Chapter 12 Boolean Algebras

12.1 Lattices and Algebraic Systems

Let (A, ≤) be a poset. Then

ub(a, b) = {c| a ≤ c, b ≤ c} **upper** *bound*

lub(a, b) = {c| c∈ub(a,b), ∄d .∍. d∈ub(a,b), d≤c,c≠d}

least *upper bound (d < c)*

lb(a, b) = {c| c≤a, c≤b} **lower** *bound*

glb(a, b) = {c| c∈lb(a,b), ∄d .∍. d∈lb(a,b), c≤d,c≠d}

greatest *lower bound (c < d)*

A poset (A, ≤) is called a **lattice***,*

*if ∀a, b ∈ A, ∃***unique** *lub(a, b) and glb(a, b).*

(A, ∨) and (A, ∧) are algebraic systems.

Let (A, ≤) be a **lattice***, an* **algebraic system** *(A, ∨, ∧),*

is defined by the **lattice** *(A, ≤) where*

$\vee: A \times A \rightarrow A$ *least upper bound(***join***)*

$\wedge: A \times A \rightarrow A$ *greatest lower bound(***meet***)*

(P(S), ∪, ∩) is an algebraic system

defined by the lattice (P(S), ⊆).

(N, max, min): *(N, ≤).*

(N^+, lcm, gcd): *(N^+, |). a|b, if a divides b.*

Theorem 12.1*(ub, lb)*

$a \wedge b \leq a, b \qquad a, b \leq a \vee b$

Proof

*$\wedge$(**glb**) is lower bound, and $\vee$(**lub**)is upper bound.*

Theorem 12.2

If $a \leq b$, $c \leq d$,

$a \vee c \leq b \vee d$, *and* $\quad a \wedge c \leq b \wedge d$.

Proof

$b \leq b \vee d, a \leq b \Rightarrow a \leq b \vee d.$ *ub, tran.*

$d \leq b \vee d, c \leq d \Rightarrow c \leq b \vee d.$ *ub, tran.*

$\therefore a \vee c \leq b \vee d.$ *lub ≤ ub*

$a \wedge c \leq a, a \leq b \Rightarrow a \wedge c \leq b.$ *lb, tran.*

$a \wedge c \leq c, c \leq d \Rightarrow a \wedge c \leq d.$ *lb, tran.*

$\therefore a \wedge c \leq b \wedge d.$ *lb ≤ glb*

12.2 Principle of Duality

left vs. right

freedom vs. equality

Capitalism vs. Socialism

Flowers in the mirror

$(A, \leq)$ *vs.* $(A, \geq)$

$(A, \vee, \wedge)$ *vs* $(A, \wedge, \vee)$.

12.3 Basic Properties of Algebraic systems defined by Lattices

Let $(A, \vee, \wedge)$ be a algebraic system defined by the lattice $(A, \leq)$.

Theorem 12.3 *Both $\vee$ and $\wedge$ are* ***commutative****.*

$a \vee b = b \vee a. \qquad a \wedge b = b \wedge a.$

Proof

by the definition lub and glb.

Theorem 12.4 *Both $\vee$ and $\wedge$ are* ***associative****.*

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

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

Proof

Let $a \vee (b \vee c) = g$ and $(a \vee b) \vee c = h$.

$\therefore a \leq g, b \vee c \leq g, \therefore b \leq g, c \leq g.$ *g is ub.*

$\therefore a \vee b \leq g, c \leq g, (a \vee b) \vee c \leq g.$ *lub ≤ ub*

$\therefore h \leq g.$

$a \leq h, b \leq h, c \leq h.$ *h is ub.*

$\therefore a \leq h, b \vee c \leq h, a \vee (b \vee c) \leq h,$ *lub ≤ ub*

$\therefore g \leq h.$

Theorem 12.5 *Both $\vee$ and $\wedge$ are* ***idempotent****.*

$a \vee a = a \qquad a \wedge a = a$

Proof

$a \leq a \vee a$, *and since* $a \leq a$, $a \vee a \leq a$ *lub≤ub***.**

$\therefore a \vee a = a$

***Theorem 12.6 abortion property**.*

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

Proof

$a \le a \vee (a \wedge b).$ *$a \vee (a \wedge b)$ is ub of a*

Since, $a \wedge b \le a$ *$a \wedge b$ is lb of a*

$a \vee (a \wedge b) \le a \vee a = a.$ *T12.2, T12.5*

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

*$(A, \vee)$ and $(A, \wedge)$ are (**commutative**) **semigroups**.*

Example (N, max, min) defined by (N, ≤).

min(a, b) ≤ a, b ≤ max(a, b)

a ≤ b, and c ≤ d ⇒

min(a,c) ≤ min(b,d), and max(a,c) ≤ max(b,d).

max(a, b) = max(b, a),

min(a, b) = min(b, a). ***commutative***

min(a, min(b, c)) = min(min(a, b), c),

max(a, max(b, c)) = max(max(a, b), c). ***assoc**.*

max(a, a) = min(a, a) = a. ***idempotent***

max(a, min(a, b)) = a,

min(a, max(a, b)) = a. ***absortion***

(N, min) is a semigroup.

