DISCRETE MATHEMATICS
（离散数学）

云南大学数学系
李 建 平

Chapter 6 Order Relations and Structures

6.1 PARTIALLY ORDERED SETS

A relation R on a set A is called a **partial order** (偏序) if R is reflexive, antisymmetric, and transitive. The set A together with the partial order R is called a **partially ordered set** (偏序集合), or simply a **poset,** and we will denoted this poset by (A,R).

EXAMPLE 1

Let A be a collection of subsets of a set S. The relation $\subseteq$ of set inclusion is a partial order on A, so $(A, \subseteq)$ is a poset.

EXAMPLE 3

The relation of divisibility (aRb if and only if $a|b$) is a partial order on Z^+.

EXAMPLE 6

Let R be a partial order on a set A, and let R^{-1} be the inverse relation of R. Then R^{-1} is also a partial order. To see this, we recall the characterization of reflexive, antisymmetric, and transitive given in Section 4.4. If R has these three properties, then $\Delta \subseteq R, R \cap R^{-1} \subseteq \Delta, R^2 \subseteq R$.

By taking inverses, we have

$$\Delta = \Delta^{-1} \subseteq R^{-1}, R^{-1} \cap (R^{-1})^{-1} = R^{-1} \cap R \subseteq \Delta$$

$$(R^{-1})^2 \subseteq R^{-1}$$

So, by Section4.4, R^{-1} is reflexive, antisymmetric, and transitive. Thus R^{-1} is also a partial order.

The poset (A, R^{-1}) is called the **dual** of the poset (A, R) . and the partial order R^{-1} is called the **dual** of the partial order R .

Whenever $(A, \leq)$ is a poset, we will always use the symbol $\geq$ for the partial order $\leq^{-1}$, and thus $(A, \geq)$ will be the dual poset.

If $(A, \leq)$ is a poset, the elements a and b of A are said to be **comparable** if

$$a \leq b \quad \text{or} \quad b \leq a$$

If every pair of elements in a poset A is comparable, we say that A is a **linearly ordered** set, and the partial order is called a **linear order** (线性序). We also say that A is a **chain**（链）.

Theorem 1 If $(A, \leq)$ and $(B, \leq)$ are two posets, then $(A \times B, \leq)$ is a poset, with partial order $\leq$ defined by

$(a, b) \leq (a', b')$ if $a \leq a'$ in A and $b \leq b'$ in B.

Note that the symbol $\leq$ is being used to denote three distinct partial orders. The reader should find it easy to determine which of the three partial orders is meant at any time.

If $(A, \leq)$ is a poset, we say that $a < b$ if $a \leq b$ but $a \neq b$. Another useful partial order on $A \times B$ denote by $\prec$, is defined as follows:

$(a, b) \prec (a', b')$ if $a < a'$ or if $a = a'$ and $b \leq b'$

This ordering is called **lexicographic** (字典序), or "dictionary" order. If $(A, \leq)$ and $(B, \leq)$ are linearly ordered sets, then the lexicographic order $\prec$ on

$A \times B$ is also a linear order.

Lexicographic ordering is easily extended to Cartesian products $A_1 \times A_2 \times \cdots \times A_n$ as follows:

$(a_1, a_2, \cdots, a_n) \prec (a_1', a_2', \cdots, a_n')$ if and only if

$$a_1 < a_1' \quad \text{or}$$

$$a_1 = a_1' \quad \text{and} \quad a_2 < a_2' \quad \text{or}$$

$$a_1 = a_1', a_2 = a_2', \quad \text{and} \quad a_3 < a_3' \quad \text{or} \cdots$$

$$a_1 = a_1', a_2 = a_2', \cdots, a_{n-1} = a_{n-1}' \quad \text{and} \quad a_n \le a_n'$$

Theorem 2 The digraph of a partial order has no cycle of length greater than 1.

Proof Suppose that the digraph of the partial order $\leq$ on the set A contains a cycle of length $n \geq 2$. Then there exist distinct elements $a_1, a_2, \cdots, a_n \in A$ such that

$$a_1 \leq a_2, a_2 \leq a_3, \cdots, a_{n-1} \leq a_n, a_n \leq a_1.$$

By the transitivity of the partial order, used $n-1$ times, $a_1 \leq a_n$. By antisymmetry, $a_1 \leq a_n$ and $a_n \leq a_1$ imply that $a_n = a_1$, a contradiction to the assumption that $a_1, a_2, \cdots, a_n$ are distinct.

- Hasse Diagrams (海赛图)

Let A be a finite set, the digraph of a partial order on A has only cycles of length 1, we shall delete all such cycles from the digraph.

We shall also eliminate all edges that are implied by the transitive property. If a $\leqslant$b and b$\leqslant$c, it follows that a $\leqslant$c. So we omit the arc from a to c, we do draw the arcs from a to b and from b to c.

We also draw the digraph of a partial order with all arcs pointing upward, arrows may be omitted from the arcs, finally we replace the circles representing the vertices by dots. The resulting diagram of a partial order is called the **Hasse**

diagram of the partial order of the poset.

EXAMPLE 12

Let $S=\{a,b,c\}$ and $A=P(S)$. Draw the Hasse diagram of the poset A with the partial order $\subseteq$ (set inclusion).

Solution We first determine A, obtaining

$$A=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$$

The Hasse diagram can then be drawn as shown in Figure 6.7.

It is easily seen that if $(A,\leq)$ is a poset and $(A,\geq)$ is the dual poset, then the Hasse diagram of $(A,\geq)$

is just the Hasse diagram of $(A, \leq)$ turned upside down.

