，a，c，d；a，b，d，b，d；a，b，d，c，d；a，c，a，b，d；a，c，a，c，d；a，c，d，b，d和a，c，d，c，d是8条从a到d的通路。 ◀

矩阵乘法是第m行✕第n列得到第(m, n)个元素的值

10.5 Euler and Hamilton Paths

Euler Paths and Circuits 欧拉通路&回路

经过边

Definition 1 An *Euler circuit* in a graph G is a simple circuit containing every edge of G. An *Euler path* in G is a simple path containing every edge of G.

定义1 图G中的欧拉回路是包含G的每一条边的简单回路。图G中的欧拉通路是包含G的每一条边的简单通路。

例 1 在图 3 中，哪些无向图有欧拉回路？在没有欧拉回路的那些图中，哪些具有欧拉通路？

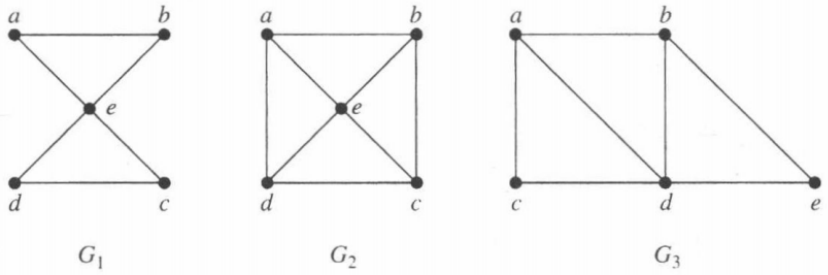


图 3　无向图 G_1、G_2 和 G_3

解　图 G_1 具有欧拉回路，例如 a，e，c，d，e，b，a。G_2 和 G_3 都没有欧拉回路（读者应当验证它）。但是 G_3 具有欧拉通路，即 a，c，d，e，b，d，a，b。G_2 没有欧拉通路（读者应当验证它）。◀

例 2 在图 4 中，哪些有向图有欧拉回路？在没有欧拉回路的那些图中，哪些具有欧拉通路？

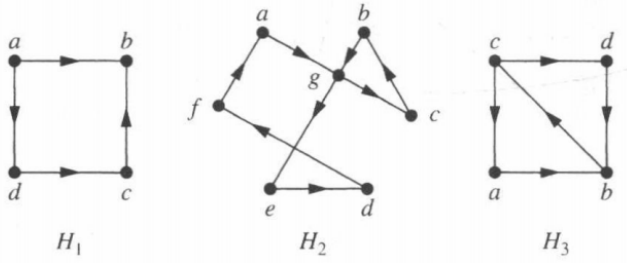


图 4　有向图 H_1，H_2 和 H_3

解　图 H_2 有欧拉回路，例如 a，g，c，b，g，e，d，f，a。H_1 和 H_3 都没有欧拉回路（读者应当验证它）。H_3 具有欧拉通路，即 c，a，b，c，d，b，但是 H_1 没有欧拉通路（读者应当验证它）。◀

NECESSARY AND SUFFICIENT CONDITIONS FOR EULER CIRCUITS AND PATHS

欧拉回路/通路 的充分必要条件

THEOREM 1　A connected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree.

定理 1　含有至少 2 个顶点的连通多重图具有欧拉回路当且仅当它的每个顶点的度都为偶数。

THEOREM 2　A connected multigraph has an Euler path but not an Euler circuit if and only if it has exactly two vertices of odd degree.

定理 2　连通多重图具有欧拉通路但无欧拉回路当且仅当它恰有 2 个度为奇数的顶点。

有欧拉通路就从一个奇数度的顶点出发，于另一个奇数度的顶点结束

Hamilton Paths and Circuits 哈密顿

经过顶点

定义 2 经过图 G 中每一个顶点恰好一次的简单通路称为哈密顿通路，经过图 G 中每一个顶点恰好一次的简单回路称为哈密顿回路。即，在图 $G=(V, E)$ 中，若 $V=\{x_0, x_1, \cdots, x_{n-1}, x_n\}$ 并且对 $0 \leqslant i<j \leqslant n$ 来说有 $x_i \neq x_j$，则图 G 中的简单通路 $x_0, x_1, \cdots, x_{n-1}, x_n$ 称为哈密顿通路。在图 $G=(V, E)$ 中，若 $x_0, x_1, \cdots, x_{n-1}, x_n$ 是哈密顿通路，则 $x_0, x_1, \cdots, x_{n-1}, x_n, x_0$（其中 $n>0$）称为哈密顿回路。

例 5 在图 10 中，哪些简单图具有哈密顿回路？或者没有哈密顿回路但是有哈密顿通路？

解 G_1 有哈密顿回路：a, b, c, d, e, a。G_2 没有哈密顿回路（可以看出包含每一个顶点的任何回路必然两次包含边 $\{a, b\}$），但是 G_2 确实有哈密顿通路，即 a, b, c, d。G_3 既无哈密顿回路也无哈密顿通路，因为包含所有顶点的任何通路都必须多次包含边 $\{a, b\}$、$\{e, f\}$ 和 $\{c, d\}$ 其中之一。 ◀

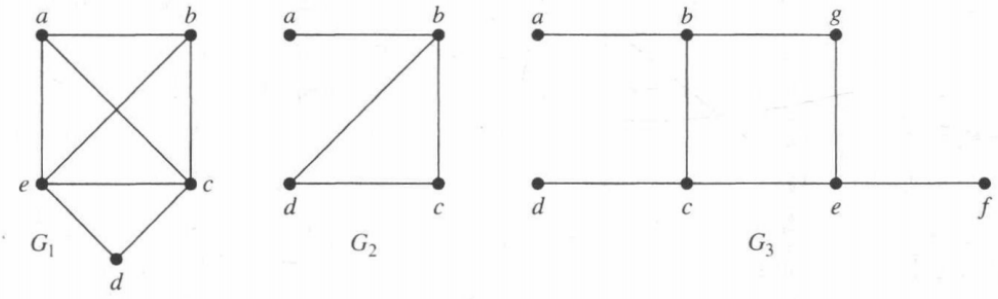


图 10 三个简单图

CONDITIONS FOR THE EXISTENCE OF HAMILTON CIRCUITS

哈密顿回路存在条件

定理 3 狄拉克定理 如果 G 是有 n 个顶点的简单图，其中 $n \geqslant 3$，并且 G 中每个顶点的度都至少为 $n/2$，则 G 有哈密顿回路。

