离散数学习题课

第十三讲——格与布尔代数

Distributive lattices

Definition:

A lattice L is called a <u>distributive</u> if $\forall a, b, c \in L$,

(1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, and

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

Comments:

- Since $(1) \Leftrightarrow (2)$, to show a lattice is distributive, we only need to verify one of them
- Distributive lattices are always modular

Bounded lattices

Definition:

A lattice L is called <u>bounded</u> if both $\bigvee L$ and $\bigwedge L$ exist, where $\bigvee L$ and $\bigwedge L$ are the supremum and the infimum of L, respectively.

Comments:

- $\bigvee L$ is usually called <u>top</u>, denoted as 1
- $\bigwedge L$ is usually called <u>bottom</u>, denoted as 0
- Finite lattices are always bounded

Complemented lattices

Definition:

Let L be a bounded lattice, $a \in L$, b is called a <u>complement</u> of a if $a \vee b = 1$ and $a \wedge b = 0$.

A lattice L is called <u>complemented</u> if every element in L has complements.

Comments:

- Complements may not be unique
- In distributive lattices, the complements are unique

Complete lattices

Definition:

A lattice L is called <u>complete</u> if $\forall S \subseteq L$, both $\bigvee S$ and $\bigwedge S$ exist, where $\bigvee S$ and $\bigwedge S$ are the supremum and the infimum of S, respectively.

Comments:

- Finite lattices are always complete
- Complete lattices are always bounded
- For any set A, $\langle \mathcal{P}(A), \subseteq \rangle$ is a complete lattice

Ideals

Definition:

Let L be a lattice, $\emptyset \neq I \subseteq L$. I is called an <u>ideal</u> of L if

(1) $\forall a, b \in I, a \vee b \in I$, and

(2) $\forall a \in I, \forall x \in L, x \preccurlyeq a \implies x \in I$

Comments:

- An ideal must be a sublattice
- Let $I(L) = \{x \mid x \text{ is an ideal of } L\}$, then $\langle I(L), \subseteq \rangle$ is a lattice
- Let $I_0(L) = I(L) \cup \{\emptyset\}$, $\langle I_0(L), \subseteq \rangle$ is a complete lattice
- $\forall S(\emptyset \neq S \subseteq I_0(L) \to \cap S \in I_0(L))$

Boolean algebras

Definition:

A complemented distributive lattice is called a <u>Boolean algebra</u>, denoted as $\langle B, \wedge, \vee, ', 0, 1\rangle$, where $'$ is the complement operation, and $0, 1$ are the bottom and top elements of B, respectively.

Comments:

If $\langle B, \wedge, \vee, ', 0, 1\rangle$ is a Boolean algebra, then

(1) $\forall a \in B, a'' = a$;

(2) $\forall a, b \in B, (a \wedge b)' = a' \vee b', (a \vee b)' = a' \wedge b'$;

(3) $\forall a, b \in B, a \preccurlyeq b \iff b' \preccurlyeq a'$

Boolean subalgebras

Definition:

Let $\langle B, \wedge, \vee, ', 0, 1\rangle$ be a Boolean algrebra. A nonemtpy subset $\emptyset \neq S \subseteq B$ is called a <u>Boolean subalgebra</u> of B, if

(1) $\forall a, b \in S, a \wedge b \in S$;

(2) $\forall a, b \in S, a \vee b \in S$; and

(3) $\forall a \in S, a' \in S$

Comments:

- Either (1) or (2) in the above conditions can be omitted
- Complemented sublattices of a Boolean algebra are not necessarily its Boolean subalgebras

Homomorphisms

Definition:

Let $\langle B_1, \wedge, \vee, ', 0, 1\rangle, \langle B_2, \cap, \cup, -, \theta, E\rangle$ be two Boolean algrebras. A function $\varphi : B_1 \to B_2$ is called a <u>homomorphism</u> from B_1 to B_2, if

(1) $\forall a, b \in B_1, \varphi(a \wedge b) = \varphi(a) \cap \varphi(b)$;

(2) $\forall a, b \in B_1, \varphi(a \vee b) = \varphi(a) \cup \varphi(b)$;

(3) $\forall a \in B_1, \varphi(a') = -\varphi(a)$.

