Modern Algebra

CS 2LC3

Ryszard Janicki

Department of Computing and Software, McMaster University, Hamilton, Ontario, Canada

- *Modern algebra* is the study of the structure of certain sets along with operations on them.
- The algebras discussed here are *semigroups, monoids, groups*, and *boolean algebras*. They are useful throughout computer science and mathematics.
- Semigroups and monoids find application in formal languages, automata theory, and coding theory.
- One boolean algebra is the standard model of the propositional calculus.
- Important in our study is not only the various algebras but their interrelationship.
- Thus, we study topics like *isomorphisms, homomorphisms*, and *automorphisms* of algebras.

The Structure of Algebras

- An algebra consists of two components:
  1. A set S of elements, called the *carrier* of the algebra.
  2. Operators defined on the carrier.
- Formally an algebra is a pair (S, Ψ), where S is a carrier and Ψ is a list of operators.
- Each operator is a total function of type $S^m \rightarrow S$ for some m, where m is called the *arity* of the operator.
- The algebra is *finite* if its carrier S is finite; otherwise, it is *infinite*.

- Formally an algebra is a pair (S, Ψ), where S is a carrier and Ψ is a list of operators.
- Each operator is a total function of type $S^m \to S$ for some m, where m is called the *arity* of the operator.
- Operators of arity 0, called *nullary* operators, are functions of no arguments.
- The nullary operators are interpreted as *constants* in the carrier.
- For example, we consider 1 to be a function that takes no arguments and returns the value one.
- Operators of arity 1 are *unary* operators; of arity 2 , *binary operators*; of arity 3 , *ternary operators*.
- Unary operators are written in prefix form (for example $-x$); binary operators in infix form (for example $a + b$).

Examples of Algebras

(a) The set of even integers and the operator $+$ form an algebra $(Even, +)$.

(b) The set of even numbers together with the operations multiplication and division is not an algebra, because division is not a total function on the even integers (division by 0 is not defined).

(c) The set $\{false, true\}$ and operators $\vee, \wedge$ and $\neg$, is an algebra $(\mathbb{B}, \vee, \wedge, \neg)$.
This is a finite algebra, because the set is finite.

Signatures

- The *signature* of an algebra consists of the name of its carrier and the list of types of its operators.
- For example, the algebra $(\mathbb{B}, \vee, \wedge, \neg)$ has the signature:
$$(\mathbb{B}, \mathbb{B} \times \mathbb{B} \to \mathbb{B}, \mathbb{B} \times \mathbb{B} \to \mathbb{B}, \mathbb{B} \to \mathbb{B})$$
- Two algebras are said to have the same signature if
  (i) they have the same number of operators and
  (ii) corresponding operators have the same types (modulo the name of the carrier).
- For example, algebras $(\mathbb{B}, \vee, \wedge, \neg)$ and $(\mathcal{P}(S), \cap, \cup, \sim)$ for some set S have the same signature.
- Algebra $(\mathcal{P}(S), \sim, \cup, \cap)$ has a different signature, since $\sim$ is of arity 1 and $\vee$ and $\cap$ are of arity 2 .

Identities

Definition

- An element 1 in S is a *left identity* (or *unit*) of binary operator $\circ$ over S if $1 \circ b = b$ (for $b \in S$);
- 1 is a *right identity* if $b \circ 1 = b$ (for $b \in S$); and
- 1 is an *identity* if it is both a left and a right identity.

Theorem

If c is a left identity of $\circ$ and d is a right identity of $\circ$, then $c = d$.

Proof.

$c = c \circ d = d$. ■

Zeros

Definition

- An element 0 in S is a *left zero* of binary operator $\circ$ over S if $0 \circ b = 0$ (for $b \in S$);
- 0 is a *right zero* if $b \circ 0 = 0$ (for $b \in S$); and
- 0 is an *zero* if it is both a left and a right zero.

- An algebra can have more than one left zero. For example, consider algebra $(\{b, c\}, \circ)$ with operator $\circ$ defined below.
  $b \circ b = b \quad c \circ b = c$
  $b \circ c = b \quad c \circ c = c$
- Both b and c are left zeros - and both are right identities!

Theorem

If c is a left zero of $\circ$ and d is a right zero of $\circ$, then $c = d$.

Proof.

$d = c \circ d = c.$ ■

Definition

1. A function $f : B \to C$ is *one-to-one* iff $f(b) = f(c) \implies b = c$ for all $b, c \in B$.
2. A function $f : B \to C$ is *onto* iff $Ran(f) = C$, i.e. for every $c \in C$ there is $b \in B$ such that $f(b) = c$.