定理 4 欧尔定理 如果 G 是有 n 个顶点的简单图，其中 $n \geqslant 3$，并且对于 G 中每一对不相邻的顶点 u 和 v 来说，都有 $\deg(u)+\deg(v) \geqslant n$，则 G 有哈密顿回路。

THEOREM 3 **DIRAC'S THEOREM** If G is a simple graph with n vertices with $n \geq 3$ such that the degree of every vertex in G is at least $n/2$, then G has a Hamilton circuit.

THEOREM 4 **ORE'S THEOREM** If G is a simple graph with n vertices with $n \geq 3$ such that $\deg(u) + \deg(v) \geq n$ for every pair of nonadjacent vertices u and v in G, then G has a Hamilton circuit.

若一个图存在哈密顿回路，就称为哈密顿图 hamilton graph。

10.6 Shortest-Path Problems

Graphs that have a number assigned to each edge are called **weighted graphs**.加权图

定理 1　迪克斯特拉算法求出连通简单无向加权图中两个顶点之间最短通路的长度。

定理 2　迪克斯特拉算法使用 $O(n^2)$ 次运算（加法和比较）求出含有 n 个顶点的连通简单无向加权图中两个顶点之间最短通路的长度。

10.7 Planar Graphs

平面图

Definition 1 A graph is called *planar* if it can be drawn in the plane without any edges crossing (where a crossing of edges is the intersection of the lines or arcs representing them at a point other than their common endpoint). Such a drawing is called a *planar representation* of the graph.

定义 1　若可以在平面中画出一个图而边没有任何交叉（其中边的交叉是表示边的直线或弧线在它们的公共端点以外的地方相交），则这个图是平面图。这种画法称为这个图的平面表示。

Euler's Formula 欧拉公式

regions面

定理 1　欧拉公式　设 G 是带 e 条边和 v 个顶点的连通平面简单图。设 r 是 G 的平面图表示中的面数。则 $r=e-v+2$。

THEOREM 1 **EULER'S FORMULA** Let G be a connected planar simple graph with e edges and v vertices. Let r be the number of regions in a planar representation of G. Then $r = e - v + 2$.

COROLLARY 1 If G is a connected planar simple graph with e edges and v vertices, where $v \geq 3$, then $e \leq 3v - 6$.

推论 1　若 G 是 e 条边和 v 个顶点的连通平面简单图，其中 $v \geqslant 3$，则 $e \leqslant 3v-6$。

COROLLARY 2 If G is a connected planar simple graph, then G has a vertex of degree not exceeding five.

推论 2　若 G 是连通平面简单图，则 G 中有度数不超过 5 的顶点。

COROLLARY 3 If a connected planar simple graph has e edges and v vertices with $v \geq 3$ and no circuits of length three, then $e \leq 2v - 4$.

推论 3 若连通平面简单图有 e 条边和 v 个顶点，$v \geqslant 3$ 并且没有长度为 3 的回路，则 $e \leqslant 2v-4$。

EXAMPLE 5 Show that K_5 is nonplanar using Corollary 1.

Solution: The graph K_5 has five vertices and 10 edges. However, the inequality $e \leq 3v - 6$ is not satisfied for this graph because $e = 10$ and $3v - 6 = 9$. Therefore, K_5 is not planar. ◀

It was previously shown that $K_{3,3}$ is not planar. Note, however, that this graph has six vertices and nine edges. This means that the inequality $e = 9 \leq 12 = 3 \cdot 6 - 6$ is satisfied. Consequently, the fact that the inequality $e \leq 3v - 6$ is satisfied does *not* imply that a graph is planar. However, the following corollary of Theorem 1 can be used to show that $K_{3,3}$ is nonplanar.

Kuratowski's Theorem 库拉图斯基

homeomorphic 同胚的：two undirected graphs are homeomorphic if they can be obtained from the same graph by a sequence of elementary subdivisions

elementary subdivision 初等细分：the removal of an edge {*u, v*} of an undirected graph and the addition of a new vertex *w together with edges* {u, w} *and* {w, v}

若一个图是平面图，则通过删除一条边 $\{u, v\}$ 并且添加一个新顶点 w 和两条边 $\{u, w\}$ 与 $\{w, v\}$ 获得的任何图也是平面图。这样的操作称为**初等细分**。若可以从相同的图通过一系列初等细分来获得图 $G_1 = (V_1, E_1)$ 和图 $G_2 = (V_2, E_2)$，则称它们是**同胚的**。

THEOREM 2 A graph is nonplanar if and only if it contains a subgraph homeomorphic to $K_{3,3}$ or K_5.