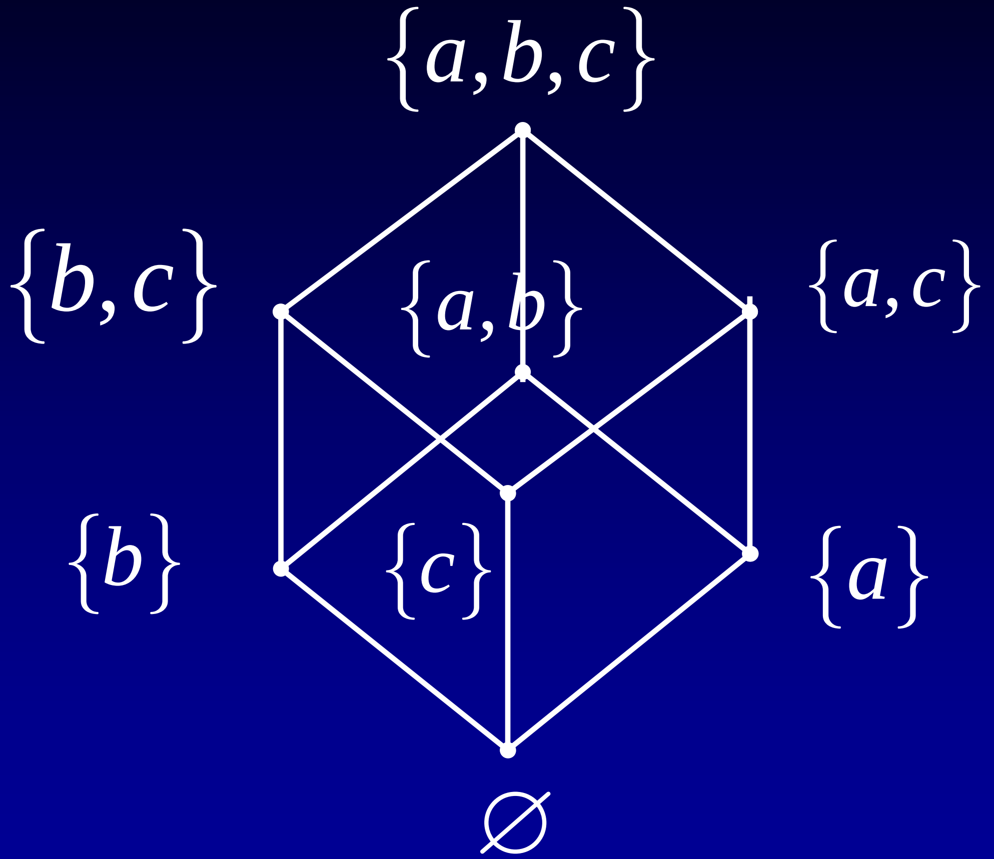
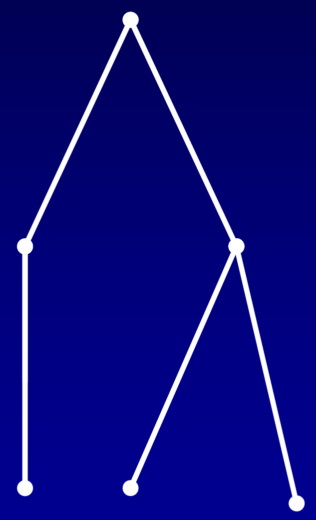


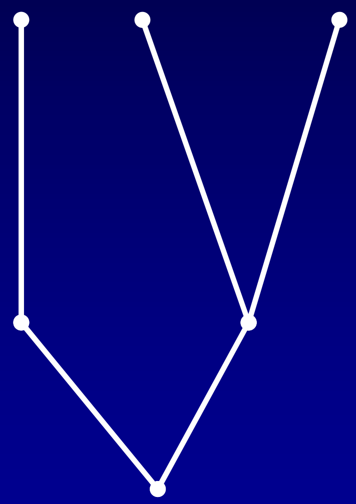
Figure 6.7

EXAMPLE 13

Figure 6.9 (a) shows the Hasse diagram of poset $(A, \leq)$, where $A = \{a, b, c, d, e, f\}$. Figure 6.9 (b) shows the Hasse diagram of the dual poset $(A, \geq)$.



(a)



(b)

Figure 6.9

- Topological sorting (拓扑排序)

If A is a poset with partial order $\leq$, we sometimes need to find a linear order $\prec$ for the set A that will merely be an extension of the given partial order in the sense that if $a \leq b$ then $a \prec b$.

The process of constructing a linear order such as $\prec$ is called **topological sorting.** This problem might arise when we have to enter a finite poset A into a computer. If $a \leq b$, then a is entered before b. A topological sorting $\prec$ will give an order of entry of the elements that meets this condition.

Isomorphism (同构)

Let $(A, \leq)$ and $(A', \leq')$ be posets and let $f : A \to A'$ be a one-to-one correspondence between A and A'. The function f is called an **isomorphism** form $(A, \leq)$ to $(A', \leq')$ if, for any a and b in A,

$$a \leq b \quad \text{if and only if} \quad f(a) \leq' f(b)$$

If $f : A \to A'$ is an isomorphism, we say that $(A, \leq)$ and $(A', \leq')$ are **isomorphic** posets (同构偏序集合).

Theorem 3 (Principle of Correspondence)

If the elements of B have any property relating to one another or to other elements of A, and if this property can be defined entirely in terms of the relation $\leq$, then the elements of B' must possess exactly the same property, defined in terms of $\leq'$.

It follows from the principle of correspondence that two finite isomorphic posets must have the same Hasse diagrams.

To be precise, let $(A, \leq)$ and $(A', \leq')$ be finite posets, let $f: A \to A'$ be a one-to-one correspondence, and let H be any Hasse diagram of $(A, \leq)$. Then

1. If f is an isomorphism and each label a of H is replaced by $f(a)$, then H will become a Hasse diagram for $(A', \leq')$.

Conversely,

2. If H becomes a Hasse diagram for $(A^{'} \leq^{'})$, whenever each label a is replace by $f(a)$, then f is an isomorphism.

EXAMPLE 17

Let $A=\{1,2,3,6\}$ and let $\leq$ be the relation “|” (divides). Figure 6.13(a) shows the Hasse diagram for $(A,\leq)$. Let

$$A^{'} = P\left(\{a,b\}\right) = \{\varnothing,\{a\}\{b\},\{a,b\}\}$$

and let $\leq^{'}$ be set containment, $\subseteq$. If $f : A \to A'$ is defined by

$$f(1)=\varnothing,\ f(2)=\{a\},\ f(3)=\{b\},\ f(6)=\{a,b\}$$

Then it is easily seen that f is a one-to-one correspondence. If each label $a \in A$ of the Hasse diagram is replaced by $f(a)$, the result is as shown in Figure 6.13(b). Since this is clearly a Hasse diagram for $(A', \leq')$, the function f is an isomorphism.

