Chapter 11
Lattice and Universal Algebra

Lattice and universal algebra are closely related. We refer to [2] for a general introduction. They are used in logic as well as some other disciplines, such as graph theory, abstract algebra, set theory, and topology etc. We refer to [1, 3] for their applications to logic, fuzzy logic, and reasoning.

11.1 Lattice

To begin with, we introduce two equivalent definitions of lattice. They are convenient in certain different situations.

Definition 11.1. A nonempty set L together with two binary operations: joint($\vee$) and meet ($\wedge$) on L is called a lattice, if it satisfies the following identities:

1. (Commutative Laws)

$$x \vee y = y \vee x; \tag{11.1}$$
$$x \wedge y = y \wedge y. \tag{11.2}$$

2. (Associative Laws)

$$x \vee (y \vee z) = (x \vee y) \vee z; \tag{11.3}$$
$$x \wedge (y \wedge z) = (x \wedge y) \wedge z. \tag{11.4}$$

3. (Idempotent Laws)

$$x \vee x = x; \tag{11.5}$$
$$x \wedge x = x. \tag{11.6}$$

4. (Absorption Laws)

$$x = x \vee (x \wedge y); \tag{11.7}$$

$$x = x \wedge (x \vee y). \tag{11.8}$$

Example 11.1. 1. (Boolean Algebra) Consider $\mathscr{D}$ with the disjunction ($\vee$) as the joint, and the conjunction ($\wedge$) as the meet.

2. (Natural Number) Consider the set of natural numbers $\mathbb{N}$. Let the joint and meet be defined as

$$\vee(a,b) = \text{lcm}(a,b);$$
$$\wedge(a,b) = \text{gcd}(a,b).$$

We leave the verification of the above lattices to the reader.

To introduce the second definition of a lattice, we need the concept of partial order.

Definition 11.2. A binary relation $\leq$ defined on a set A is a partial order on the set A if the following conditions hold identically in A:

(i) (reflexivity)
$a \leq a$;
(ii) (antisymmetry)
$a \leq b$ and $b \leq a$ imply $a = b$;
(iii) (transitivity)
$a \leq b$ and $b \leq c$ imply $a \leq c$.

If, in addition, for every a, b in A

(iv) $a \leq b$ or $b \leq a$,

then we say $\leq$ is a total order on A.

Definition 11.3. • A nonempty set with a partial order on it is called a partially ordered set, briefly, poset.

- A nonempty set with a total order on it is called a totally ordered set, or linearly ordered set, or a chain.
- In a partial ordered set, if $a \leq b$ but $a \neq b$, then it is said that $a < b$.

Example 11.2. 1. Let $\text{Su}(A)$ denote the power set of A, and $\leq$ be $\subseteq$. Then $(\text{Su}(A), \leq)$ is a partial ordered set. Note that power set of A is the set of all subsets of A.

2. Let $\mathbb{N}$ be the set of natural numbers, and let $\leq$ be the relation "divides". Then $(\mathbb{N}, \leq)$ is a partial ordered set. Note that if $\leq$ has the conventional meaning as $2 \leq 3$, then $(\mathbb{N}, \leq)$ is a totally ordered set.

Definition 11.4. Let A be a subset of a poset P.

1. $p \in P$ is an upper bound (a lower bound) of A, if $a \leq p$ ($p \leq a$) for all $a \in A$.
2. $p \in P$ is the least upper bound of A, or supremum of A (denoted by $p = \sup A$), if p is an upper bound of A, and for any other upper bound of A, say, b, we have $p \leq b$.

3. $p \in P$ is the greatest lower bound of A, or infimum of A denoted by $p = \inf A$, if p is a lower bound of A, and and for any other lower bound of A, say, b, we have $p \geq b$.
4. For $a, b \in P$, we say b covers a, or a is covered by b (denoted by $a \prec b$), if $a < b$, and whenever $a \leq c \leq b$ it follows that $a = c$ or $c = b$.
5. An interval is defined as: $[a,b] = \{c \in P \mid a \leq c \leq b\}$.
6. An open interval is defined as: $(a,b) = \{c \in P | a < c < b\}$.

Definition 11.5. A finite poset P can be described by a directed graph $(\mathscr{N}, \mathscr{E})$, where $\mathscr{N}$ is the set of nodes and $\mathscr{E}$ is the set of edges. The graph is constructed as following:

(i) $\mathscr{N} = P$;
(ii) $\mathscr{E} \subset P \times P$, and $(a,b) \in \mathscr{E}$ (i.e., there is an edge from a to b), iff $b < a$.