定理 2 一个图是非平面图当且仅当它包含一个同胚于 $K_{3,3}$ 或 K_5 的子图。

解 G 有同胚于 K_5 的子图 H。H 是这样获得的：删除 h、j 和 k 以及所有与这些顶点关联的边。H 是同胚于 K_5 的，因为从 K_5（带有顶点 a、b、c、g 和 i）通过一系列初等细分，添加顶点 d、e 和 f 就可以获得 H（读者应当构造出这样一系列初等细分）。因此，G 是非平面图。◀

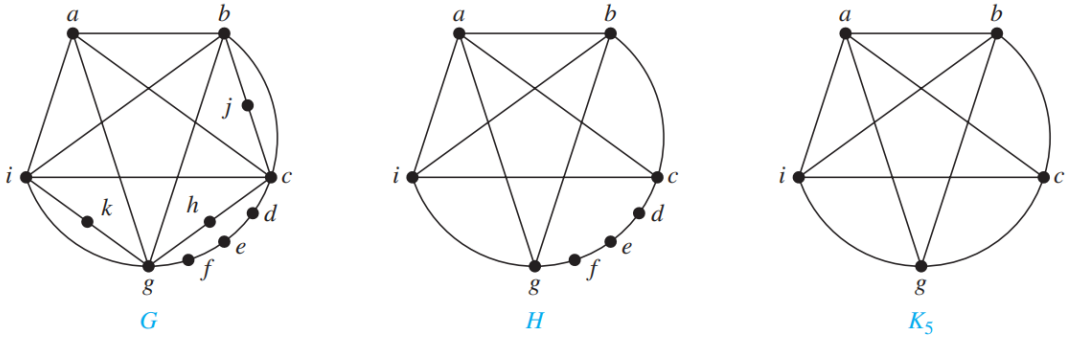


FIGURE 13 The undirected graph G, a subgraph H homeomorphic to K_5, and K_5.

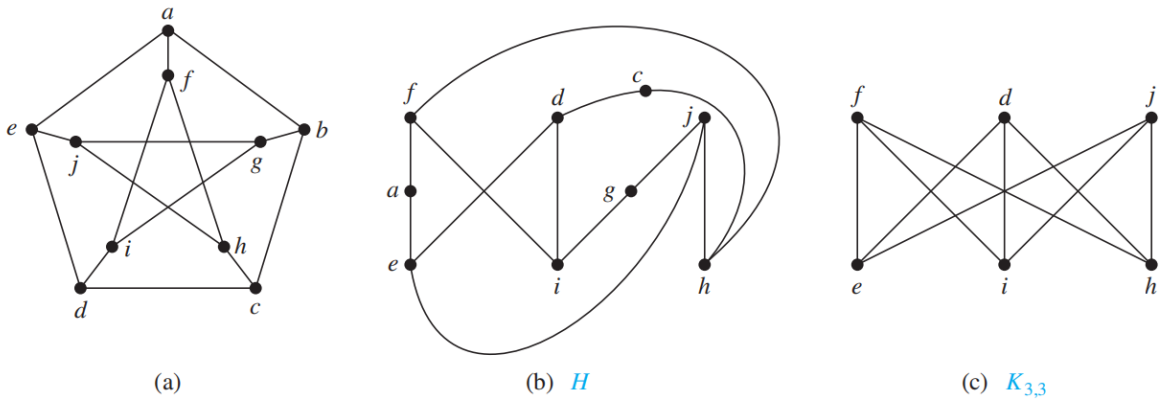


FIGURE 14 (a) The Petersen graph, (b) a subgraph H homeomorphic to $K_{3,3}$, and (c) $K_{3,3}$.

解 彼得森图的子图 H 是这样获得的：删除 b 和以 b 为端点的 3 条边，如图 14b 所示，它同胚于带有顶点集合 $\{f, d, j\}$ 和 $\{e, i, h\}$ 的 $K_{3,3}$，因为可以通过一系列初等细分（删除 $\{d, h\}$ 并添加 $\{c, h\}$ 和 $\{c, d\}$，删除 $\{e, f\}$ 并添加 $\{a, e\}$ 和 $\{a, f\}$，删除 $\{i, j\}$ 并添加 $\{g, i\}$ 和 $\{g, j\}$）来获得它。因此，彼得森图不是平面图。 ◀

10.8 Graph Coloring

平面中的每幅地图都可以表示成一个图。为了建立这样的对应关系，地图的每个区域都表示成一个顶点。若两个顶点所表示的区域具有公共边界，则用边连接这两个顶点。只相交于一个点的两个区域不算是相邻的。这样所得到的图称为这个地图的**对偶图**。根据地图的对偶图的构造方式，显然在平面中的任何地图都具有可平面的对偶图。图 2 显示了对应于图 1 所示地图的对偶图。

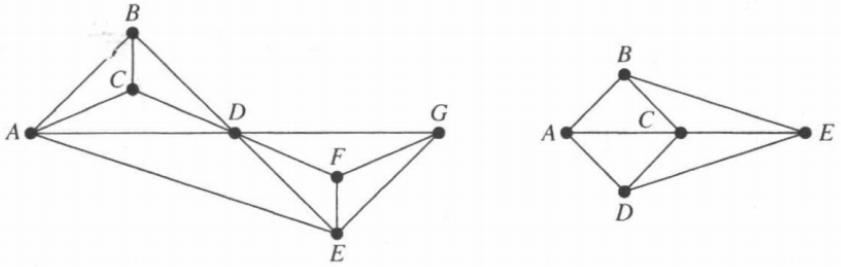


图 2　图 1 中的地图的对偶图

dual graph 对偶图

定义 1　简单图的着色是对该图的每个顶点都指定一种颜色，使得没有两个相邻的顶点颜色相同。

定义 2　图的着色数是着色这个图所需要的最少颜色数。图 G 的着色数记作 $\chi(G)$（这里 χ 是希腊字母 chi）。

chromatic number ⊠(G): the least number of colors needed for the coloring of this graph

定理 1　四色定理　平面图的着色数不超过 4。

四色原理（平面内）

THEOREM 1　**THE FOUR COLOR THEOREM**　The chromatic number of a planar graph is no greater than four.