(N, max) is a momoid with identity 0.

Example (N^+, lcm, gcd) *defined by* $(N^+, |)$.

$gcd(a, b) \mid a, b \mid lcm(a, b)$.

$a \mid b$ *and* $c \mid d \Rightarrow$

$gcd(a, c) \mid gcd(b, d)$, *and* $lcm(a, c) \mid lcm(b, d)$.

$lcm(a, b) = lcm(b, a)$

$gcd(a, b) = gcd(b, a)$. ***commutative***

$lcm(a, lcm(b, c)) = lcm(lcm(a, b), c)$,

$lcm(a, lcm(b, c)) = lcm(lcm(a, b), c)$. ***assoc***.

$lcm(a, a) = gcd(a, a) = a$. ***idempotent***

$lcm(a, gcd(a, b)) = a$,

$gcd(a, lcm(a, b)) = a$. ***absortion***

(N^+, lcm) *is a monoid with identity with 1*

(N^+,gcd) *is a semigroup.*

Example $(P(S), \cup, \cap)$ *defined by* $(P(S), \subseteq)$.

$A \cap B \subseteq A, B \subseteq A \cup B$.

$A \subseteq B$ *and* $C \subseteq D$

$A \cup C \subseteq B \cup D$, *and* $A \cap C \subseteq B \cap D$.

$A \cup B = B \cup A$

$A \cap B = B \cap A$ ***commutative***

$(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$ ***associative***

$A \cup A = A \cap A = A$ ***idempotent***

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

$A \cap (A \cup B) = A$ ***absortion***

$(P(S), \cup)$ *is a monoid with identity* $\emptyset$.

$(P(S), \cap)$ *is a monoid with identity S.*

12.4 Distributive and Complemented Lattices

A lattice is a **distributive** *lattice, if*

the meet(∧) operation distributes over the join(∨) operation and

the join(∨) operation distributes over the meet(∧) operation.

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

Since ∨ and ∧ are comutative

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

Theorem 12.7 *If the meet operation distributes over the join operation, the join operation distributes over the meet operation, and vice versa.*

Proof

Assume ∧ distributes over ∨ and consider

$(a \vee b) \wedge (a \vee c)$	
$= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c)$	*∧ distributes over ∨*
$= a \vee ((a \vee b) \wedge c)$	*abortion*
$= a \vee ((a \wedge c) \vee (b \wedge c))$	*∧ distributes over ∨*
$= ((a \vee (a \wedge c)) \vee (b \wedge c)$	*∨ is associative*
$= a \vee (b \wedge c)$	*abortion*

Let $(A, \leq)$ be a lattice.

*$0 \in A$ is called **universal lower bound(bottom)**, if $^{\forall}a \in A, 0 \leq a$.*

*$1 \in A$ is called **universal upper bound(top)**, if $^{\forall}a \in A, a \leq 1$.*

***Theorem 12. 7** If there exists a **universal lower(upper)bound**, it is **unique**.*

***Proof** Assume $^{\exists}$**two** universal lower bound a and b*

$a \leq b, b \leq a. \therefore a = b.$

Example

$(2^A, \subseteq)$ universal lower bound(0) is $\emptyset$,

universal upper bound(1) is A.

***Theorem 12.8** Let $(A, \leq)$ ba a lattice, and 0 and 1 be **universal lower** and **upper bounds**. Then $^{\forall}a \in A$,*

$0 \vee a = a,$	*0 is **identity** for* $\vee$
$0 \wedge a = 0,$	*0 is **zero** for* $\wedge$
$1 \vee a = 1,$	*1 is **zero** for* $\vee$
$1 \wedge a = a.$	*1 is **identity** for* $\wedge$

Proof

$1 \leq 1 \vee a$,(ub) and $1 \vee a \leq 1$(uub)

$\therefore 1 \vee a = 1.$

$1 \wedge a \leq a$(lb) and $1 \wedge a \geq a \wedge a$(uub, Thm12.2) $= a$

$\therefore 1 \wedge a = a.$

Let (A, ≤) ba a lattice, and 0 and 1 be a ***universal lower*** *and* ***upper bounds****, respectively. Then*

a is said to be a ***complement*** *of b, if*

$a \vee b = 1$ *and* $a \wedge b = 0$.

(Example) (P(A), $\subseteq$*)* $A \cup \overline{A} = S$, $A \cap \overline{A} = \emptyset$.