Inverse

Definition

Let 1 be the identity of binary operator $\circ$ on S. Then b has a right inverse c with respect to $\circ$ and c has a left inverse b with respect to $\circ$ if $b \circ c = 1$. Elements b and c are called inverses of each other if $b \circ c = c \circ b = 1$.

Examples of inverses:

- In algebra $(\mathbb{Z}, +)$, 0 is an identity. Every element $b \in \mathbb{Z}$ has an inverse $-b$.
- In algebra $(\mathbb{R}, \cdot)$, 1 is an identity. Every element $b \in \mathbb{R}$ except 0 has an inverse $\frac{1}{b}$.
- Consider the set F of functions of arity 1 over a set S , and let $\bullet$ be function composition: $(f \bullet g)(b) = f(g(b))$. Then the function id given by $id(b) = b$ (for all $b \in S$) is an identity. Every onto function has a right inverse, every one-to-one function has a left inverse. Every one-to-one and onto function has an inverse.

Definition

A subset T of a set S is *closed* under an operator if applying the operator to elements of T always produces a result in T.

Example of closed operators

(a) The set of even integers is closed under $+$ because the sum of two even integers is even.

(b) Subset $\{0,1\}$ of the integers is not closed under $+$ because $1+1$ is not in this subset.

(c) Subset $\{0,1\}$ of the integers is closed under $\uparrow$ (maximum) because the maximum of any two of these integers is one of the integers. $\square$

Definition

(T, Φ) is a subalgebra of (S, Φ) if

(a) $\emptyset \subset T \subseteq S$, and

(b) T is closed under every operator in Φ.

Examples

(a) Algebra $\langle \mathbb{N}, + \rangle$ is a subalgebra of $\langle \mathbb{Z}, + \rangle$ because $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{N}$ is closed under $+$.

(b) $\langle \{0,1\}, + \rangle$ is not a subalgebra of $\langle \mathbb{Z}, + \rangle$ because $\{0,1\}$ is not closed under $+$.

(c) Algebra $\langle \{0,1\}, \cdot \rangle$ is a subalgebra of $\langle \mathbb{N}, \cdot \rangle$.

(d) Any algebra is a subalgebra of itself. $\square$

Definition

Let algebras $A = (S, \Phi)$ and $\hat{A} = (\hat{S}, \hat{\Phi})$ have the same signature. A function $h : S \to \hat{S}$ is an isomorphism from A to $\hat{A}$ if:

(a) Function h is one-to-one and onto.

(b) For each pair of corresponding nullary operators (constants) c in Φ and $\hat{c}$ in $\hat{\Phi}$, $h(c) = \hat{c}$.

(c) For each pair of corresponding unary operators $\sim$ in Φ and $\hat{\sim}$ in $\hat{\Phi}$, $h(\sim b) = \hat{\sim} h(b)$ (for b in S).

(d) For each pair of corresponding binary operators $\circ$ in Φ and $\hat{\circ}$ in $\hat{\Phi}$, $h(b \circ c) = h(b) \hat{\circ} h(c)$.

A and $\hat{A}$ are isomorphic, and $\hat{A}$ is the isomorphic image of A under h.

- Property (d) is sometimes depicted as the commuting diagram.

$$\begin{tikzcd} S \times S \arrow[r, "\circ"] \arrow[d, "h \quad h"'] & S \arrow[d, "h"'] \\ \hat{S} \times \hat{S} \arrow[r, "\hat{\circ}"] & \hat{S} \end{tikzcd}$$

Examples of Isomorphism

1. Let $A = (\mathbb{B}, \vee)$ and $\hat{A} = (\mathbb{B}, \wedge)$. Clearly A and $\hat{A}$ have the same signature. Define $h : \mathbb{B} \to \mathbb{B}$ by $h(b) = \neg b$. Function h is one-to-one and onto. Moreover:

$$h(b \vee c) = \neg(b \vee c) = \neg b \wedge \neg c = h(b) \wedge h(c).$$

2. Let $A = (\mathbb{N}, +)$ and $\hat{A} = (\mathit{even}, +)$, where *even* is the set of even natural numbers. A and $\hat{A}$ have the same signature. Define $h : \mathbb{N} \to \mathit{even}$ by $h(b) = 2 \cdot b$ (for $b \in \mathbb{N}$). Function h is one-to-one and onto. Moreover:

$$h(b + c) = 2 \cdot (b + c) = 2 \cdot b + 2 \cdot c = h(b) + h(c).$$

3. Let $A = (\mathbb{R}^+, \cdot)$ and $\hat{A} = (\mathbb{R}, +)$, where $\mathbb{R}^+$ is the set of positive real numbers. A and $\hat{A}$ have the same signature. Define $h : \mathbb{R}+ \to \mathbb{R}$ by $h(r) = \log(r)$ for $r > 0$, so that $h^{-1}(r) = 2^r$. Function h is clearly one-to-one and onto. Moreover:

$$h(b \cdot c) = \log(b \cdot c) = \log(b) + \log(c) = h(b) + h(c).$$

Theorem

1. *An isomorphism maps identities to identities, zeros to zeros, and inverses to inverses.*
2. *If $\hat{A}$ is an isomorphic image of A, then A is an isomorphic image of $\hat{A}$.*
3. *Let $\mathcal{C}$ be a set of algebras. The relation "A is isomorphic to $\hat{A}$" is an equivalence relation.*

Definition

An isomorphism from A to A is called an automorphism.

Examples of automorphism:

- Let $A = \hat{A} = (S, \Phi)$. Let h be the identity function on S,i.e. $h(b) = b$ for $b \in S$. Here h is automorphism.
- Let $A = \hat{A} = (\mathbb{Z}, +)$ and h be defined as $h(b) = -b$ for all $b \in \mathbb{Z}$. Again h is automorphism.

Homomorphism

Definition

Let algebras $A = (S, \Phi)$ and $\hat{A} = (\hat{S}, \hat{\Phi})$ have the same signature. A function $h : S \to \hat{S}$ is a homomorphism from A to $\hat{A}$ if it satisfies:

(a) For each pair of corresponding nullary operators c in Φ and $\hat{c}$ in $\hat{\Phi}$, we have $h(c) = \hat{c}$.

(b) For each pair of corresponding unary operators $\sim$ in Φ and $\hat{\sim}$ in $\hat{\Phi}$, $h(\sim b) = \hat{\sim} h(b)$ (for $b \in S$).

(c) For each pair of corresponding binary operators $\circ$ in Φ and $\hat{\circ}$ in $\hat{Phi}$, $h(b \circ c) = h(b) \hat{\circ} h(c)$ (for $b \in S$).

- An isomorphism is a homomorphism that is also one-to-one and onto.

Theorem

Let h be a homomorphism from $A = (S, \Phi)$ to $\hat{A} = (\hat{S}, \hat{\Phi})$. Then $(h(S), \hat{\Phi})$ is a subalgebra of $\hat{A}$, called the homomorphic image of A under h.

Proof.

We show that $(h(S), \hat{\Phi})$ satisfies the definition of a subalgebra.

(a) Since $h : S \to \hat{S}$, $h(S) \subseteq \hat{S}$.

(b) We show that $h(S)$ is closed under each binary operator $\hat{\circ}$ in $\hat{\Phi}$. Let $\hat{b}$ and $\hat{c}$ be in $h(S)$. Then there exist values b, c in S that satisfy $h(b) = \hat{b}$ and $h(c) = \hat{c}$. Moreover we have:

$$\hat{b}\hat{\circ}\hat{c} = h(b)\hat{\circ}h(c) = h(b \circ c).$$

Hence, $\hat{b}\hat{\circ}\hat{c}$ is in $h(S)$ and $h(S)$ is closed under $\hat{\circ}$. Similarly, $h(S)$ is closed under all the nullary and unary operators of $\hat{\Phi}$.

■

Examples of Homomorphism

(a) Function $h.b = 5 \cdot b$ is a homomorphism from algebra $\langle \mathbb{N}, + \rangle$ to itself. There are no unary operators, and $h(b+c) = 5 \cdot (b+c) = 5 \cdot b + 5 \cdot c = h.b + h.c$ (for b and c in $\mathbb{N}$). Actually, for any integer k (including 0), $h.b = k \cdot b$ is a homomorphism from $\langle \mathbb{N}, + \rangle$ to itself.

(b) Let $\oplus$ be the function defined by $b \oplus c = (b + c) \textbf{ mod } 5$. Then $h.b = b \textbf{ mod } 5$ is a homomorphism from $\langle \mathbb{N}, \oplus \rangle$ to $\langle 0..4, \oplus \rangle$.

Lattices as Algebras

Definition

A lattice is an algebra $(S, \sqcup, \sqcap)$, where $\sqcup$ and $\sqcap$, called *join* and *meet* are two binary, commutative and associative operators that satisfy, for all $a, b \in S$:

(a) $a \sqcup (a \sqcap b) = a$

(b) $a \sqcap (a \sqcup b) = a$

(c) $a \sqcup a = a$

(d) $a \sqcap a = a$

The axioms (a) and (b) are called *absorption laws*, (c) and (d) are called *idempotency laws*.