[Proof]:

例 2　K_n 的着色数是什么？

解　通过给每个顶点指定一种不同的颜色，用 n 种颜色可以构造 K_n 的着色。使用的颜色能否更少一些？答案是不能。没有两个顶点可以指定相同的颜色，因为这个图的每两个顶点都是相邻的。因此，K_n 的着色数 $=n$。即 $\chi(K_n)=n$。（回忆一下，当 $n\geqslant 5$ 时 K_n 不是平面图，所以这个结果与四色定理并不矛盾。）图 5 显示了使用 5 种颜色对 K_5 着色。 ◀

例 3　完全二分图 $K_{m,n}$ 的着色数是什么？其中 m 和 n 都是正整数。

解　需要的颜色数似乎依赖于 m 和 n。不过，由 10.2 节的定理 4 可知，仅仅需要两种颜色，因为 $K_{m,n}$ 是二分图，所以 $\chi(K_{m,n})=2$。这意味着，可以用一种颜色为 m 个顶点着色，用另外一种颜色为 n 个顶点着色。因为边都只能连接 m 个顶点中的一个顶点与 n 个顶点中的一个顶点，所以没有相邻的顶点具有相同的颜色。图 6 显示了带有两种颜色的 $K_{3,4}$ 的着色。 ◀

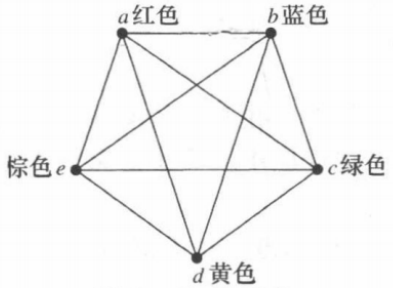


图 5　K_5 的着色

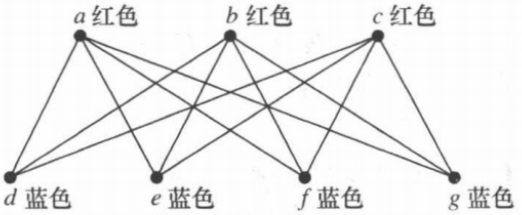


图 6　$K_{3,4}$ 的着色

11 Trees

11.1 Introduction to Trees

Definition 1　A *tree* is a connected undirected graph with no simple circuits.

连通+无向+n个顶点&n-1条边是一棵树；连通+无向+没有简单回路是一棵树

root

Definition 2　A *rooted tree* is a tree in which one vertex has been designated as the root and every edge is directed away from the root.

定义 2　有根树是指定一个顶点作为根并且每条边的方向都离开根的树。

parent 父母 of v in a rooted tree: the vertex u such that (u, v) is an edge of the rooted

tree

child 孩子 of a vertex v in a rooted tree: any vertex with v as its parent

internal vertex 内点: a vertex that has children

leaf 树叶: a vertex with no children

Definition 3 A rooted tree is called an *m-ary tree* if every internal vertex has no more than m children. The tree is called a *full m-ary tree* if every internal vertex has exactly m children. An m-ary tree with $m = 2$ is called a *binary tree*.

Links

定义 3　若有根树的每个内点都有不超过 m 个孩子，则称它为 m 叉树。若该树的每个内点都恰好有 m 个孩子，则称它为满 m 叉树。把 $m=2$ 的 m 叉树称为二叉树。

full m-ary tree 满二叉树: a tree with the property that every internal vertex has exactly m children 每个内点都有m个孩子

ordered tree 有序树: a tree in which the children of each internal vertex are linearly ordered

例 3　在图 7 中的有根树，对某个正整数 m 来说是否为满 m 叉树？

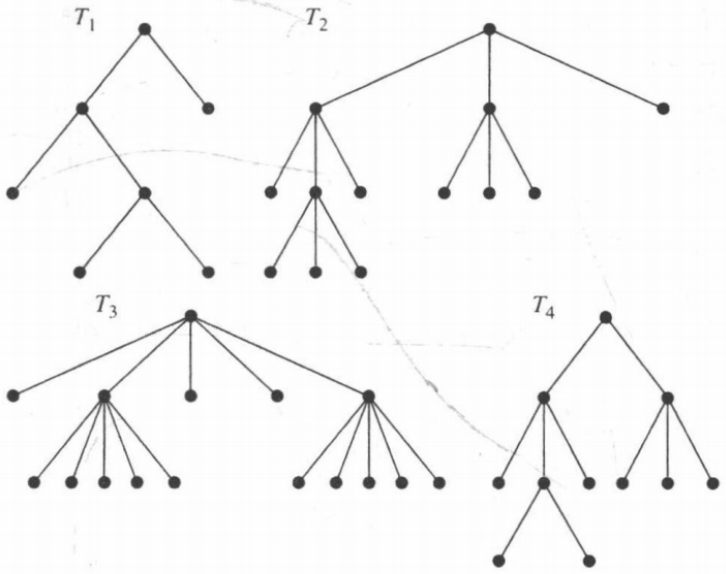


图 7　4 个有根树

解　T_1 是满二叉树，因为它的每个内点都有 2 个孩子。T_2 是满三叉树，因为它的每个内点都有 3 个孩子。在 T_3 中每个内点都有 5 个孩子，所以它是满五叉树。对任何 m 来说，T_4 都不是满 m 叉树，因为它的有些内点有 2 个孩子而有些内点有 3 个孩子。 ◀

Properties of Trees

THEOREM 2 A tree with n vertices has $n - 1$ edges.

THEOREM 3 A full m-ary tree with i internal vertices contains $n = mi + 1$ vertices.

THEOREM 4 A full m-ary tree with

(*i*) n vertices has $i = (n - 1)/m$ internal vertices and $l = [(m - 1)n + 1]/m$ leaves,
(*ii*) i internal vertices has $n = mi + 1$ vertices and $l = (m - 1)i + 1$ leaves,
(*iii*) l leaves has $n = (ml - 1)/(m - 1)$ vertices and $i = (l - 1)/(m - 1)$ internal vertices.