If a is a ***complement*** *of b, b also is a* ***complement*** *of a. (commutative)*

An element may have ***many*** *complements, if any.*

Example: Fig 12.1

But 0 and 1 are ***unique complements*** *of each other.*

A lattice is said to be a ***complemented lattice****, if every elements has* ***complement(s)****.*

Theorem 12.9 *In a* ***distributive*** *lattice, if an element has a* ***complement*** *then this* ***complement*** *is* ***unique****.*

Proof *Suppose a has two complements* a_1 *and* a_2

$a \vee a_1 = 1, a \wedge a_1 = 0.$

$a \vee a_2 = 1, a \wedge a_2 = 0.$

$a_1 = a_1 \wedge 1$	*1 is the* ***identity*** *for* $\wedge$
$= a_1 \wedge (a \vee a_2)$	a_2 *is the* ***complement*** *of a*
$= (a_1 \wedge a) \vee (a_1 \wedge a_2)$	$\wedge$ ***distributes*** *over* $\vee$

$= \underline{0} \vee (a_1 \wedge a_2)$	*a_1 is the **complement** of a*
$= (\underline{a \wedge a_2}) \vee (a_1 \wedge a_2)$	*a_2 is the **complement** of a*
$= (a \vee a_1) \wedge a_2$	*$\wedge$ **distributes** over $\vee$*
$= 1 \wedge a_2$	*a_1 is the **complement** of a*
$= a_2$	*1 is an **identity** for $\wedge$.*

12.5 Boolean Lattice and Boolean algebra

*A **complemented** and **distributive** lattice is called a **boolean lattice**.*

*Since every element has a unique complement, **complement** is an **algebraic operator**.*

***complement**: **unary** operator on A.*

$\neg: A \to A$

*A boolean lattice $(A, \leq)$ defines an **boolean algebra** $(A, \vee, \wedge, \neg)$*

$\vee$ *join*

$\wedge$ *meet*

$\neg$ *complement*

$a \vee \neg a = 1,$ $\qquad a \wedge \neg a = 0.$

$\neg(\neg a) = a.$

Example

$(2^A, \cup, \cap, \overline{\ })$ *is a **boolean algebra** defined by the **boolean lattice** $(2^A, \subseteq)$*

Theorem 12.10 DeMorgan's laws

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

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

Proof

$(a \vee b) \vee (\neg a \wedge \neg b)$	
$= ((a \vee b) \vee \neg a) \wedge ((a \vee b) \vee \neg b)$	$\vee$ dist. over $\wedge$
$= ((a \vee \neg a) \vee b) \wedge (a \vee (b \vee \neg b))$	$\vee$ comm, assoc.
$= (1 \vee b) \wedge (a \vee 1)$	complement
$= 1 \wedge 1 = 1$	uub
$(a \vee b) \wedge (\neg a \wedge \neg b)$	
$= (a \wedge(\neg a \wedge\neg b)) \vee (b \wedge(\neg a \wedge\neg b)$	$\wedge$ dist. over $\vee$
$= 0 \vee 0 = 0$	..., ulb

$\therefore$ $a \vee b$ is a complement of $\neg a \wedge \neg b$

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

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

$(\{0, 1\}, \vee, \wedge, \neg)$ is a ***boolean algebra*** *defined by a lattice $(\{0, 1\}, \leq)$ with $(0 \leq 1)$*

$0 \vee 0 = 0,\ \ 0 \vee 1 = 1,\ \ 0 \vee 0 = 1,\ \ 1 \vee 1 = 1.$

$0 \wedge 0 = 0,\ \ 0 \wedge 1 = 0,\ \ 0 \wedge 1 = 0,\ \ 1 \wedge 1 = 1.$

$\neg 0 = 1, \neg 1 = 0.$

$(\{0, 1\}, \wedge, \vee, \neg)$ is a ***boolean algebra*** *defined by a lattice $(\{0, 1\}, \leq)$ with $(1 \leq 0)$*

$0 \wedge 0 = 0,\ \ 0 \wedge 1 = 0,\ \ 0 \wedge 1 = 0,\ \ 1 \wedge 1 = 1.$

$0 \vee 0 = 0,\ \ 0 \vee 1 = 1,\ \ 0 \vee 0 = 1,\ \ 1 \vee 1 = 1.$

Principle of Duality

12.6 Uniqueness of Finite Boolean Algebra

Boolean algebra
freedom?

Every *finite* ***boolean algebra*** *has* 2^n *elements*
for ***some*** $n > 0$.

There is a ***unique boolean algebra*** *of* 2^n *element*
for ***every*** $n > 0$.