Comments:

- Either (1) or (2) in the above conditions can be omitted

Some important results

- The intersection of (any number of) subalgebras is also a subalgebra, if the intersection is nonempty
- Let $V_1 = \langle A, \circ_1, \circ_2, \cdots \circ_n \rangle, V_2 = \langle B, \circ_1', \circ_2', \cdots \circ_n' \rangle$, be two algebraic systems. If $\varphi : A \to B$ is a homomorphism from V_1 to V_2, then $\varphi(V_1)$ is a subalgebra of V_2.
- Let $\langle B_1, \wedge, \vee, ', 0, 1 \rangle, \langle B_2, \cap, \cup, -, \theta, E \rangle$ be two Boolean algrebras. If $\varphi : B_1 \to B_2$ is a homomorphism, then
  (1) $\varphi(0) = \theta$;
  (2) $\varphi(1) = E$;

Representation theorem

Notations:

Let L be a lattice, $a, b \in L$, b is said to <u>cover</u> a if

$$a \prec b \text{ and } \forall c \in L(a \prec c \preccurlyeq b \rightarrow b = c).$$

Let L be a lattice, $x \in B$ is called an <u>atom</u> if x covers 0, where 0 is the bottom of L.

The representation theorem for finite Boolean algebras

For any finite Boolean algebra $V = \langle B, \wedge, \vee, ', 0, 1 \rangle$,

$$V \cong \langle \mathcal{P}(A), \cap, \cup, \sim, \emptyset, A \rangle,$$

where $A = \{x \mid x \text{ is an atom of } B\}$.

Duality Principle

The principle of Duality:

Any algebraic equality derived from the axioms of Boolean algebra remains true when the operators $\vee$ and $\wedge$ are interchanged and the identity elements 0 and 1 are interchanged.

Comments:

- The equality <u>should not</u> contain other symbols
- The equality must hold for <u>all</u> Boolean algebras

Problems

1. Let L be a lattice, $\emptyset \neq I \subseteq L$. I is called an <u>ideal</u> of L if

   (1) $\forall a, b \in I, a \vee b \in I$, and

   (2) $\forall a \in I, \forall x \in L, x \preccurlyeq a \implies x \in I$

   Let $I(L) = \{x \mid x \text{ is an ideal of } L\}$, $I_0(L) = I(L) \cup \{\emptyset\}$.

   Show that

   (1) Let $\varphi : L \to I_0(L), \forall a \in L, \varphi(a) = \{x \mid x \in L \text{ and } x \preccurlyeq a\}$,

   then φ is a homomorphism.

   (2) If L is finite, then $L \cong I(L)$.

Problems (cont.)

2. Let G be a group, $L(G)$ denote the set of all subgroups of G, then $\langle L(G), \subseteq \rangle$ is a lattice, called the lattice of subgroups. Prove or disprove:

   (1) $\langle L(G), \subseteq \rangle$ is always bounded

   (2) $\langle L(G), \subseteq \rangle$ is always complemented

   (3) $\langle L(G), \subseteq \rangle$ is always complete

   (4) $\langle L(G), \subseteq \rangle$ is always distributive

Comments

Facts:

(1) $\langle L(G), \subseteq \rangle$ is distributive if and only if $\forall S \subseteq G$,

$|S| < \infty \to \langle S \rangle$ is cyclic.

(2) $\langle L_N(G), \subseteq \rangle$ is modular, where $L_N(G)$ denotes the set of all normal subgroups of G.

(3) H is an atom of $\langle L(G), \subseteq \rangle$ if and only if $|H|$ is prime.