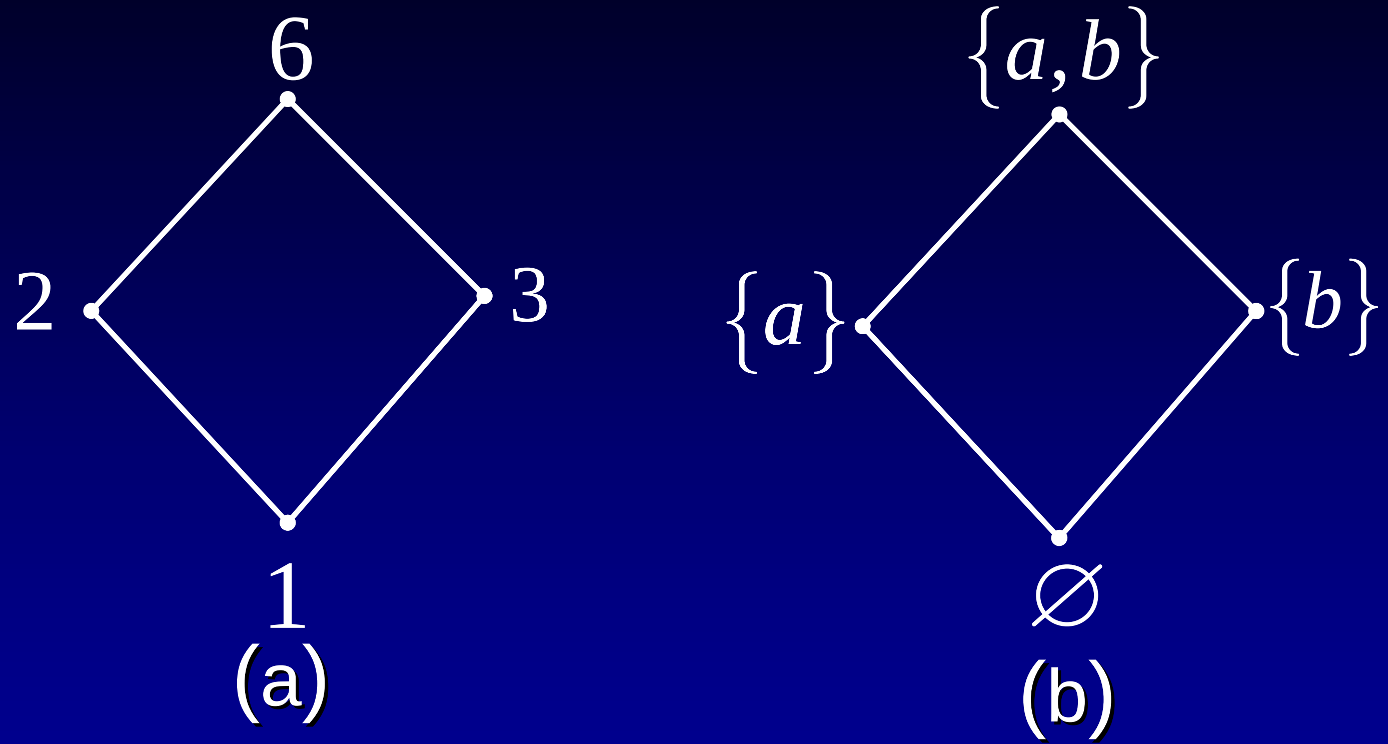


Figure 6.13

6.2 EXTREMAL ELEMENTS OF PARTIALLY ORDERED SETS

An element $a \in A$ is called a **maximal element** of A if there is no element c in A such that $a < c$ (see Section 6.1). An element $b \in A$ is called a **minimal element** of A if there is no element c in A such that $c < b$.

If $(A, \leq)$ is a poset and $(A, \geq)$ is its dual poset, an element $a \in A$ is a maximal element of $(A, \geq)$ if and only if a is a minimal element of $(A, \leq)$. Also, a is a minimal element of $(A, \geq)$ if and only if it is a maximal element of $(A, \leq)$.

Theorem 1 Let A be a finite nonempty poset with partial order $\leq$. Then A has at least one maximal element and at least one minimal element.

Proof Let a be any element of A . If a is not maximal, we can find an element $a_1 \in A$ such that $a < a_1$. If a_1 is not maximal, we find an element $a_2 \in A$ such that $a_1 < a_2$. This argument cannot be continued indefinitely, since A is a finite set. Thus we eventually obtain the finite chain

$$a < a_1 < a_2 < \cdots < a_{k-1} < a_k,$$

which cannot be extended. Hence we cannot have $a_k < b$ for $b \in A$, so a_k is a maximal element of $(A, \leq)$.

This same argument says that the dual poset $(A, \geq)$ has a maximal element, so $(A, \leq)$ has a minimal element.

We can give an algorithm for finding a topological sorting of a given finite poset $(A, \leq)$. SORT is ordered by increasing index, that is, SORT[1] $\prec$ SORT[2] $\prec \cdots$, The relation on $\prec$ defined in this way is a topological sorting of $(A, \leq)$.

- ALGORITHM for finding a topological sorting of a finite poset $(A, \leq)$.

Step 1 Choose a **minimal element** a of A.

Step 2 Make a the next entry of SORT and replace A with $A - \{a\}$.

Step 3 Repeat Steps 1 and 2 until $A = \varnothing$.

End of Algorithm

EXANPLE 4

Let $A = \{a, b, c, d, e\}$, and let the Hasse diagram of a partial order $\leq$ on A be as shown in

Figure 6.23(a). Figure 6.23(f) shows the completed array SORT and the Hasse diagram of the poset corresponding to SORT.