$a \in A$ *is called to* ***cover*** $b \in A$,
if $b \le a$, $\not\exists c \in A$.э. $b < c < a$.*(Hasse diagram)*
$b \le c \le a,\ b \ne c,\ c \ne a$

Let $(A, \le)$ *be a lattice with* ***bottom*** *0.*
An element is called ***atom****, if it covers 0.*

Lemma 12.0
Let $(A, \le)$ *be a* ***finite*** *lattice with* ***bottom*** *0.*
$\forall b \ne 0 \in A$, $\exists$*an* ***atom*** $a \in A$.э. $a \le b$.

Proof
If b is an atom, $b \le b$.
If b is not an atom, since $(A, \le)$ *is a* ***finite*** *lattice,*
$\exists$*a chain* $0 < b_i < \ldots < b_2 < b_1 < b$
b_i *is an atom*

Lemma 12.1 *In a* ***distributed*** *lattice,*
if $b \wedge \neg c = 0$*, then* $b \leq c$*.*

Proof

$(b \wedge \neg c) \vee c = c$	$b \wedge \neg c = 0$
$(b \vee c) \wedge (\neg c \vee c) = c$	*distributive*
$b \vee c = c$	*1 is a identity for* $\wedge$*.*
$\therefore\ b \leq c$	*c is lub.*

Lemma 12.2 *Let* $(A, \vee, \wedge, \neg)$ *be a* ***finite boolean*** *algebra. Then*

$^{\forall}b \in A\text{-}\{0\}$, $1 \leq {}^{\exists}k \leq |A|$, $1 \leq {}^{\forall}i \leq k$, a_i*'s are* ***atoms*** *of A,*

$$b = a_1 \vee a_2 \vee \ldots \vee a_k.$$

Proof

Since $^{\forall}b \in A\text{-}\{0\}$, $1 \leq {}^{\exists}k \leq |A|$, $1 \leq {}^{\forall}i \leq k$,
a_i*'s are* ***atoms*** *of A and* $a_i \leq b$*.* — *L12.0*
$c = a_1 \vee a_2 \vee \ldots \vee a_k \leq b$*.* — *T12.2*
Suppose $b \wedge \neg c \neq 0$*.*
$^{\exists}$*an atom* $a \in A$ *.∋.* $a \leq b \wedge \neg c$*.* — *L12.0*
$\therefore\ a \leq b$ *and* $a \leq \neg c$*.* — *T12.2*
Since a is an atom, $a \leq c$
$\therefore\ a \leq c \wedge \neg c = 0$ — *T12.2*
But contradiction!
$\therefore\ b \wedge \neg c = 0$
$\therefore\ b \leq c$ — *L12.1*
$b = c = a_1 \vee a_2 \vee \ldots \vee a_k$*.*

Lemma 12.3 *Let $(A, \vee, \wedge, \neg)$ be a **finite** boolean algebra. Then*
$^{\forall}b \in A\text{-}\{0\}, 1 \le {}^{\exists}k \le |A|, 1 \le {}^{\forall}i \le k$, *$a_i$'s are **atoms** of A,*

$$b = a_1 \vee a_2 \vee \ldots \vee a_k.$$

*is the **unique** way to represent b as **join** of **atoms**.*

Proof

Suppose an alternative representation

$b = c_1 \vee c_2 \vee \ldots \vee c_t$.   *join of atoms*

$\therefore$ *For* $1 \le {}^{\forall}j \le t$,

$c_j \le b$.   *c_j's are atoms*

$\therefore c_j \wedge b = c_j$.

$c_j \wedge (a_1 \vee a_2 \vee \ldots \vee a_k) = c_j$.   *repalce b*

$(c_j \wedge a_1) \vee \ldots \vee (c_j \wedge a_k) = c_j$.   *$\wedge$ dist. over $\vee$.*

$\therefore 1 \le {}^{\exists}i \le k$.э. $c_j \wedge a_i \ne 0$.

Since both c_j and a_i are atoms, $c_j = a_i$.

$\therefore 1 \le {}^{\forall}j \le t, 1 \le {}^{\exists}i \le k$.э. $c_j = a_i$.

$\therefore t = k$.

Q.E.D.

Theorem 12.11 *Let (A, $\vee$, $\wedge$, $\neg$) be a* ***finite*** *boolean algebra and S be a set of* ***atoms****. Then (A, $\vee$, $\wedge$, $\neg$) is* ***isomorphic*** *to the boolean algebra (2^S, $\cup$, $\cap$, $^-$).*