BALANCED *m*-ARY TREES 平衡的m叉树

level of a vertex 顶点的层: the length of the path from the root to this vertex
height of a tree 树高: the largest level of the vertices of a tree
balanced tree: a tree in which every leaf is at level h or h − 1, where h is the height of the tree

THEOREM 5 There are at most m^h leaves in an m-ary tree of height h.

COROLLARY 1 If an m-ary tree of height h has l leaves, then $h \geq \lceil \log_m l \rceil$. If the m-ary tree is full and balanced, then $h = \lceil \log_m l \rceil$. (We are using the ceiling function here. Recall that $\lceil x \rceil$ is the smallest integer greater than or equal to x.)

推论 1 若一棵高度为 h 的 m 叉树带有 l 个树叶，则 $h \geq \lceil \log_m l \rceil$。若这棵 m 叉树是满的和平衡的，则 $h = \lceil \log_m l \rceil$（这里使用向上取整函数。$\lceil x \rceil$ 是大于或等于 x 的最小整数）。

根的高度是0

11.2 Applications of Trees

binary search tree 二叉搜索树

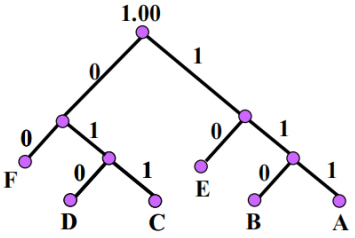
Decision Trees 决策树

THEOREM 1 A sorting algorithm based on binary comparisons requires at least $\lceil \log_2 n! \rceil$ comparisons.

COROLLARY 1 The number of comparisons used by a sorting algorithm to sort n elements based on binary comparisons is $\Omega(n \log n)$.

Huffman coding 哈夫曼编码

〖Example 1〗 Use Huffman coding to encode the following symbols with the frequencies listed: *A*:0.08, *B*:0.10, *C*:0.12, *D*:0.15, *E*:0.20, *F*:0.35. What is the average number of bits used to encode a character?



Solution:

The encoding produced encodes *A* by 111, *B* by 110, *C* by 011, *D* by 010, *E* by 10, and *F* by 00.

The average number of bits used to encode a symbol using this encoding is

$$3 \cdot 0.08 + 3 \cdot 0.10 + 3 \cdot 0.12 + 3 \cdot 0.15 + 2 \cdot 0.20 + 2 \cdot 0.35 = 2.45.$$

左边的点权重>右边

Game Trees 博弈树

Definition 1 The *value of a vertex in a game tree* is defined recursively as:

(*i*) the value of a leaf is the payoff to the first player when the game terminates in the position represented by this leaf.

(*ii*) the value of an internal vertex at an even level is the maximum of the values of its children, and the value of an internal vertex at an odd level is the minimum of the values of its children.

定义 1　博弈树中顶点的值递归地定义为：

i)一个树叶的值是当游戏在这个树叶所表示的局面里终止时第一个选手的得分。

ii)偶数层内点的值是这个内点的孩子的最大值，奇数层内点的值是这个内点的孩子的最小值。

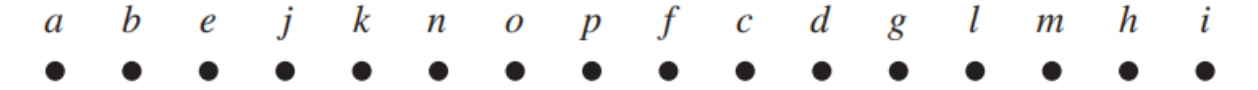
THEOREM 3 The value of a vertex of a game tree tells us the payoff to the first player if both players follow the minmax strategy and play starts from the position represented by this vertex.

定理 3　博弈树顶点的值说明，如果两个选手都遵循最小最大策略并且从博弈树的某一个顶点所表示的局面开始进行游戏，则这个顶点的值表明第一个选手的得分。

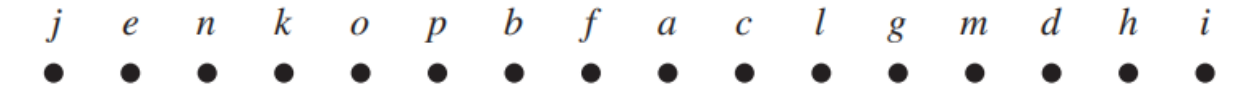
11.3 Tree Traversal

遍历算法

preorder traversal 前序：Visit root, visit subtrees left to right



inorder traversal 中序：Visit leftmost subtree, visit root, visit other subtrees left to right