Such a graph is called the Hasse diagram of poset P.

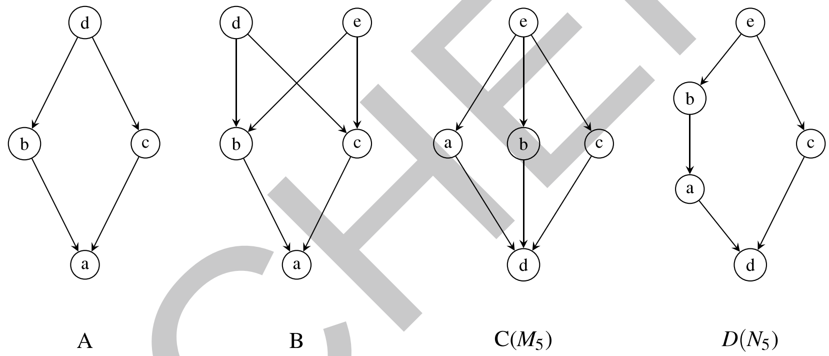

Fig. 11.1 Examples of Hasse diagrams

Fig 11.1 describes Hasse diagrams of four posets A, B, M_5 and N_5.
Now we are ready to introduce the second definition of a lattice

Definition 11.6. A poset L is a lattice iff for any two elements $a, b \in L$ both $\sup\{a,b\}$ and $\inf\{a,b\}$ exist.

Consider Fig 11.1, we can see A, C, D are lattices, but B is not, because in B the $\sup\{b,c\}$ does not exist.

Definition 11.1 and Definition 11.6 are equivalent in the following sense: if L is a lattice by one of the two definitions then we can construct in a simple and uniform fashion on the same set L a lattice by the other definition. We state it as a theorem.

Theorem 11.1. *(i) If L is a lattice by Definition 11.1, define $\leq$ on L as follows: $a \leq b$ iff $a = a \wedge b$, then L satisfies the conditions in Definition 11.6.*

(ii) If L is a lattice by Definition 11.6, define the operations $\vee$ and $\wedge$ by $a \vee b = \sup\{a,b\}$, and $a \wedge b = \inf\{a,b\}$, then L satisfies the conditions in Definition 11.1.

Proof. (i) We need to show that $\leq$ is partial order and $\sup\{a,b\}$, $\inf\{a,b\}$ exist.

- (reflexivity) $a \wedge a = a$ implies $a \leq a$.
- (antisymmetry) Assume $a \leq b$ and $b \leq a$. Then we have $a = a \wedge b$, and $b = a \wedge b$, thus $a = b$.
- (transitivity) Assume $a \leq b$ and $b \leq c$. Then we have $a = a \wedge b$ and $b = b \wedge c$. By associativity,

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

  Hence, $a \leq c$.

We conclude that $\leq$ is partial order.
Next, we prove $\sup\{a,b\}$ and $\inf\{a,b\}$ exist.
Using absorption laws, we have $a = a \wedge (a \vee b)$. So $a \leq a \vee b$. Similarly, $b \leq a \vee b$. Hence, $a \vee b$ is an upper bound of $\{a,b\}$.
For arbitrary upper bound u of $\{a,b\}$, since $a \leq u$, $b \leq u$, we have $a \vee u = (a \wedge u) \vee u = u$ (by L4(a)), similarly $b \vee u = u$. Then $a \vee b \vee u = a \vee u = u$. Using absorption laws again, we have $(a \vee b) \wedge u = (a \vee b) \wedge [(a \vee b) \vee u] = a \vee b$, then $a \vee b \leq u$. Thus $\sup\{a,b\} = a \vee b$.
A similar argument shows that $\inf\{a,b\} = a \wedge b$.

(ii) A straightforward computation shows that the defined $\vee$ and $\wedge$ satisfy equations (11.1)-(11.8).

□

11.2 Isomorphic Lattices and Sublattices

Definition 11.7. Two lattices L_1 and L_2 are isomorphic if there is a bijective α from L_1 to L_2 such that for every $a, b \in L_1$ the following two equations hold:

(i) $\alpha(a \vee b) = \alpha(a) \vee \alpha(b)$;
(ii)$\alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$.

Such an α is called an isomorphism.

One would naturally like to reformulate the definition of isomorphism in terms of the corresponding order relations.

Definition 11.8. If P_1 and P_2 are two posets and α is a map from P_1 to P_2, then we say α is **order-preserving** if $\alpha(a) \leq \alpha(b)$ holds in P_2 whenever $a \leq b$ holds in P_1.

But a bijection α which is order-preserving may not be isomorphism, see Fig 11.2 for example.