Proof

Let (A, $\leq$) be a ***boolean lattice*** *and S be set of* ***atoms****.*

$f: A \rightarrow 2^S$

$f(b) = \{a \in S \mid a \leq b\}$

f is ***one-to-one onto****.(Lemma 12.2. 12.3)*

Thers is a ***isomorphism*** *f from*

any ***finite boolean lattice*** *(A, $\leq$) to*

finite power set latice *(2^S, $\subseteq$)*

where S is a set of ***atoms*** *of A.*

Any ***finite boolean algebra*** *(A, $\vee$, $\wedge$, $\neg$)*

is ***isomorphic*** *to the*

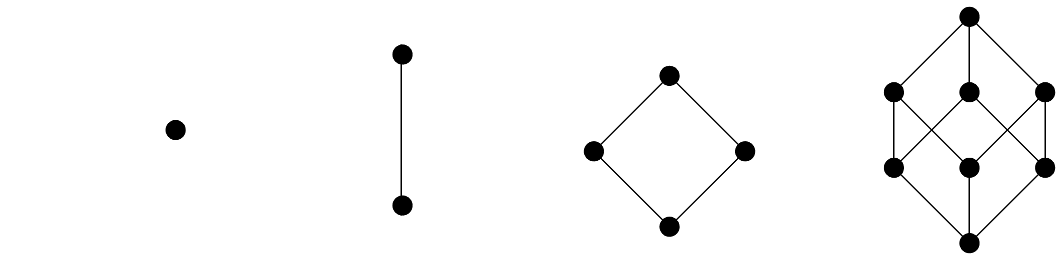
finite power set boolean algebra *(2^S, $\cup$, $\cap$, $^-$).*

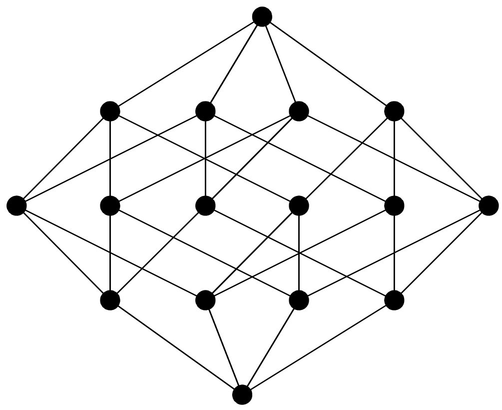
where S is a set of ***atoms*** *of A.*

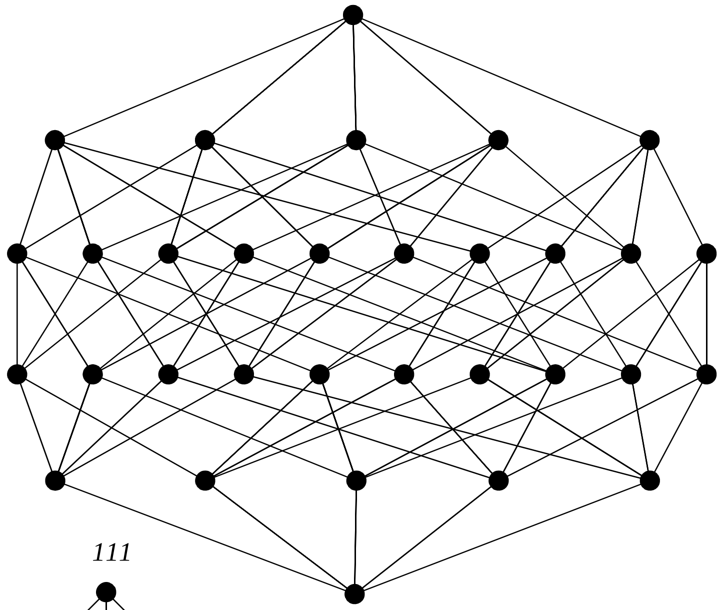
There exists a ***unique finite boolean algebra***

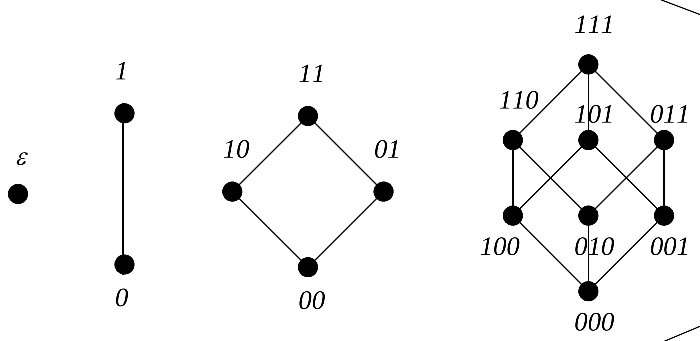
of $\mathbf{2^n}$ *elements for any n > 0, and*