postorder traversal 后序：Visit subtrees left to right; visit root

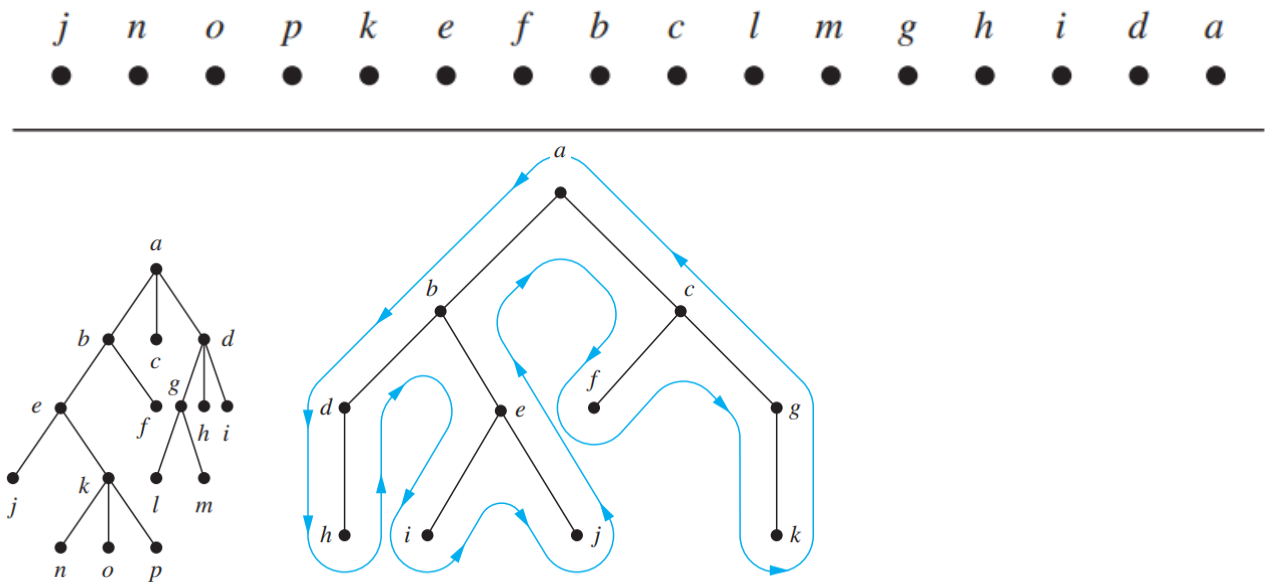


FIGURE 9 **A shortcut for traversing an ordered rooted tree in preorder, inorder, and postorder.**

Infix, Prefix, and Postfix Notation 中缀、前后缀记法

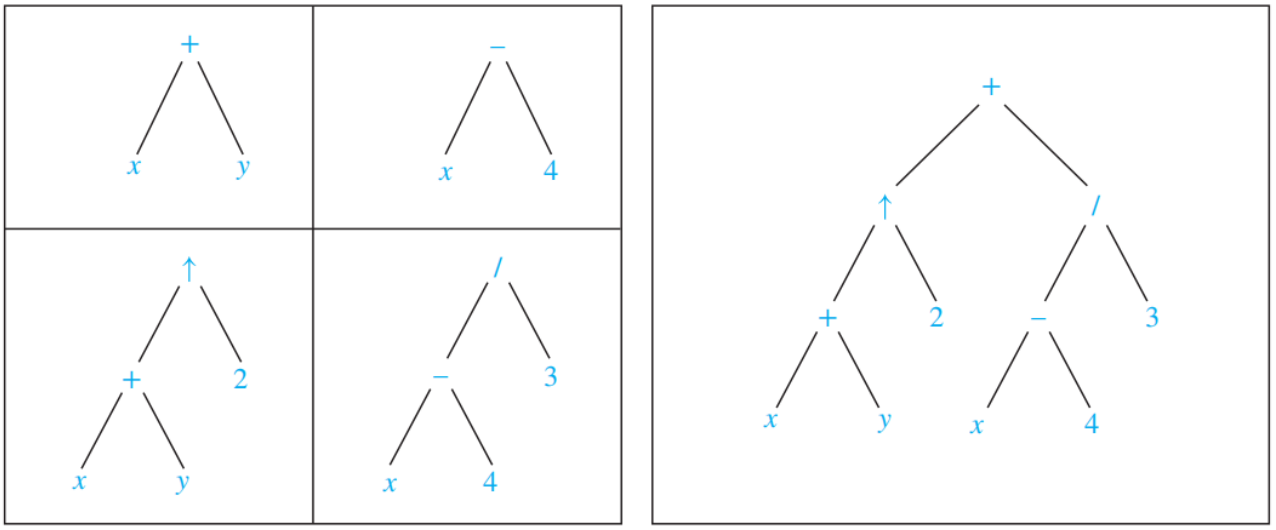


FIGURE 10 **A binary tree representing $((x + y) \uparrow 2) + ((x - 4)/3)$.**

The fully parenthesized expression obtained in this way is said to be in **infifix form.** 中缀

prefix form 前缀

EXAMPLE 6 What is the prefix form for $((x + y) \uparrow 2) + ((x - 4)/3)$?

Solution: We obtain the prefix form for this expression by traversing the binary tree that represents it in preorder, shown in Figure 10. This produces $+ \uparrow + x\ y\ 2\ /\ -\ x\ 4\ 3$. ◀

postfix form 后缀

EXAMPLE 8 What is the postfix form of the expression $((x + y) \uparrow 2) + ((x - 4)/3)$?

Solution: The postfix form of the expression is obtained by carrying out a postorder traversal of the binary tree for this expression, shown in Figure 10. This produces the postfix expression: $x\ y + 2 \uparrow x\ 4 - 3\ /\ +$. ◀