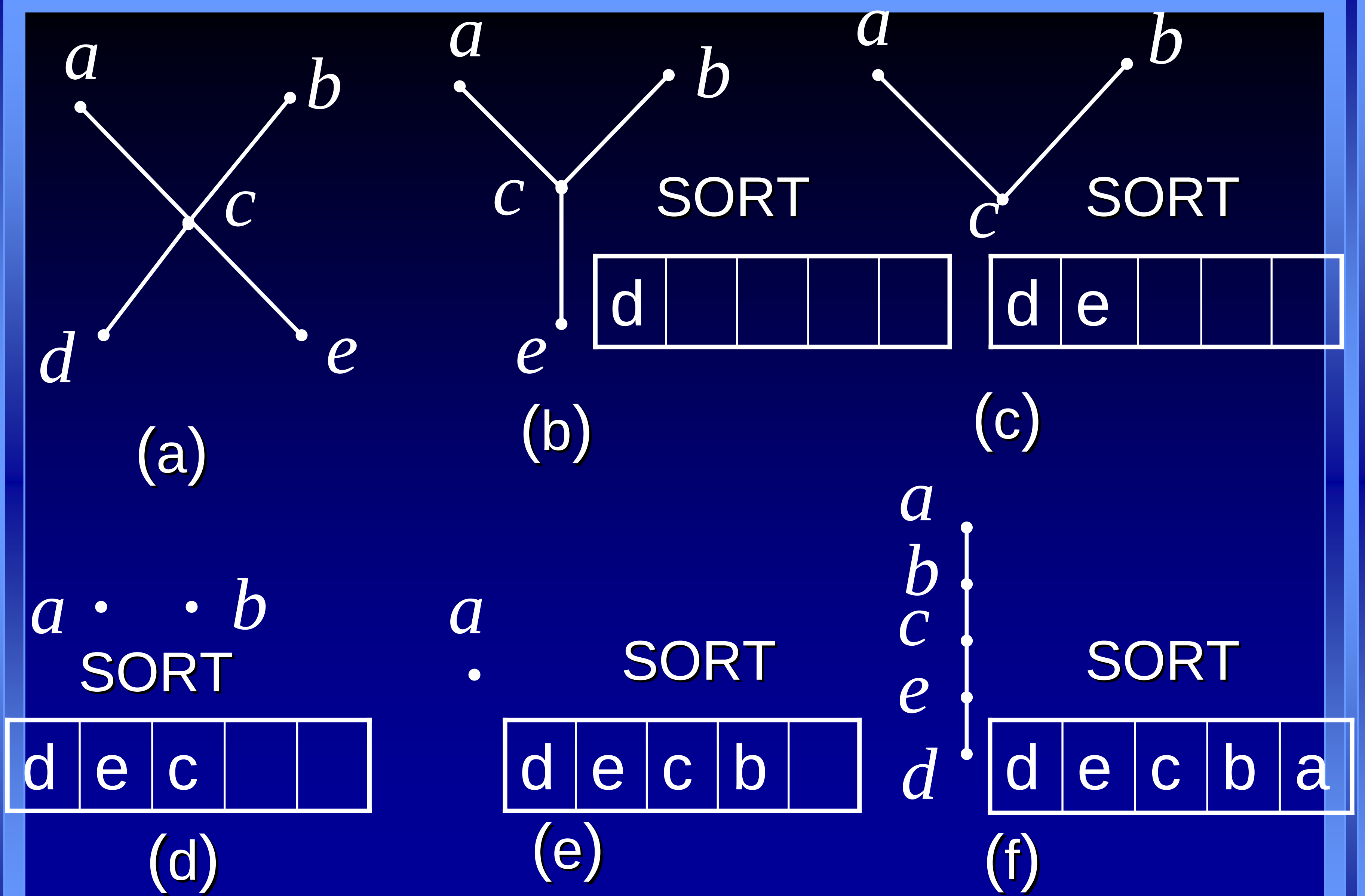

a
b
c
d
e
(a)
a
b
c
e
SORT
d
(b)
a
b
c
SORT
d e
(c)
a
b
SORT
d e c
(d)
a
SORT
d e c b
(e)
a
b
c
e
d
SORT
d e c b a
(f)

Figure 6.23

An element $a \in A$ is called a **greatest element** of A if $x \leq a$ for all $x \in A$. An element $a \in A$ is called a **least element** of A if $a \leq x$ for all $x \in A$.

An element a of $(A, \leq)$ is a greatest (or least) element if and only if it is a least (or greatest) element of $(A, \geq)$.

Theorem 2 A poset has at most one greatest element and at most one least element.

Proof Suppose that a and b are greatest elements of poset A. Then, since b is a greatest element, we have $a \leq b$. Similarly, since a is a greatest element, we have $b \leq a$. Hence $a = b$ by the antisymmetry property. Thus, if the poset has a greatest element, it only has one such element. Since this fact is true for all posets, the dual poset $(A, \geq)$ has at most one greatest element. So $(A, \leq)$ also has at most one least element.

The greatest element of a poset, if it exists, is denoted by I and is often called the **unit element**.

Similarly, the least element of a poset, if it exists, is denoted by 0 and is often called the **zero element**.

Consider a poset and a subset B of A.

An element $a \in A$ is called an **upper bound** of B if $b \leq a$ for all $b \in B$. An element $a \in A$ is called a **lower bound** of B if $a \leq b$ for all $b \in B$.

Let A be a poset and B a subset of A. An element $a \in A$ is called a **least upper bound** (LUB) of B if a is an upper bound of B and $a \leq a'$, whenever a' is an upper bound of B. Thus a =LUB(B) if $b \leq a$ for all $b \in B$, and if whenever $a' \in A$ is also an upper bound of B, then $a \leq a'$. An element $a \in A$ is called a **greatest lower bound** (GLB) of B if a is a lower bound of B and $a' \leq a$, whenever a' is a lower bound of B.

Theorem 3 Let $(A, \leq)$ be a poset. Then a subset B of A has at most one LUB and at most one GLB.

We conclude this section with some remarks about LUB and GLB in a finite poset A, as viewed from the Hasse diagram of A. Let $B = \{b_1, b_2, \cdots, b_r\}$. If a = LUB(B), then a is the first vertex that can be reached from $b_1, b_2, \cdots, b_r$ by upward paths.

If a =GLB(B), then a is the first vertex that can be reached from $b_1, b_2, \cdots, b_r$ by downward paths.

Theorem 4 Suppose that $(A, \leq)$ and $(A^{'} \leq^{'})$ are isomorphic posets under the isomorphism $f : A \rightarrow A'$.

(a) If a is a maximal (minimal) element of $(A, \leq)$, then $f(a)$ is a maximal (minimal) element of $(A^{'} \leq^{'})$.

(b) If a is the greatest (least) element of $(A, \leq)$, then $f(a)$ is the greatest (least) element of $(A^{'} \leq^{'})$.

(c) If a is an upper bound (lower bound, least upper bound, greatest lower bound) of a subset B of A, then $f(a)$ is an upper bound (lower bound, least upper bound, greatest lower bound) for the subset $f(B)$ of A' .

(d) If every subset of $(A, \leq)$ has a LUB(GLB), then every subset of $(A' \leq')$ has a LUB(GLB).

6.3 LATTICES (格)

A **lattice** is a poset $(L, \leq)$ in which every subset $\{a, b\}$ consisting of two elements has a least upper bound and a greatest lower bound. We denote LUB($\{a, b\}$) by $a \vee b$ and call it the **join** of a and b. Similarly, we denote GLB($\{a, b\}$) by $a \wedge b$ and call it the **meet** of a and b.

EXAMPLE 1

Let S be a set and let $L = P(S)$. As we have seen, $\subseteq$,containment, is a partial order on L . Let A and B

belong to the poset $(L, \subseteq)$. Then $A \vee B$ is the set $A \cup B$. The element $A \wedge B$ in $(L, \subseteq)$ is the set $A \cap B$. Thus, L is a lattice.

EXAMPLE 2

Consider the poset $L = (Z^+, \leq)$, where for a and b in Z^+, $a \leq b$ if and only if $a \mid b$. Then L is a lattice in which the join and meet of a and b are their least common multiple and greatest common divisor, respectively (see Section 1.4). That is,

$a \vee b$ =LCM (a, b) and $a \wedge b$=GCD(a, b)

EXAMPLE 3

Let n be a positive integer and let D_n be the set of all positive divisors of n . Then D_n is a lattice under the relation of divisibility as considered in the example 2.

Let $(L,\leq)$ be a poset and let $(L,\geq)$ be the dual poset $(L,\geq)$. If $(L,\leq)$ is a lattice, we can show that $(L,\geq)$ is also a lattice. In fact, for any a and b in L , the least upper bound of a and b in $(L,\leq)$ is equal to the greatest lower bound of a and b in $(L,\geq)$.

Theorem 1 If $(L_1,\leq)$ and $(L_2,\leq)$ are lattices, then

$(L, \leq)$ is a lattice, where $L = L_1 \times L_2$, and the partial order $\leq$ of L is the product partial order.

Proof We denote the join and meet in L_1 by $\vee_1$ and $\wedge_1$, respectively, and the join and meet in L_2 by $\vee_2$ and $\wedge_2$, respectively. We already know from Theorem 1 of Section 6.1 that L is a poset. We now need to show that if (a_1, b_1) and $(a_2, b_2) \in L$, then $(a_1, b_1) \vee (a_2, b_2)$ and $(a_1, b_1) \wedge (a_2, b_2)$ exist in L.