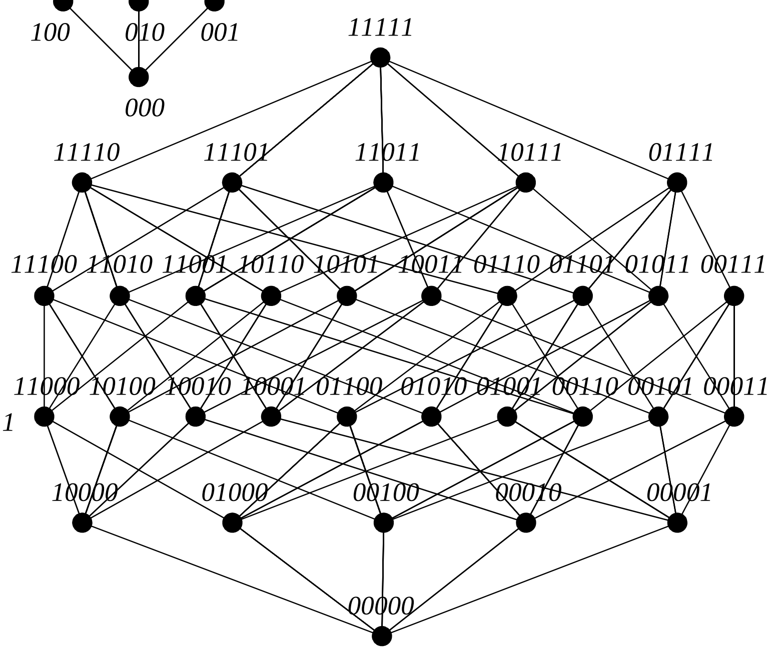
there is ***no*** *other finite boolean algebra.*

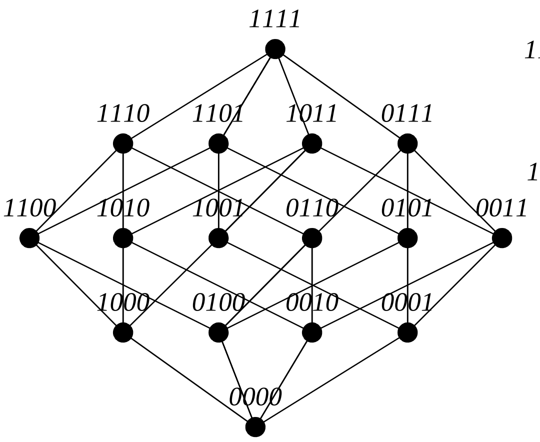







ε
1
0
11
10
01
00
111
110
101
011
100
010
001
000


11111
11110 11101 11011 10111 01111
11100 11010 11001 10110 10101 10011 01110 01101 01011 00111
11000 10100 10010 10001 01100 01010 01001 00110 00101 00011
10000 01000 00100 00010 00001
00000


1111
1110 1101 1011 0111
1100 1010 1001 0110 0101 0011
1000 0100 0010 0001
0000

12.7 Boolean Functions and Boolean Expressions

Let $(A, \vee, \wedge, \neg)$ be a boolean algebra.
Consider a function $f: A^n \rightarrow A$
    function
        $(|A|^n \times 1)$ table of $|A|$ values.
        ***closed form expression** with n variables.*

Let $(A, \vee, \wedge, \neg)$ be a boolean algebra.
*A **boolean expression** over $(A, \vee, \wedge, \neg)$ is defined*
1. *$a \in A$ is a **boolean expression**,*
2. *Any variable name is a **boolean expression**,*
3. *If e_1 and e_2 are **boolean expressions**, then*
   *$e_1 \vee e_2$, $e_1 \wedge e_2$, $\neg e_1$ are **boolean expressions**.*

***Syntactic grammar** of boolean expressions*

$B \rightarrow a$	$a \in A$.	
$\quad \mid \; v$	$v \in V$	*variable name.*
$\quad \mid \; B \vee B \mid B \wedge B \mid \neg B$		

Boolean expression over $(A, \vee, \wedge, \neg)$ is
    *a **language** over $A \cup V \cup \{\vee, \wedge, \neg\}$*
        *where V is a set of **variable** names.*

*A boolean expression that contains n **distinct** variable, is called a boolean expression with n-variables.*

*Let $E(x_1, \ldots, x_n)$ be a **boolean expression** of n-variables over an boolean algebra $(A, \vee, \wedge, \neg)$.*

$E(a_1, \ldots, a_n) \in A$ where $a_1, \ldots, a_n \in A$

assignment of values $a_1, \ldots, a_n$

to the variable $x_1, \ldots, x_n$.

Example

$E(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2) \wedge \neg(x_2 \vee x_3)$

$E(0, 1, 0) = (0 \vee 1) \wedge (1 \vee 0) \wedge \neg(1 \vee 0) = 0$

*Two boolean expressions of n variables are **equivalent**, if **every** assignment of values to n variables results same values.*

Let $E_1, E_2: A^n \to A$.