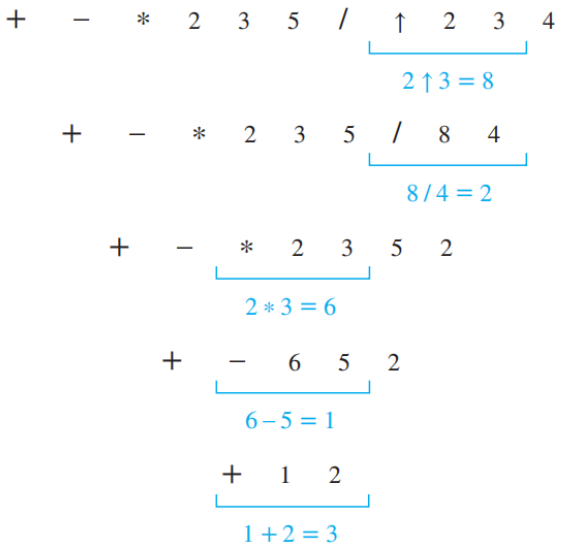


FIGURE 12 **Evaluating a prefix expression.**

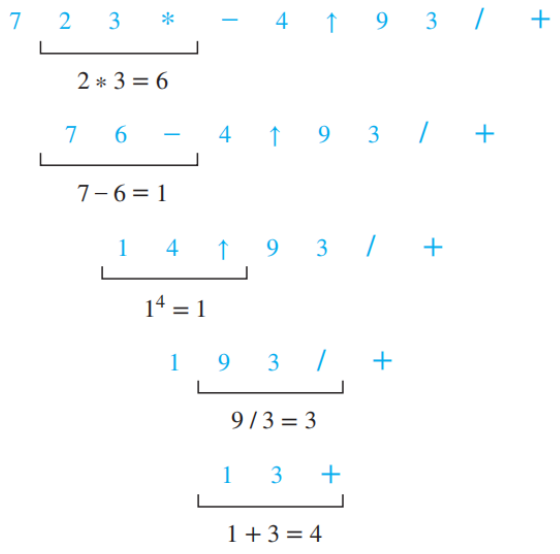


FIGURE 13 **Evaluating a postfix expression.**

例 10 求表示复合命题$(\neg(p \wedge q)) \leftrightarrow (\neg p \vee \neg q)$的有序根树。然后用这个有根树求这个表达式的前缀、后缀和中缀形式。

解 这个复合命题的有序根树是自底向上地构造的。首先，构造$\neg p$和$\neg q$的子树(其中把$\neg$当作一元运算符)。另外，构造$p \wedge q$的子树。然后构造$\neg(p \wedge q)$和$(\neg p) \vee (\neg q)$的子树。最后，用这两个子树来构造最终的有根树。这个过程的步骤显示在图 14 中。

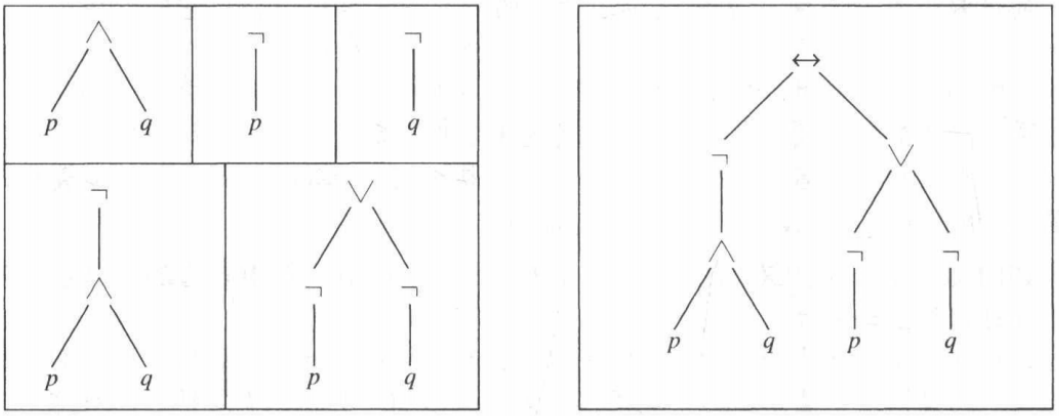


图 14 构造一个复合命题的有根树

求表达式的前缀、后缀和中缀形式时，可以分别以前序、后序和中序来遍历这个有根树(包含括号)。这些遍历分别给出$\leftrightarrow \neg \wedge pq \vee \neg p \neg q$、$pq \wedge \neg p \neg q \neg \vee \leftrightarrow$和$(\neg(p \wedge q)) \leftrightarrow ((\neg p) \vee (\neg q))$。◀

因为前缀表达式和后缀表达式都是无二义性的，而且不用来回扫描就容易求出它们的值，所以它们在计算机科学里大量使用。这样的表达式对编译器的构造是特别有用的。

11.4 Spanning Trees

生成树

Definition 1 Let G be a simple graph. A *spanning tree* of G is a subgraph of G that is a tree containing every vertex of G.

定义 1 设 G 是简单图。G 的生成树是包含 G 的每个顶点的 G 的子图。

THEOREM 1 A simple graph is connected if and only if it has a spanning tree.

定理 1 简单图是连通的当且仅当它有生成树。

depth-first search 深度优先搜索 also called **backtracking** 回溯

例 3 用深度优先搜索来找出图 6 所示图 G 的生成树。

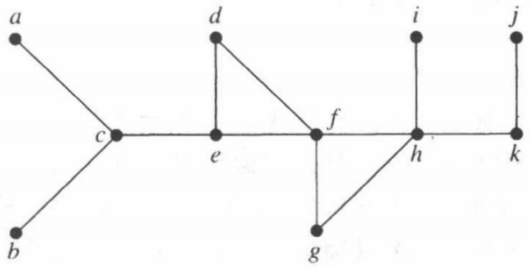
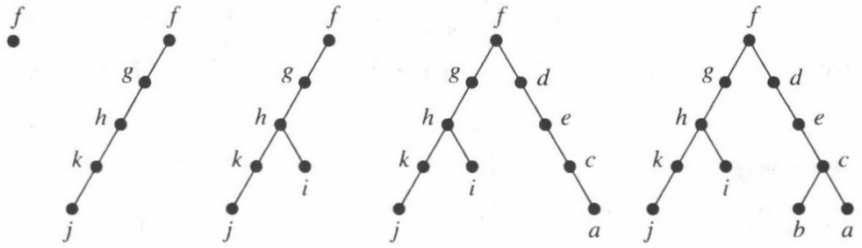


图 6 图 G

解 图 7 显示了用深度优先搜索产生 G 的生成树的步骤。任意地从顶点 f 开始。一条通路是这样建立的：依次添加与还不在通路上的顶点相关联的边，只要有可能就这样做。这样就产生通路 f，g，h，k，j(注意也可能建立其他的通路)。下一步，回溯到 k。不存在从 k 开始，包含还没有访问过的顶点的通路。所以回溯到 h。形成通路 h，i。然后回溯到 g，然后再回溯到 f。从 f 建立通路 f，d，e，c，a。然后再回溯到 c 并且形成通路 c，b。这样就产生了生成树。 ◀



Depth-first search (also called backtracking) -- this procedure forms a rooted tree, and the underlying undirected graph is a spanning tree.