Corollaries:

(1) If G is cyclic, then $\langle L(G), \subseteq \rangle$ is distributive

(2) If G is abelian, then $\langle L(G), \subseteq \rangle$ is modular

Problems (cont.)

3. Let L be a distributive lattice, $a \in L$. $\forall x \in L$, let

$$f(x) = x \vee a, g(x) = x \wedge a.$$

(1) Show that, both f and g are endomorphisms.

(2) Find $f(L)$ and $g(L)$.

4. Let L be a distributive lattice, $a, b \in L$. Let

$$X = \{x \mid x \in L \text{ and } a \wedge b \preccurlyeq x \preccurlyeq a\}$$

$$Y = \{y \mid y \in L \text{ and } b \preccurlyeq y \preccurlyeq a \vee b\}$$

Then, both X and Y are sublattices of L.

Show that, $X \cong Y$.

Problems (cont.)

5. Let $\langle B, \wedge, \vee, ', 0, 1\rangle$ be a Boolean algrebra. $\forall x, y \in B$, let
$$x \oplus y = (x \wedge y') \vee (x' \wedge y)$$
Show that, $\langle B, \oplus\rangle$ is an abelian group.
6. Let $\varphi : B_1 \to B_2$ be a homomorphism between two Boolean algebras. Show that, $\varphi^{-1}(0) = \{x \mid x \in B_1 \text{ and } \varphi(x) = 0\}$ is an ideal of B_1.
7. For any given $n \in \mathbb{N}^+$, let $D_n = \{k \mid k \in \mathbb{N}^+ \text{ and } k \mid n\}$. Find a necessary and sufficient conditions under which $\langle D_n, \gcd, \mathrm{lcm}\rangle$ is a Boolean algebra.

Sylow Theorems

- First Sylow Theorem

Let G be a finite group with $|G| = p^k m$, where p is prime and $p \nmid m$. Then

(1) $\exists H \leq G,\ |H| = p^k$.

(2) $\forall H \leq G, \forall i \in \mathbb{Z}_k,$

$$|H| = p^i \implies \exists H'(H' \leq G \wedge |H'| = p^{i+1} \wedge H \trianglelefteq H')$$

Sylow Theorems (cont.)

Definitions:

A group H is called a <u>p-group</u>, if $|H| = p^k$, where p is prime, $k \in \mathbb{N}$.

A subgroup $H \leq G$ is called a <u>Sylow p-subgroup</u> of G, if

$$|H| = p^k \text{ and } |G| = p^k m, \text{ where } p \nmid m$$

Let $\mathrm{Syl}_p(G) = \{H \mid H \text{ is a Sylow } p\text{-subgroup of } G\}$

Examples: If $|G| = 144 = 2^4 \cdot 3^2$, then

$\mathrm{Syl}_2 = \{H \leq G \mid |H| = 2^4\}$, $\mathrm{Syl}_3 = \{H \leq G \mid |H| = 3^2\}$,

$\mathrm{Syl}_5 = \{H \leq G \mid |H| = 5^0\} = \{\{e\}\}$

Sylow Theorems (cont.)

Let G be a finite group. Then, for any prime p,

- Second Sylow Theorem

(1) If H is a p-subgroup of G, and $K \in \mathrm{Syl}_p(G)$, then $\exists g \in G$,

$$gHg^{-1} \leq K.$$

(2) $\forall H, K \in \mathrm{Syl}_p(G)$, $\exists g \in G$, $gHg^{-1} = K$.

(3) $\left|\mathrm{Syl}_p(G)\right| = [G : N(K)] \mid |G|$, where $K \in \mathrm{Syl}_p(G)$.

- Third Sylow Theorem

(1) $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$.

(2) $\left|\mathrm{Syl}_p(G)\right| \mid m$, where $|G| = p^k m, p \nmid m$.

Thank you

Any questions?