$E_1(x_1, \ldots, x_n) = E_2(x_1, \ldots, x_n)$, *if and only if,*

$\forall (a_1, \ldots, a_n) \in A^n,$

$E_1(a_1, \ldots, a_n) = E_2(a_1, \ldots, a_n).$

Example

$(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_3) = x_1 \wedge (x_2 \vee \neg x_3)$

***Equivalence** of two boolean expressions*

1. *Check every $|A|^n$ cases.*
2. *Properties of boolean algebra.*

$f: A^n \to A$ vs $E(x_1, \ldots, x_n)$

Not every function f has

*the **equivalent** boolean expression $E(x_1, \ldots, x_n)$*

*$f: A^n \to A$ is called **boolean function**,*

*if it can be specified by a **boolean expression***

*But $\{0, 1\}^n \to \{0, 1\}$ is always a **boolean function***

***Proof** Let $f: \{0, 1\}^n \to \{0, 1\}$.*

Let $(x_1, \ldots, x_n) \in V^n$. Then

*$\tilde{x}_1 \wedge \ldots \wedge \tilde{x}_n$ is a **minterm**, if $\tilde{x}_i = x_i$ or $\tilde{x}_i = \neg x_i$.*

*$\tilde{x}_1 \vee \ldots \vee \tilde{x}_n$ is a **maxterm**, if $\tilde{x}_i = x_i$ or $\tilde{x}_i = \neg x_i$.*

There are 2^n minterms and maxterms, resp.

***Disjunctions**($\vee$) of minterms whose f value is 1 is*

***equivalent** to f.*

$$\vee_{f(x_1 x, \ldots, x_n)=1} \tilde{x}_1 \wedge \ldots \wedge \tilde{x}_n$$

$$= (\tilde{x}_1 \wedge \ldots \wedge \tilde{x}_n) \vee \ldots \vee (\tilde{z}_1 \wedge \ldots \wedge \tilde{z}_n)$$

disjunctive normal form

***Conjunctions**($\wedge$) of maxterms whose f value is 0 is*

***equivalent** to f.*

$$\wedge_{f(x_1 x, \ldots, x_n)=0} \tilde{x}_1 \vee \ldots \vee \tilde{x}_n$$

$$= (\tilde{x}_1 \vee \ldots \vee \tilde{x}_n) \wedge \ldots \wedge (\tilde{z}_1 \vee \ldots \vee \tilde{z}_n)$$

conjunctive normal form

12.8 Propositional Calculus

*A **proposition** is a statement that may be either be **true**(T) or **false**(F)*

Consider a boolean lattice, ({F, T}, {F ≤ T})

*A **bolean algebra** ({F, T}, ∨, ∧, ¬) defined by a boolean lattice ({F, T}, {F ≤ T}).*

disjunction	∨
conjunction	∧
negation	¬

tautology	⇔ *T(1)*
contradiction	⇔ *F(0)*
disjunction	⇔ ***join***(∨, *lub*)
conjunction	⇔ ***meet***(∧, *glb*)
negation	⇔ ***complement***(¬)

condition	⇔ ***complement meet***	
$p \to q$	$\neg p \vee q$	$p \leq q.$
biconditional	⇔ ***complement meet join***	
$p \leftrightarrow q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$	$p = q.$
	$\equiv (\neg p \vee q) \wedge (p \vee \neg q)$	

12.9 Digital Network

$OR_n: \{0, 1\}^n \to \{0, 1\}$ *n-input OR gate*

$OR_n(x_1, \ldots, x_n) = x_1 \vee \ldots \vee x_n.$

$AND_n: \{0, 1\}^n \to \{0, 1\}$ *n-input AND gate*

$AND_n(x_1, \ldots, x_n) = x_1 \wedge \ldots \wedge x_n$.

$NOT_1: \{0, 1\} \rightarrow \{0, 1\}$ 1-input NOT gate

$NOT_1(x) = \neg x$.

Let $f: \{0, 1\}^n \rightarrow \{0, 1\}$ be a boolean function. Then f is equivalent to the composition of three gates.

Proof

*Let **disjuntive** normal form has $d(\leq 2^n)$ **minterms***

$1 \leq {}^\forall j \leq d$, we define minterm $i_j = AND_n(\hat{x}_1, \ldots, \hat{x}_n)$

where $1 \leq {}^\forall k \leq n$, $\hat{x}_k = x_k$, if $\tilde{x}_k = x_k$; $NOT_1(x_k)$ if $\tilde{x}_k = \neg x_k$.

Then f is equivalent to $OR_d(i_1, \ldots, i_m)$.