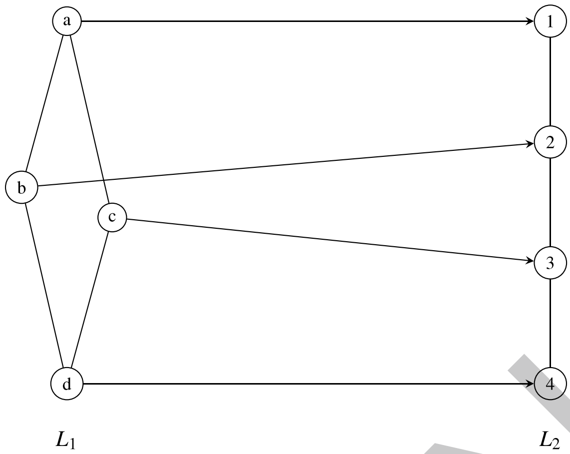

Fig. 11.2 An order-preserving bijection

Theorem 11.2. *Two lattices L_1 and L_2 are isomorphic iff there is a bijection α from L_1 to L_2 such that both α and α^{-1} are order-preserving.*

Proof. (Necessity) For $a \leq b$ in L_1, since α is isomorphism, $\alpha(a) = \alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$. Thus $\alpha(a) \leq \alpha(b)$, α is order-preserving. As α^{-1} is also an isomorphism, it is also order-preserving.

(Sufficiency) Let α be a bijection from L_1 to L_2 such that both α and α^{-1} are order-preserving. We want to prove $\alpha(a \vee b) = \alpha(a) \vee \alpha(b)$, that is to say $\alpha(a \vee b)$ is the supremum of $\{\alpha(a), \alpha(b)\}$.

Since $a \leq a \vee b$ in L_1, we have $\alpha(a) \leq \alpha(a \vee b)$. Similarly, $\alpha(b) \leq \alpha(a \vee b)$. Thus $\alpha(a \vee b)$ is an upper bound of $\{\alpha(a), \alpha(b)\}$.

Next, for arbitrary $u \in L_2$ such that $\alpha(a) \leq u$, $\alpha(b) \leq u$. Since α^{-1} is order-preserving, $a \leq \alpha^{-1}(u)$. Similarly, $b \leq \alpha^{-1}(u)$. Thus $a \vee b \leq \alpha^{-1}(u)$, then $\alpha(a \vee b) \leq u$. This implies that $\alpha(a \vee b) = \alpha(a) \vee \alpha(b)$. Similarly, it can be argued that $\alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$. □

Definition 11.9. If L is a lattice and $H \neq \emptyset$ is a subset of L such that for every pair of elements $a, b \in H$ both $a \vee b$ and $a \wedge b$ are in H, then we say that H with the same operations (restricted to H) is a sublattice of L.

Definition 11.10. A lattice L_1 can be embedded into a lattice L_2 if there is a sublattice of L_2 isomorphic to L_1; in this case we also say L_2 contains a copy of L_1 as a sublattice.

11.3 Matrix Expression of Finite Lattice

Assume $L = \{v_1, \cdots, v_n\}$ is a finite set and there exists an r-ary operators $\pi : \underbrace{L \times \cdots \times L}_{r} \to L$. To use matrix approach we simply identify

$$v_i \sim \delta_n^i, \quad i = 1, \cdots, n. \tag{11.9}$$

$\delta_n^i \in \Delta_n$ is called the vector form of v_i. Denote

$$\pi(v_{i_1}, \cdots, v_{i_k}) = v_{\mu(i_1, \cdots, i_k)}, \quad 1 \le i_1, \cdots, i_k \le k.$$

Then we can construct a matrix, called the structure matrix of π as

$$M_\pi = \delta_n \left[\mu(1,1,\cdots,1) \; \mu(1,1,\cdots,2) \; \cdots \; \mu(1,1,\cdots,n) \cdots \; \mu(n,n,\cdots,n) \right]. \tag{11.10}$$

It is easy to check that in vector form we have

$$\pi(x_1, \cdots, x_k) = M_\pi \ltimes_{i=1}^k x_i, \quad x_i \in \Delta_n. \tag{11.11}$$

Example 11.3. Consider Galois field $\mathbb{Z}_5$. We identify

$$i \sim \delta_5^{i+1}, \quad i = 0, 1, 2, 3, 4.$$

Then for addition $+$ (mod 5), the structure matrix is

$$M_a = \delta_5[1\ 2\ 3\ 4\ 5\ 2\ 3\ 4\ 5\ 1\ 3\ 4\ 5\ 1\ 2\ 4\ 5\ 1\ 2\ 3\ 5\ 1\ 2\ 3\ 4].$$

For product $\times$ (mod 5), the structure matrix is

$$M_p = \delta_5[1\ 1\ 1\ 1\ 1\ 1\ 2\ 3\ 4\ 5\ 1\ 3\ 5\ 2\ 4\ 1\ 4\ 2\ 5\ 3\ 1\ 5\ 4\ 3\ 2].$$

Now assume $L = \{v_1, \cdots, v_n\}$ is given and there are two binary operators $\vee$ and $\wedge$. Assume the structure matrices of these two operators are M_d and M_c respectively. Then we have the following result.