We can verify that

$$(a_1, b_1) \vee (a_2, b_2) = (a_1 \vee_1 a_2, b_1 \vee_2 b_2)$$

$$(a_1, b_1) \wedge (a_2, b_2) = (a_1 \wedge_1 a_2, b_1 \wedge_2 b_2)$$

Thus L is a lattice.

Properties of Lattices

We recall the meaning of $a \vee b$ and $a \wedge b$.

1. $a \leq a \vee b$ and $b \leq a \vee b$; $a \vee b$ is an upper bound of a and b .

2. If $a \leq c$ and $b \leq c$, then $a \vee b \leq c$; $a \vee b$ is the least upper bound of a and b .

1'. $a \wedge b \leq a$ and $a \wedge b \leq b$; $a \wedge b$ is a lower bound of a and b .

2'. If $c \leq a$ and $c \leq b$, then $c \leq a \wedge b$; $a \wedge b$ is bound of a and b.

Theorem 2

Let L be a lattice. Then for every a and b in L,

(a) $a \vee b = b$ if and only if $a \leq b$.

(b) $a \wedge b = a$ if and only if $a \leq b$.

(c) $a \wedge b = a$ if and only if $a \vee b = b$.

Theorem 3 Let L be a lattice. Then

1. Idempotent Properties（幂等性）

(a) $a \vee a = a$

(b) $a \wedge a = a$

2. Commutative Properties（交换性）

(a) $a \vee b = b \vee a$

(b) $a \wedge b = b \wedge a$

3. Associative Properties（结合性）

(a) $a \vee (b \vee c) = (a \vee b) \vee c$

(b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

4. Absorption Properties（吸收性）

(a) $a \vee (a \wedge b) = a$

(b) $a \wedge (a \vee b) = a$

Theorem 4 Let L be a lattice. Then, for every a, b, and c in L,

1. If $a \le b$, then

   (a) $a \vee c \le b \vee c$

   (b) $a \wedge c \le b \wedge c$

2. $a \le c$ and $b \le c$ if and only if $a \vee b \le c$.

3. $c \le a$ and $c \le b$ if and only if $c \le a \vee b$.

4. If $a \le b$ and $c \le d$, then

   (a) $a \vee c \le b \vee d$

   (b) $a \wedge c \le b \wedge d$

- Special Types of Lattices

A lattice L is said to be **bounded** if it has a greatest element I and a least element 0.

Theorem 5 Let $L = \{a_1, a_2, \cdots, a_n\}$ be a finite lattice. Then L is bounded.

Proof the greatest element of L is $a_1 \vee a_2 \vee \cdots \vee a_n$, and its least element is $a_1 \wedge a_2 \wedge \cdots \wedge a_n$.

A lattice L is called **distributive** if for any elements a , b , and c in L , we have the following **distributive properties**（分配性）:

1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

If L is not distributive, we say that L is **nondistributive.**

EXAMPLE 18 Show that the lattices picture in Figure 6.44 are nondistributive.

Solution

(a) We have

$$a \wedge (b \vee c) = a \wedge I = a$$

while $(a \wedge b) \vee (a \wedge c) = b \vee 0 = b$.

(b) Observe that $a \wedge (b \vee c) = a \wedge I = a$

while $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$.

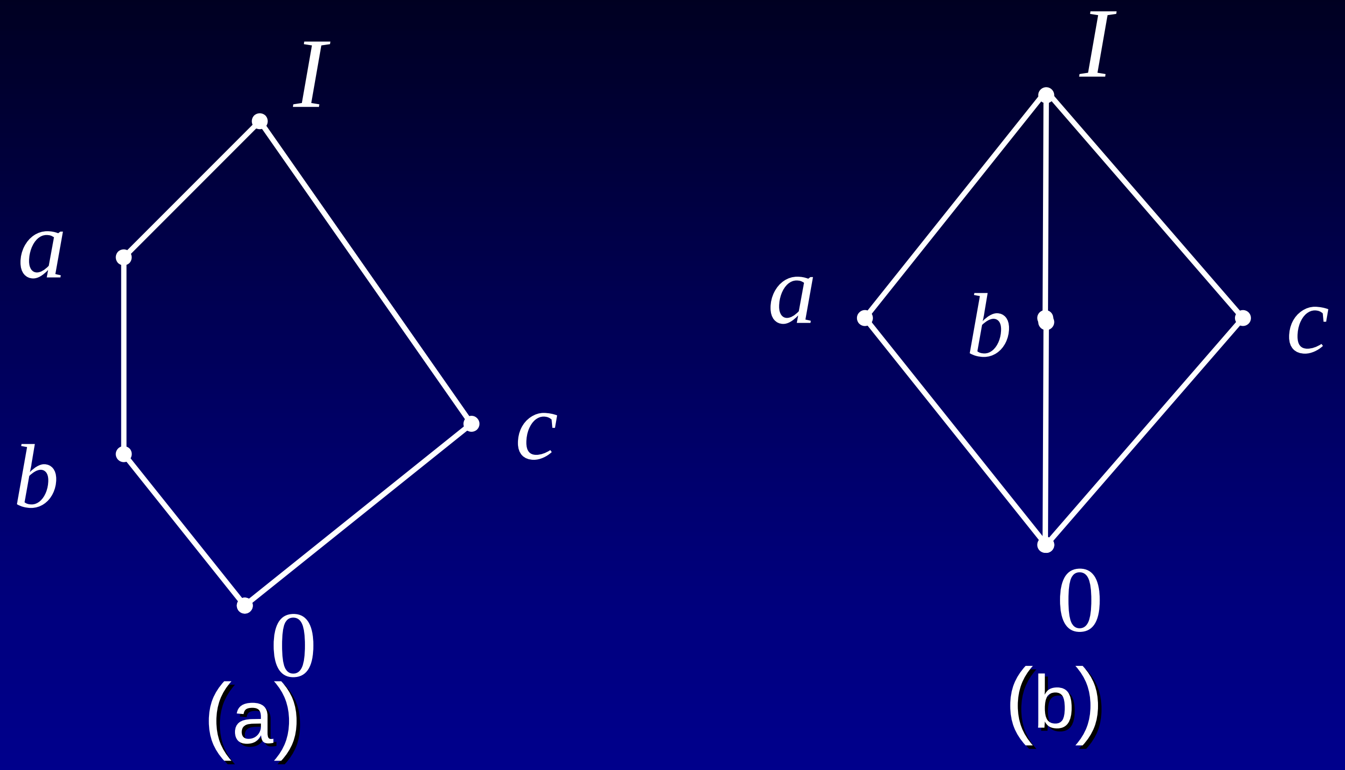


Figure 6.44

Theorem 6 A lattice L is nondistributive if and only if it contains a sublattice that is isomorphic to one of the two lattices of Example 18.