*Let **conjuntive** normal form has $c(\leq 2^n)$ **maxterms***

$1 \leq {}^\forall j \leq c$, we define maxterm $t_j = OR_n(\hat{x}_1, \ldots, \hat{x}_n)$

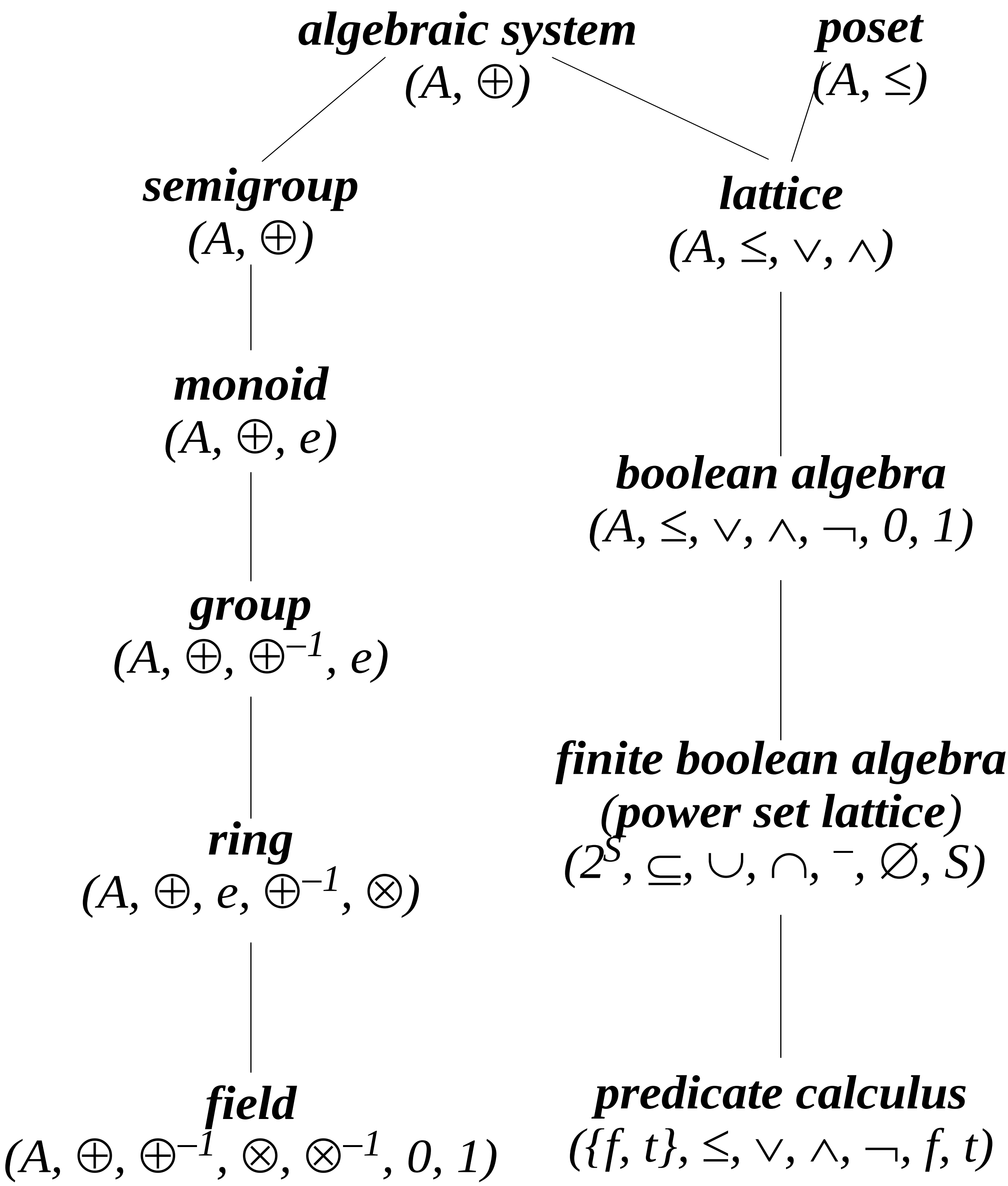
where $1 \leq {}^\forall k \leq n$, $\hat{x}_k = x_k$, if $\tilde{x}_k = x_k$; $NOT_1(x_k)$ if $\tilde{x}_k = \neg x_k$.

Then f is equivalent to $AND_c(i_1, \ldots, i_m)$.

Furthermore,

*f is equivalent to the composition of **three** gates, OR_2, AND_2, and NOT_1.*

*f is equivalent to the composition of **two** gates, NOR_2, $NAND_2$.*


algebraic system
$(A, \oplus)$
poset
$(A, \leq)$
semigroup
$(A, \oplus)$
lattice
$(A, \leq, \vee, \wedge)$
monoid
$(A, \oplus, e)$
boolean algebra
$(A, \leq, \vee, \wedge, \neg, 0, 1)$
group
$(A, \oplus, \oplus^{-1}, e)$
finite boolean algebra
(power set lattice)
$(2^S, \subseteq, \cup, \cap, ^{-}, \emptyset, S)$
ring
$(A, \oplus, e, \oplus^{-1}, \otimes)$
field
$(A, \oplus, \oplus^{-1}, \otimes, \otimes^{-1}, 0, 1)$
predicate calculus
$(\{f, t\}, \leq, \vee, \wedge, \neg, f, t)$