Theorem 11.3. *Let L be described as above.* $(L, \vee, \wedge)$ *is a lattice, iff*

1. (Commutative Laws)

$$M_d(I - W_{[n]}) = 0; \tag{11.12}$$
$$M_c(I - W_{[n]}) = 0. \tag{11.13}$$

2. (Associative Laws)

$$M_d(I_n \otimes M_d) = M_d^2; \tag{11.14}$$
$$M_c(I_n \otimes M_c) = M_c^2. \tag{11.15}$$

3. (Idempotent Laws)

$$M_d M_r^n = I; \qquad (11.16)$$
$$M_c M_r^n = I. \qquad (11.17)$$

Note that where $M_{r,n}$ is the order reducing matrix.

4. (Absorption Laws)

$$\mathrm{Blk}_i\left(M_d(I_n \otimes M_c)M_r^n W_{[n]}\right) = I_n; \quad i = 1, \cdots, n; \qquad (11.18)$$
$$\mathrm{Blk}_i\left(M_c(I_n \otimes M_d)M_r^n W_{[n]}\right) = I_n. \quad i = 1, \cdots, n. \qquad (11.19)$$

Proof. (11.12)-(11.19) are one-one corresponding to (11.1)-(11.8). We prove one of them, say, (11.19). Note that in vector form the equation (11.19) can be expressed as

$$\begin{aligned} x &= M_c x M_d x y = M_c(I_n \otimes M_d)x^2 y \\ &= M_c(I_n \otimes M_d)M_r^n x y = M_c(I_n \otimes M_d)M_r^n W_{[n]} y x. \end{aligned}$$

Then we have

$$M_c(I_n \otimes M_d)M_r^n W_{[n]} y = I_n, \quad \forall y \in \Delta_n.$$

Let $y = \delta_n^i$. Then we have

$$\mathrm{Blk}_i\left(M_c(I_n \otimes M_d)M_r^n W_{[n]}\right) = I_n.$$

□

Next, we consider when a Hasse diagram represents a lattice. A Hasse diagram, denoted by $\mathscr{H} = (\mathscr{N}, \mathscr{E})$, can be described by a matrix, denoted by $M_{\mathscr{H}}$ and called its incidence matrix, or Hasse matrix.

Let $|\mathscr{N}| = n$, then $M_{\mathscr{H}} \in \mathscr{B}_{n\times n}$, which is defined by its entries $m_{i,j}$ as follows:

$$m_{i,j} = \begin{cases} 1, & (i,j) \in \mathscr{E} \\ 0, & \text{otherwise.} \end{cases}$$

We consider the incidence matrices of the diagrams in Fig. 11.1.

Example 11.4. Consider the figures A, B, C, and D in Fig. 11.1. We construct the incidence matrix of A first. Consider the first column, which indicates a. Now since both $b > a$ we have $m_{2,1} = 1$. Similarly, since $c > a$, we have $m_{3,1} = 1$. For column 2, which indicates b. Since only $d > b$, we have $m_{4,2} = 1$. Continuing this procedure column by column, the incidence matrix of A is constructed as

$$\mathscr{J}_A = \begin{array}{c} \begin{matrix} \mathrm{a} & \mathrm{b} & \mathrm{c} & \mathrm{d} \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array} \begin{matrix} a \\ b \\ c \\ d \end{matrix}$$

Similarly, the incidence matrices of B, C, and D can be constructed as

$$\mathscr{J}_B = \begin{bmatrix} 0&0&0&0&0\\ 1&0&0&0&0\\ 1&0&0&0&0\\ 0&1&1&0&0\\ 0&1&1&0&0 \end{bmatrix}.$$

$$\mathscr{J}_C = \begin{bmatrix} 0&0&0&1&0\\ 0&0&0&1&0\\ 0&0&0&1&0\\ 0&0&0&0&0\\ 1&1&1&0&0 \end{bmatrix}.$$

$$\mathscr{J}_D = \begin{bmatrix} 0&0&0&1&0\\ 1&0&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&0\\ 0&1&1&0&0 \end{bmatrix}.$$

Next, we consider when a Boolean matrix is a Hasse matrix. We have the following result.