Let L be a bounded lattice with greatest element I and least element 0, and let $a \in L$. An element $a' \in L$ is called a **complement** (补) of a if

$$a \vee a' = I \text{ and } a \wedge a' = 0 .$$

Theorem 7 Let L be a bounded distributive lattice. If a complement exists, then it is unique.

A lattice L is called complemented if it is bounded and if every element in L has a complement.

6.4 FINITE BOOLEAN ALGEBRAS

We restrict our attention to the lattices $(P(S), \subseteq)$, where S is a finite set.

Theorem 1 If $S_1 = \{x_1, x_2, \cdots, x_n\}$ and $S_2 = \{y_1, y_2, \cdots, y_n\}$ are any two finite sets with n elements, then the lattices $(P(S_1), \subseteq)$ and $(P(S_2), \subseteq)$ are isomorphic. Consequently, the Hasse diagrams of these lattices may be drawn identically.

Proof Arrange the sets as show in Figure 6.58 so that each element of S_1 is directly over the correspondingly numbered element in S_2. For each subset A of S_1, let $f(A)$ be the subsets of S_2 consisting of all elements that correspond to the elements of A. Figure 6.59 shows a typical subset A of S_1 and the corresponding subset $f(A)$ of S_2. It is easily seen that the function f is a one-to-one correspondence from subsets of S_1 to subsets of S_2. Equally clear is the fact that if A and B are any subsets of S_1, then $A \subseteq B$ if and only if $f(A) \subseteq f(B)$.

Thus the lattices $(P(S_1), \subseteq)$ and $(P(S_2), \subseteq)$ are isomorphic.

$$\begin{array}{cccccc}
S_1: & x_1 & x_2 & \cdots & x_n \\
& \updownarrow & \updownarrow & & \updownarrow \\
S_2: & y_1 & y_2 & \cdots & y_n
\end{array}$$

Figure 6.58

$$S_1: x_1 \ \overset{A}{\boxed{x_2 \quad x_3 \quad x_4}} \cdots x_n$$

$$S_2: y_1 \ \overset{f(A)}{\boxed{y_2 \quad y_3 \quad y_4}} \cdots y_n$$

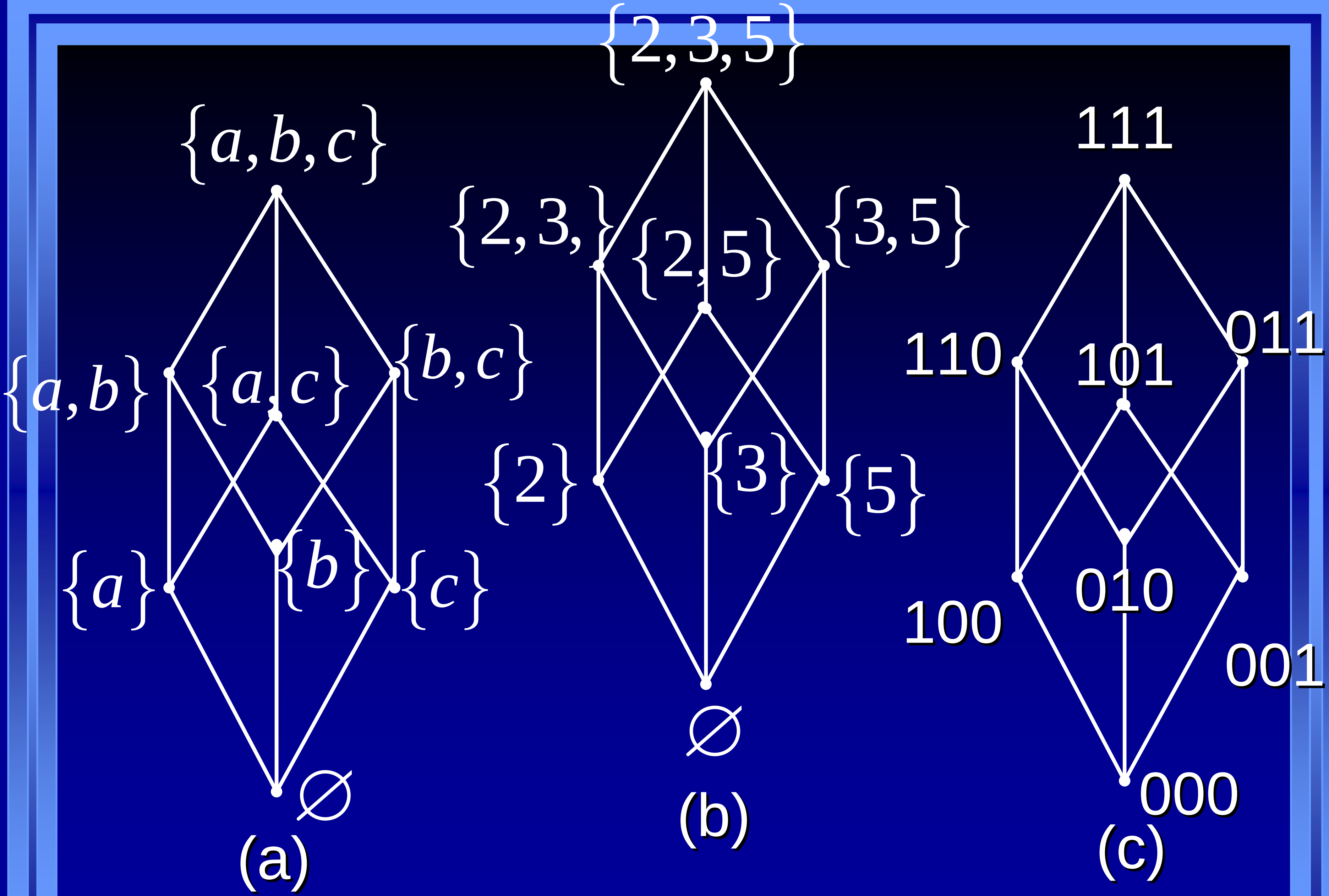
Figure 6.59

The essential point of this theorem is that the lattice $(P(S),\subseteq)$ is completely determined as a poset by the number $|S|$ and does not depend in any way on the nature of the element in S .

Thus, for each $n=0,1,2,\cdots,$ there is only one type of lattice having the from $(P(S),\subseteq)$. This lattice depends only on n , not on S ,and it has 2^n elements. If a set S has n elements, then all subsets of S can be represented by sequences of 0's and 1's of length n . We can therefore label the Hasse diagram of a lattice $(P(S),\subseteq)$ by such sequences.

EXAMPLE 2

Figure 6.60(c) shows how the diagrams that appear in Figure 6.60(a) and (b) can be labeled by sequences of 0’s and 1’s. This labeling serves equally well to describe the lattice of Figure 6.60(a) or (b), or for that matter the lattice $(P(S), \subseteq)$ that arises from any set S having three elements.