1. **Arbitrarily choose a vertex of the graph as root.**
2. **From a path starting at this vertex by successively adding edges, where each new edge is incident with the last vertex in the path and a vertex not already in the path.**
3. **Continue adding edges to this path as long as possible.**
4. **If the path goes through all vertices of the graph, the tree consisting of this path is a spanning tree.**
5. **If the path does not go through all vertices, more edges must be added. Move back to the next to last vertex in the path, if possible, form a new path starting at this vertex passing through vertices that were not already visited. If this cannot be done, move back another vertex in the path.**
6. **Repeat this process.**

1. 任意选择图形的一个顶点作为根。
2. 从这个顶点开始的路径，连续添加边，其中每条新的边都与路径中的最后一个顶点和一个还没不在路径中的顶点相连
3. 继续向这条路径添加边，越长越好。

4. 如果该路径穿过图形的所有顶点，那么由该路径组成的树就是一棵生成树。

5. 如果路径没有穿过所有顶点，就必须增加更多的边。如果可能的话，回到路径中的最后一个顶点，形成一条新的路径。从这个顶点开始，穿过尚未访问的顶点。如果做不到这一点，就向后移动路径中的另一个顶点。

6. 重复这个过程。

一个图的深度优先搜索所选择的边称为**树边**。这个图所有其他的边都必然连接一个顶点与这个顶点在树中的祖先或后代。这些边都称为**背边**(练习 43 要求证明这个事实)。

例 4 图 8 中突出了从顶点 f 开始的深度优先搜索所找到的树边，用粗线显示这些树边。用细黑线显示背边(e, f)和(f, h)。◀

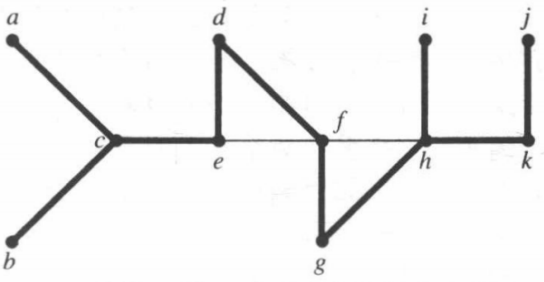


图 8　例 4 中深度优先搜索的树边和背边

tree edges and back edges

Breadth-first search

1. **Arbitrarily choose a vertex of the graph as a root, and add all edges incident to this vertex.**
2. **The new vertices added at this stage become the vertices at level 1 in the spanning tree. Arbitrarily order them.**
3. **For each vertex at level 1, visited in order, add each edge incident to this vertex to the tree as long as it does not produce a simple circuit. Arbitrarily order the children of each vertex at level 1. This produces the vertices at level 2 in the tree.**
4. **Follow the same procedure until all the vertices in the tree have been added.**

1.任意选择图的一个顶点作为根，并将所有与该顶点相关的边相连。
2.在此阶段添加的新顶点将成为生成树中的级别1。任意排序他们。
3.对于级别1的每个顶点，按顺序访问，添加每个边只要它不产生简单的回路，就可以入射到树的这个顶点。任意排序级别为1的每个顶点的子顶点。这将生成树中级别为2的顶点。
4.按照相同的过程进行操作，直到添加了树中的所有顶点。

11.5 Minimum Spanning Trees

spanning tree: a tree containing all vertices of a graph
生成树：包含图的所有顶点的树
minimum spanning tree: a spanning tree with smallest possible sum of weights of its edges
最小生成树：边的权之和最小

Definition 1 A *minimum spanning tree* in a connected weighted graph is a spanning tree that has the smallest possible sum of weights of its edges.

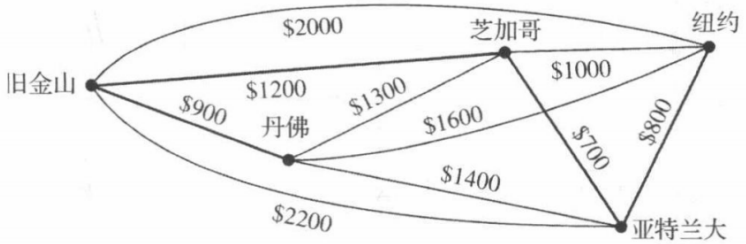
Prim's algorithm 普林算法

普林算法(Prim's algorithm)：产生加权图里最小生成树的过程，通过依次添加与已经在树里的顶点相关联的所有边中权最小的边，使得再添加边时不会产生简单回路。

克鲁斯卡尔算法(Kruskal's algorithm)：产生加权图里最小生成树的过程，通过依次添加还不在树里的权最小的边，使得再添加边时不会产生简单回路。

例 1 用普林算法设计连接图 1 所表示的所有计算机的具有最小成本的通信网络。

解 办法是求图 1 的最小生成树。普林算法是这样执行的：选择权最小的初始边，并且依次添加与树里顶点关联的不形成回路的权最小的边。在图 2 中，加颜色的边表示普林算法所产生的最小生成树，并且显示在每个步骤上所做的选择。 ◀



选择	边	权
1	{芝加哥，亚特兰大}	$ 700
2	{亚特兰大，纽约}	$ 800
3	{芝加哥，旧金山}	$1200
4	{旧金山，丹佛}	$ 900
	总计：	$3600

图 2　图 1 加权图的最小生成树

读者应当注意普林算法与克鲁斯卡尔算法的区别。在普林算法里，选择与已在树中的一个顶点相关联且不形成回路的权最小的边；相对地，在克鲁斯卡尔算法里，选择不一定与已在树中的一个顶点相关联且不形成回路的权最小的边。注意，在普林算法里，若没有对边排序，则在这个过程的某个阶段上，对添加的边来说就可能有多于一种的选择。因此，为了让这个过程是确定的，就需要对边进行排序。例 3 说明如何使用克鲁斯卡尔算法。