Proposition 11.1. *A Boolean matrix $H \in \mathscr{B}_{n\times n}$ is a Hasse matrix, iff*

$$h_{i,j}h_{j,i} = 0, \quad i,j = 1,\cdots,n. \tag{11.20}$$

Proof. Denote the corresponding nodes as $N_1, \cdots, N_n$.

(Necessity) If H is a Hasse matrix, then it is clear that (i) $h_{i,i} = 0$, $i = 1,\cdots,n$; (ii) if $h_{i,j} = 1$, then $N_j < N_i$, and hence $h_{j,i} = 0$. Hence, (11.20) is true.

(Sufficiency) If $h_{i,j} = 1$ draw a directed edge from i to j. Since there is no a pair of points, which have more than one edges, the graph is a Hasse one. □

Finally, we consider when a Hasse matrix is a lattice. Precisely, the Hasse graph corresponding to this Hasse matrix is a lattice.

Let $\mathscr{J}$ be a Hasse matrix. Then we define a matrix

$$U_{\mathscr{J}} := \sum_{k=0}^{n-1} \mathscr{J}^{(k)}. \tag{11.21}$$

Note that here we use Boolean power.

Lemma 11.1. $N_i \geq N_j$, *iff* $u_{i,j} = 1$.

Proof. Denote by $U_s = \mathscr{J}^{(s)}$. then it is easy to see that $u^s_{i,j} = 1$ means on the graph there is a path, starting from N_i, reaches N_j at s steps. That is, there is a path from N_i to N_j with length s. It follows that $N_i \geq N_j$. The lemma follows immediately. □

Definition 11.11. 1. Let $X = (x_1,\cdots,x_n) \in \mathscr{B}_{1\times n}$ (X could be a row or a column.) The support of X, denoted by supp(X) is an index set $\{i_1,\cdots,i_k\} \subset \{1,2,\cdots,n\}$, such that $i_j \in supp(X)$, iff $x_{i_j} = 1$.
2. Let $W \in M_{n\times n}$ and $I = \{i_1,\cdots,i_k\} \subset \{1,2,\cdots,n\}$ be a subindex. then the submatrix W_I of W is defined as

$$W_I = \begin{bmatrix} w_{i_1,i_1} & w_{i_1,i_2} & \cdots & w_{i_1,i_k} \\ w_{i_2,i_1} & w_{i_2,i_2} & \cdots & w_{i_2,i_k} \\ \vdots & & & \\ w_{i_k,i_1} & w_{i_k,i_2} & \cdots & w_{i_k,i_k} \end{bmatrix}.$$

Now we are ready to present the condition for a Hasse matrix to be a lattice.

Let $\mathscr{J} \in \mathscr{B}_{n\times n}$ be a Hasse matrix and $U_{\mathscr{J}}$ be defined by (11.22). For any $1 \le i < j \le n$ we define two index sets:

$$\begin{aligned} C^{i,j} &:= \text{supp}\left(\text{Col}_i(U_{\mathscr{J}}) \wedge \text{Col}_j(U_{\mathscr{J}})\right); \\ R^{i,j} &:= \text{supp}\left(\text{Row}_i(U_{\mathscr{J}}) \wedge \text{Row}_j(U_{\mathscr{J}})\right). \end{aligned}$$

Using them, we construct two sub-matrices correspondingly as

$$M_{C^{i,j}}; \quad M_{R^{i,j}}.$$

Then we have the following:

Theorem 11.4. *$\mathscr{J}$ is a lattice, iff for each pair (i,j) ($i \neq j$), we have*

(i) $|C^{i,j}| := \alpha \ge 1$, $|R^{i,j}| := \beta \ge 1$;
(ii) $M_{C^{i,j}}$ *has a row, which equals* $\mathbf{1}_\alpha^T$;
(iii) $M_{R^{i,j}}$ *has a column, which equals* $\mathbf{1}_\beta$.

Proof. Consider its corresponding graph, where i corresponds a node N_i, $i = 1,\cdots,n$. We have to show that any two nodes N_i and N_j have the sup$\{N_i,N_j\}$ and inf$\{N_i,N_j\}$. We first consider the existence of sup$\{N_i,N_j\}$.