$\{a,b,c\}$
$\{a,b\}$
$\{a,c\}$
$\{b,c\}$
$\{a\}$
$\{b\}$
$\{c\}$
$\varnothing$
(a)
$\{2,3,5\}$
$\{2,3,\}$
$\{2,5\}$
$\{3,5\}$
$\{2\}$
$\{3\}$
$\{5\}$
$\varnothing$
(b)
111
110
101
011
010
100
001
000
(c)

Figure 6.60

If the Hasse diagram of the lattice corresponding to a set with n elements is labeled by sequences of 0's and 1's of length n , as described previously, then the resulting lattice is named B_n. The properties of the partial order on B_n can be described directly as follows. If $x = a_1 a_2 \cdots a_n$ and $y = b_1 b_2 \cdots b_n$ are two elements of B_n , then

1. $x \leq y$ if and only if $a_k \leq b_k$ (as numbers 0 or 1) for $k = 1, 2, \cdots n$.
2. $x \wedge y = c_1 c_2 \cdots c_n$, where c_k =min$\{a_k, b_k\}$.
3. $x \vee y = d_1 d_2 \cdots d_n$, where d_k=max$\{a_k, b_k\}$.

4. x has a complement $x' = z_1 z_2 \cdots z_n$, where $z_k = 1$ if $x_k = 0$, and $z_k = 0$ if $x_k = 1$.

The truth of these statements can be seen by noting that $(B_n, \leq)$ is isomorphic with $(P(S), \subseteq)$, so each x and y in B_n correspond to subsets A and B of S. Then $x \leq y, x \wedge y, x \vee y,$ and x' correspond to $A \subseteq B$, $A \cap B$, $A \cup B$, and $\overline{A}$ (set complement), respectively (verify) Figure6.61 shows the Hasse diagrams of the lattices B_n for $n = 0, 1, 2, 3$.

Each lattice $(P(S), \subseteq)$ is isomorphic with B_n, where $n = |S|$.

A finite lattice is called a **Boolean algebra** if it is isomorphic with B_n for some nonnegative integer n.

Each B_n is a Boolean algebra and so is each lattice $(P(S), \subseteq)$, where S is a finite set.

EXAMPLE 4

Consider the lattices D_{20} and D_{30} of all positive integer divisors of 20 and 30, respectively, under the partial order of divisibility. Since D_{20} has six elements and $6 \neq 2^n$ for any integer $n \geq 0$, we conclude that D_{20} is **not** a Boolean algebra. The poset D_{30} has eight elements, and since $8 = 2^3$, it could be a Boolean algebra. In fact, we see that the one-to-one correspondence $f: D_{30} \to B_3$ defined by

$$f(1)=000,\ f(2)=100,\ f(3)=010$$
$$f(5)=001,\ f(6)=110,\ f(10)=101$$
$$f(15)=011,\ f(30)=111$$

is an isomorphism. Thus D_{30} is a Boolean algebra.

If a finite lattice L does not contain 2^n element for some nonnegative integer n, we know that L cannot be a Boolean algebra. If $|L|=2^n$, then L may or may not be a Boolean algebra.

The following theorem gives a partial answer.

Theorem 2 Let

$$n = p_1 p_2 \cdots p_k$$

where the p_i are distinct primes. Then D_n is a Boolean algebra.

Proof: Let $S = \{p_1, p_2, \cdots, p_k\}$. If $T \subseteq S$ and a_T is the product of the primes in T. Then $a_T \mid n$. Any divisor of n must be of the form a_T for some subset T of S (where we let $a_\varnothing = 1$). We may verify that if V and T are subsets of S, $V \subseteq T$ if and only if $a_V \mid a_T$. Also, it follows from the proof of Theorem 6 of Section 1.4 that

$a_{V\cap T} = a_V \wedge a_T$ =GCD(a_V, a_T) and $a_{V\cup T} = a_V \vee a_T$ =LCM(a_V, a_T). Thus the function $f: P(S) \to D_n$ given by $f(T) = (a_T)$ is an isomorphism from $P(S)$ to D_n. Since $P(S)$ is a Boolean algebra, so is D_n.

Theorem 3 (Substitution Rule for Boolean Algebras) Any formula involving $\cup$ or $\cap$ that holds for arbitrary subsets of a set S will continue to hold for arbitrary elements of Boolean algebra L if $\wedge$ is substituted for $\cap$ and $\vee$ for $\cup$.

EXAMPLE 6

If L is any Boolean algebra and x , y , and z are in L , then the following three properties hold.

1. $(x')'=x$ **Involution Property**（乘方性）
2. $(x\wedge y)'=x'\vee y'$
3. $(x\vee y)'=x'\wedge y'$

De Morgan's Laws

In a similar way, we can list other properties that must hold in any Boolean algebra by the substitution rule. Next we summarize all the basic properties of a Boolean algebra $(L,\leq)$, and next to each one, we list the corresponding property for subsets of a set S. We suppose that x, y, and z are arbitrary elements in L, and A, B, and C are arbitrary subsets of S. Also, we denote the greatest and least elements of L by I and 0, respectively.

1. $x \leq y$ if and only if $x \vee y = y$.
2. $x \leq y$ if and only if $x \wedge y = x$.
3. (a) $x \vee x = x$. (b) $x \wedge x = x$.
4. (a) $x \vee y = y \vee x$. (b) $x \wedge y = y \wedge x$.
5. (a) $x \vee (y \vee z) = (x \vee y) \vee z$.
   (b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

6. (a) $x \vee (x \wedge y) = x.$ (b) $x \wedge (x \vee y) = x.$

7. (a) $0 \leq x \leq I$ for all x in L .

8. (a) $x \vee 0 = x.$ (b) $x \wedge 0 = 0.$

9. (a) $x \vee I = I.$ (b) $x \wedge I = x.$

10.(a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$

(b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$

11. Every element x has a unique complement x' satisfying

(a) $x \vee x' = I.$ (b) $x \wedge x' = 0.$

12. (a) $0' = I.$ (b) $I' = 0.$

13. $(x')' = x$

14. (a) $(x \wedge y)' = x' \vee y'$.

(b) $(x \vee y)' = x' \wedge y'$.

1'. $A \subseteq B$ if and only if $A \cup B = B$.

2'. $A \subseteq B$ if and only if $A \cap B = A$.

3'. (a) $A \cup A = A$.

(b) $A \cap A = A$.

4'. (a) $A \cup B = B \cup A$.

(b) $A \cap B = B \cap A$.

5'. (a) $A \cup (B \cup C) = (A \cup B) \cup C$.

(b) $A \cap (B \cap C) = (A \cup B) \cup C$.

6'. (a) $A \cup (A \cap B) = A$.

(b) $A \cap (A \cup B) = A$.

7'. $\varnothing \subseteq A \subseteq S$ for all A in $P(S)$.

8'. (a) $A \cup \varnothing = A$.

(b) $A \cap \varnothing = \varnothing$.

9'. (a) $A \cup S = S$.

(b) $A \cap S = A$.

10'. (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

11'. Every element A has a unique complement $\overline{A}$ satisfying

(a) $A \cup \overline{A} = S$.