From the construction it is clear that $s \in C^{i,j}$ implies that N_s is a common upper bound of N_i and N_j. If $|C^{i,j}| = \alpha^{i,j} = 0$, it is obvious that N_i and N_j have no common upper bound. Now assume $\alpha^{i,j} > 0$ and $C^{i,j} = \{u_1,\cdots,u_{\alpha^{i,j}}\}$. Then we can construct the matrix $M_{C^{i,j}}$, which corresponds to the set of common upper bounds of N_i and N_j. Now if a column equals $\mathbf{1}_{\alpha^{i,j}}$ then it corresponds the least common upper bound, we denote its index by $u_{i,j}$. Note that if such column exists, it is unique. If there is no such a column, which equals to $\mathbf{1}_{\alpha^{i,j}}$, then it is clear that the least common upper bound does not exist.

A similar argument shows that $\inf N_i,N_j$ exists, iff there exists a unique row of index $\ell_{i,j}$ in $M_{R^{i,j}}$, which equals $\mathbf{1}^T_{\beta^{i,j}}$. □

From the constructive proof of Theorem 11.4 one sees easily that if matrix H is a lattice, then its structure matrices corresponding to $\vee$ and $\wedge$ are as follows.

$$\begin{aligned} M_d &= \delta_n[u_{11} \ \cdots \ u_{1n} \ \cdots \ u_{nn}]; \\ M_c &= \delta_n[\ell_{11} \ \cdots \ \ell_{1n} \ \cdots \ \ell_{nn}]; \end{aligned} \tag{11.22}$$

We give some examples to illustrate it.

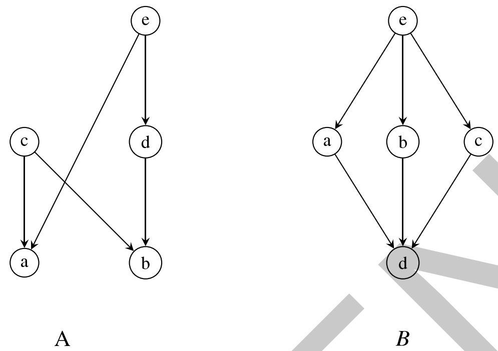

Fig. 11.3 ?

Example 11.5. 1. Consider graph A in Fig. 11.3. The incidence matrix is

$$\mathscr{I}_A = \begin{bmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 1&1&0&0&0 \\ 0&1&0&0&0 \\ 1&0&0&1&0 \end{bmatrix}.$$

By direct computation we have

$$U_{\mathscr{I}_A} = \begin{bmatrix} 1&0&0&0&0 \\ 0&1&0&0&0 \\ 1&1&1&0&0 \\ 0&1&0&1&0 \\ 1&1&0&1&1 \end{bmatrix}.$$

Then c and e are upper bound of $\{a,b\}$. Since

$$U_{3,5} = \begin{bmatrix} 1&0 \\ 0&1 \end{bmatrix},$$

there is no smallest elements of $\{c,e\}$, which means $\{a,b\}$ has no sup. A is not a lattice.

2. Consider the graph B in Fig. 11.3. We have

$$\mathscr{J}_B = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

We can calculate that

$$U_{\mathscr{J}_B} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Thus e is the largest element and d is the smallest. It is easy to see that

$$\begin{array}{l} a \vee b = e \;\; a \vee c = e \;\; a \vee d = a \;\; a \vee e = e \;\; b \vee c = e \\ b \vee d = b \;\; b \vee e = e \;\; c \vee d = c \;\; c \vee e = e \;\; d \vee e = e. \end{array}$$

Thus

$$M_d = \delta_5[1\,5\,5\,1\,5\,5\,2\,5\,2\,5\,5\,5\,3\,3\,5\,1\,2\,3\,4\,5\,5\,5\,5\,5\,5].$$

Similarly, we can get

$$M_c = \delta_5[1\,4\,4\,4\,1\,4\,2\,4\,4\,2\,4\,4\,3\,4\,3\,4\,4\,4\,4\,4\,1\,2\,3\,4\,5]$$

11.4 Distributive and Modular Lattices

Definition 11.12. A distributive lattice is a lattice which satisfies either of the distributive laws:

(i)

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z); \tag{11.23}$$

(ii)

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z). \tag{11.24}$$

This definition is well posed, because we have the following equivalence.

Theorem 11.5. *A lattice satisfies (11.23) if and only if it satisfies (11.24).*

Proof. We prove (11.24) $\Rightarrow$ (11.23), and leave the proof of (11.23) $\Rightarrow$ (11.24) to the reader.

Assume (11.24) holds. Then

$$\begin{aligned} x\wedge(y\vee z) &= (x\wedge(x\vee z))\wedge(y\vee z) && (by\ (11.8)) \\ &= x\wedge((x\vee z)\wedge(y\vee z)) && (by\ (11.4)) \\ &= x\wedge(z\vee(x\wedge y)) && (by\ (11.24)) \\ &= (x\vee(x\wedge y))\wedge(z\vee(x\wedge y)) && (by\ (11.7)) \\ &= (x\wedge y)\vee(x\wedge z). && (by\ (11.24)) \end{aligned}$$

□

Remark 11.1. 1. Every lattice satisfies the following two inequalities:

$$(x\wedge y)\vee(x\wedge z)\le x\wedge(y\vee z); \tag{11.25}$$
$$x\vee(y\wedge z)\le(x\vee y)\wedge(x\vee z). \tag{11.26}$$

We leave the proof to the reader.
2. For finite lattices, (11.23) and (11.24) have the following equivalent forms (11.27) and (11.28) respectively.

$$M_c(I_n\otimes M_d)=M_dM_c(I_{n^2}\otimes M_c)(I_n\otimes W_{[n]})M_r^n; \tag{11.27}$$
$$M_d(I_n\otimes M_c)=M_cM_d(I_{n^2}\otimes M_c)(I_n\otimes W_{[n]})M_r^n. \tag{11.28}$$

Definition 11.13. A modular lattice is any lattice which satisfies the following modular law:

$$x\le y \text{ implies } x\vee(y\wedge z)=y\wedge(x\vee z). \tag{11.29}$$

Remark 11.2. It is easy to see that every lattice satisfies

$$x\le y \text{ implies } x\vee(y\wedge z)\le y\wedge(x\vee z).$$

Proposition 11.2. *Every distributive lattice is a modular lattice.*

Proof. Using (11.24) and noticing that $x\vee y=y$ whenever $x\le y$, the conclusion follows. □

Example 11.6. Recall Fig 11.1, we can check that

1. In C (which will be called M_5 in the sequel), $a\vee(b\wedge c)=a\vee d=a$, but $(a\vee b)\wedge(a\vee c)=e\wedge e=e$. Hence M_5 is not distributive.
2. It is easy to verify that M_5 does satisfy the modular law, and hence is a modular.
3. In D, (which will be called N_5 in the sequel), $a\le b$, $a\vee(b\wedge c)=a\vee d=a$, but $b\wedge(a\vee c)=b\wedge e=b$. Hence N_5 is not modular and therefore, is not distributive.

The following two theorems are important in verifying modular and/or distributive lattice.

Theorem 11.6 (Dedekind [2]). *L is a non-modular lattice iff N_5 can be embedded into L.*

Theorem 11.7 (Birkhoff [2]). *L is a non-distributive lattice iff M5 or N5 can be embedded into L.*

11.5 Algebra

Definition 11.14. A type of algebras is a set $\mathscr{F}$ of function symbols such that a nonnegative integer n is assigned to each member f of $\mathscr{F}$. This integer is called the arity of f, and f is said to be an n-ary function symbol. The subset of n-ary function symbols in $\mathscr{F}$ is denoted by $\mathscr{F}_n$.

Definition 11.15. If $\mathscr{F}$ is a type of algebras then an algebra $\mathbf{A}$ of type $\mathscr{F}$ is an ordered pair $\langle A, F\rangle$ where A is a nonempty set and F is a family of finitary operations on A indexed by the type $\mathscr{F}$ such that corresponding to each n-ary function symbol f in $\mathscr{F}$ there is an n-ary operation $f^{\mathbf{A}}$ on A. The set A is call the underlying set of $\mathbf{A} = \langle A, F\rangle$, and the $f^{\mathbf{A}}s$ are called the fundamental operations of $\mathbf{A}$. In addition,

(i) $\mathbf{A}$ is unary, if all of its operations are unary, and it is mono-unary if it has just one unary operation.
(ii) $\mathbf{A}$ is groupoid, if it has just one binary operation.
(iii) $\mathbf{A}$ is finite if $|A|$ is finite, and trivial if $|A| = 1$.