(b) $A \cap \overline{A} = \varnothing$.

12'.(a) $\overline{\varnothing} = S$.

(b) $\overline{S} = \varnothing$.

13'. $\overline{(\overline{A})} = A$

14'. (a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

(b) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

EXAMPLE 8 Show that if n is a positive integer and $p^2 \mid n$, where p is a prime number, then D_n is not a Boolean algebra.

Solution Suppose that $p^2 \mid n$,then we have $n = p^2 q$ and p is an element of D_n .

If D_n is a Boolean algebra, then p must have a complement p' such that GCD(p,p')=1 and LCM(p,p')=n. By Theorem 6 of Section 1.4, we have pp'=n, which leads p'=n/p=pq, then GCD(p,pq)=1, but this is impossible. Hence, D_n can not be a Boolean algebra.

If we combine Example 8 and Theorem 2, we see that D_n is a Boolean algebra if and only if n is the product of distinct primes， i.e., if and only if no prime divides n more than once.

6.5 FUNCTIONS ON BOOLEAN ALGEBRAS

Suppose that the x_k represent proposition, and $f(x_1, x_2, \cdots x_n)$ represents a compound sentence constructed from the x_k's. If we think of the value 0 for a sentence as meaning that the sentence is false, and 1 as meaning that the sentence is true, then tables such as Figure 6.71(a) show us how truth or falsity of $f(x_1, x_2, \cdots x_n)$ depends on the truth or falsity of its component sentences x_k. Thus such tables are called **truth tables**.

Boolean Polynomials

Let $x_1, x_2, \cdots x_n$ be a set of n symbols. A **Boolean polynomial** $p(x_1, x_2, \cdots x_n)$ in the variables x_k, is defined recursively as follows:

1. $x_1, x_2, \cdots x_n$ are all Boolean polynomials.
2. The symbols 0 and 1 are Boolean polynomials.
3. If $p(x_1, x_2, \cdots x_n)$ and $q(x_1, x_2, \cdots x_n)$ are two Boolean polynomials, then so are

$$p(x_1, x_2, \cdots x_n) \vee q(x_1, x_2, \cdots, x_n)$$

and

$$p(x_1, x_2, \cdots x_n) \wedge q(x_1, x_2, \cdots, x_n).$$

4. If $p(x_1, x_2, \cdots x_n)$ is a Boolean polynomial, then so is

$$(p(x_1, x_2, \cdots x_n))'.$$

By tradition, (0)’ is denoted 0’, (1)’ is denoted 1’, and $(x_k)'$ is denoted $x_k\,'$.

5. There are no Boolean polynomials in the variables x_k other than those that can be obtained by repeated use of rules 1, 2, 3, and 4.

Boolean polynomials are also called **Boolean expressions**.

Boolean polynomials can also be written in a graphical or schematic way. If x and y are variables, then the basic polynomials $x \vee y$, $x \wedge y$, and x' are shown schematically in Figure 6.73. The symbol for $x \vee y$ is called an “**or gate**”, that for $x \wedge y$ is called an “**and gate**”**,** and the symbol for x' is called an “**inverter**”（转换器）.

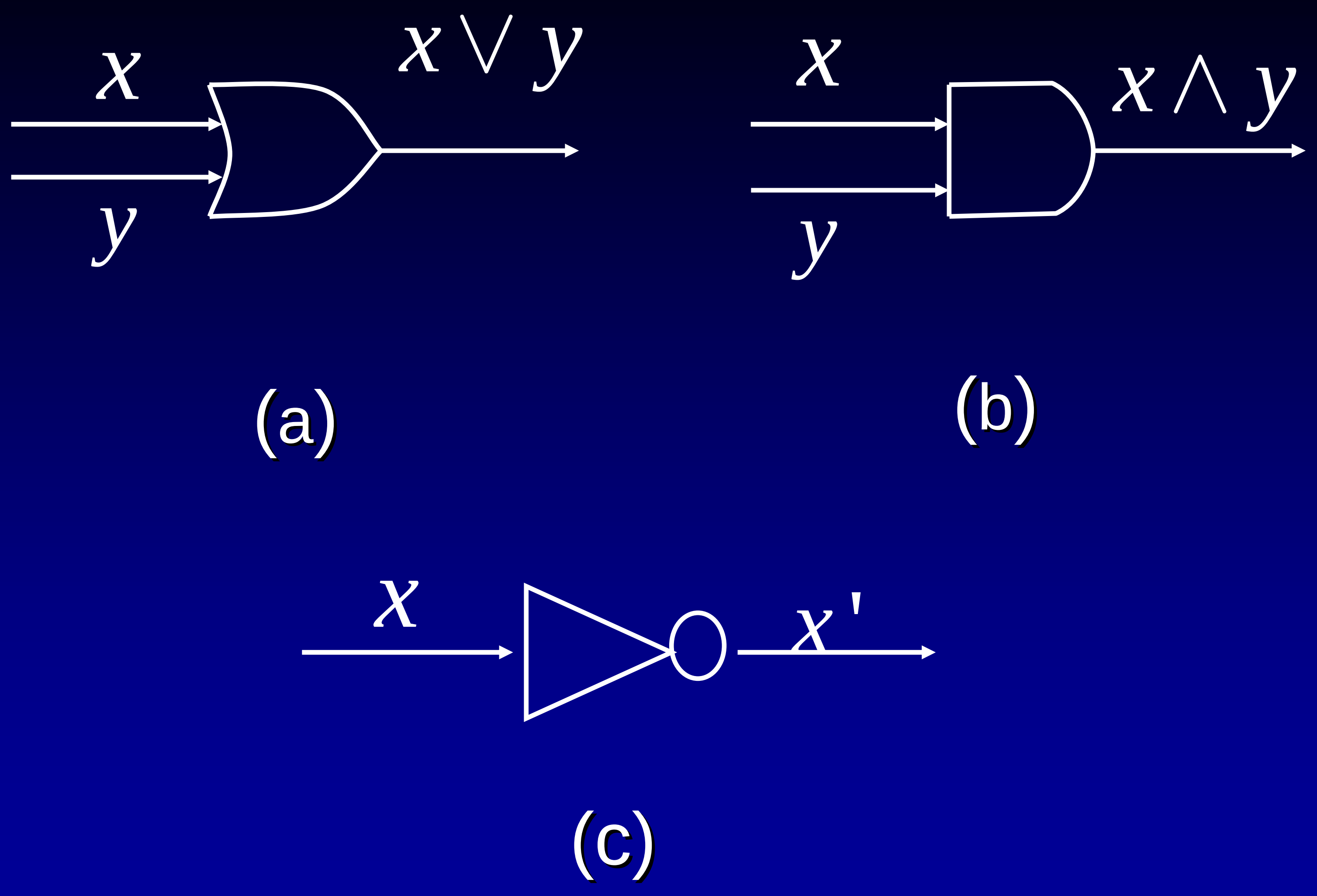


Figure 6.73

The end