Example 11.7. 1. A group $\mathbf{G}$ is an algebra $\langle G, \cdot, ^{-1}, 1\rangle$ with a binary, a unary, and a nullary operations in which the following identities are true:

(i)

$$x\cdot(y\cdot z) = (x\cdot y)\cdot z. \tag{11.30}$$

(ii)

$$x\cdot 1 = 1\cdot x = x. \tag{11.31}$$

(iii)

$$x\cdot x^{-1} = x^{-1}\cdot x \approx 1. \tag{11.32}$$

2. A group $\mathbf{G}$ is Abelian (or commutative) if the following identity is true:

(iv)

$$x\cdot y = y\cdot x. \tag{11.33}$$

3. A semigroup is a groupoid $\langle G, \cdot\rangle$ in which (11.30) is true.
4. A ring is an algebra $\langle R, +, \cdot, -, 0\rangle$, where $+$ and $\cdot$ are binary, $-$ is unary and 0 is nullary, satisfying the following conditions:

(i) $\langle R, +, -, 0\rangle$ is an Abelian group
(ii)$\langle R, \cdot\rangle$ is a semigroup
(iii)

$$x\cdot(y+z) = (x\cdot y) + (x\cdot z). \tag{11.34}$$

$$(x+y)\cdot z = (x\cdot z) + (y\cdot z). \tag{11.35}$$

5. A semi-lattice is a semigroup $\langle S, \cdot \rangle$ which satisfies the commutative law (11.33) and the idempotent law

$$x \cdot x = x. \tag{11.36}$$

6. An algebra $\langle L, \vee, \wedge \rangle$ with two binary operations satisfying (11.1)-(11.8) is a lattice.
7. An algebra $\langle L, \vee, \wedge, 0, 1 \rangle$ with two binary and two nullary operations is a bounded lattice, if it satisfies:

   (i) $\langle L, \vee, \wedge \rangle$ is a lattice
   (ii)$x \wedge 0 \approx 0$; $x \vee 1 \approx 1$.

8. A Boolean algebra is an algebra $\langle B, \vee, \wedge, \neg, 0, 1 \rangle$ with two binary, one unary, and two nullary operations which satisfy:

   (i) $\langle B, \vee, \wedge \rangle$ is a distributive lattice
   (ii)

$$x \wedge 0 = 0; \quad x \vee 1 = 1. \tag{11.37}$$

   (iii)

$$x \wedge (\neg x) = 0; \quad x \vee (\neg x) = 1. \tag{11.38}$$

Definition 11.16. Let **A** and **B** be two algebras of the same type $\mathscr{F}$. Then a function $\alpha : A \to B$ is an isomorphism from **A** to **B** if α is one-to-one and onto, and for every n-ary $f \in \mathscr{F}$, for $a_1, \cdots, a_n \in A$, we have

$$\alpha f^{\mathbf{A}}(a_1, \cdots, a_n) = f^{\mathbf{B}}(\alpha a_1, \cdots, \alpha a_n). \tag{11.39}$$

We say **A** is isomorphic to **B**, written $\mathbf{A} \cong B$, if there is an isomorphism from **A** to **B**. If α is an isomorphism from **A** to **B** we may simply say "$\alpha : \mathbf{A} \to \mathbf{B}$ is an isomorphism".

Definition 11.17. Let **A** and **B** be two algebras of the same type. Then **B** is a subalgebra of A if $B \subseteq A$ and every fundamental operation of **B** is the restriction of the corresponding operation of **A**, i.e., for each function symbol f, f^B is f^A restricted to B; we write simply $B \leq A$.

Consider finite algebras. The following result is obvious.

Proposition 11.3. *Let* **A** *and* **B** *be two finite algebras of the same type* $\mathscr{F}$. $\alpha : \mathbf{A} \to \mathbf{B}$ *is an isomorphism, iff for each* $f \in \mathscr{F}$ *the structure matrices of* f^A *and* f^B *(corresponding to* $\{a_1, \cdots, a_n\}$ *and* $\{b_1 = \alpha(a_1), \cdots, b_n = \alpha(a_n)\}$*) are the same.*

Exercise 8

1. Verify that the two objects in Example 11.1 are lattice.
2. For a given lattice prove that (11.23) ⇒ (11.24).
3. For any lattice prove (11.25) and (11.26).
4. Prove that a n-elements lattice is modular, iff

$$\mathrm{Col}_i(M_d M_c) = \mathrm{Col}_i(M_c M_d W_{[n]}), i \in \{(j-1)n+k \,|\, \mathrm{Col}_j(D_{n,n} W_{[n]}) = \mathrm{Col}_j(M_c), 1 \le k \le n\},$$

where $D_{n,n}$ is the dummy matrix defined in (6.27).

References

1. Barnes, D., Mac, J.: An Algebraic Introduction to Mathematical Logic. Springer-Verlag, New York (1975)
2. Burris, S., Sankappanavar, H.: A Course in Universal Algebra. Number 78 in Graduate Texts in Mathematics. Springer-Verlag (1981)
3. Kerre, E., Huang, C., Ruan, D.: Fuzzy Set Theory and Approximate Reasoning. Wuhan University Press (2004)