Example (Examples of Algebra Lattices)

- $(\mathbb{B}, \vee, \wedge)$ - Boolean Lattice,
- $(\mathcal{P}(S), \cup, \cap)$, where $S \neq \emptyset$ is a set - Set Lattice,
- $(\mathcal{R}, \uparrow, \downarrow)$, where $\uparrow$ is a maximum, and $\downarrow$ is a minimum, is a lattice.

Theorem

Let $(S, \sqcup, \sqcap)$ be a lattice algebra. Define a relation $\preceq$ on S as follows, for all $a, b \in S$: $\quad a \preceq b \iff a \sqcap b = a$.

The pair $(S, \preceq)$ is a partial order lattice.

Proof.

First note that $a = a \sqcap b \implies b = b \sqcup (b \sqcap a) = (a \sqcap b) \sqcup b = a \sqcup b$, so also $a \preceq b \iff a \sqcup b = b$. We will show that $\preceq$ is a partial order. From $a \sqcap a = a$ we have $a \preceq a$. Consider $a \preceq b \wedge b \preceq a$. We have $a \sqcap b = a \wedge a \sqcap b = b$ so $a = b$. Consider $a \preceq b \wedge b \preceq c$. Here we have $a \sqcap c = (a \sqcap b) \sqcap c = a \sqcap (b \sqcap c) = a \sqcap b = a$, so $a \preceq c$. Hence $\preceq$ is a partial order. We will show $a \sqcap b = glb(\{a, b\})$ and $a \sqcup b = lub(\{a, b\})$. We have $(a \sqcap b) \sqcup a = a \iff a \sqcap b \preceq a$ and $(a \sqcap b) \sqcup b = a \iff a \sqcap b \preceq b$, so $a \sqcap b$ is a lower bound of $\{a, b\}$. Consider c such that $c \preceq a \wedge c \preceq b$. Hence $c \sqcap a = c \wedge c \sqcap b = c$, i.e. $c = c \sqcap c = (c \sqcap a) \sqcap (c \sqcap b) = (a \sqcap b) \sqcap c)$, which means $c \preceq a \sqcap b$. So $a \sqcap b = glb(\{a, b\}$. Similarly we can show that $a \sqcup b = lub(\{a, b\})$. ■

Theorem

Let $(S, \preceq)$ be a partial order lattice. Define an algebra $(S, \sqcup, \sqcap)$, where $\sqcup, \sqcap$ are binary operators defined as follows, for all $a, b \in S$:

- $a \sqcap b = lub(\{a, b\})$,
- $a \sqcap b = glb(\{a, b\})$.

The algebra $(S, \sqcup, \sqcap)$ is a lattice algebra.

Proof.

Directly from the definition we have that $\sqcup, \sqcup$ are binary and symmetric. Moreover $lub(\{a, lub(\{b, c\})) = lub(\{a, b, c\})$ so lub is associative. and similarly for glb.
Since $glb(\{a\}) = lub(\{a\}) = a$, then the axioms (c) and (d) are satisfied.
Note that if $a \preceq b$ then $glb(\{a, b\}) = a$ and $lub(\{a, b\}) = b$. Since $c = glb(\{a, b\}) \preceq a$, so $lub(\{a, c\}) = a$, i.e. $lub(\{a, glb(\{a, b\})\}) = a$, or $a \sqcup (a \sqcap b) = a$, so the axiom (a) is satisfied. Similarly for (b). ∎

- Lattice algebra and partial order lattice are different model of the same concept, they are equivalent, however different applications, one of the models might be more convenient.

Sequences

Alphabet: an *arbitrary* (usually finite) set of elements, often denoted by the symbol Σ.

Sequence:

- an element $x = (a_1, a_2, \ldots, a_k) \in \Sigma^k$, where Σ^k is a Cartesian product of Σ's.
  For convenience we write $x = a_1 a_2 \ldots a_k$.
- a function $\phi : \{1, \ldots, k\} \to \Sigma$, such that $\phi(1) = a_1, \ldots, \phi(k) = a_k$.

♣ The two above definitions are in a sense identical since: $\underbrace{\Sigma \times \ldots \times \Sigma}_{n} \equiv \{f \mid f : \{1, \ldots, k\} \to \Sigma\}$.

- Frequently a *sequence* is considered as a primitive undefined concept that is understood and does not need any explanation.

Sequences and strings

- If the elements of Σ are *symbols*, then a *finite* sequence of symbols is often called a *string* or a *word*.
- The *length* of a sequence x, denoted $|x|$, is the number of elements composing the sequence.
- The *empty sequence*, ε, is the sequence consisting of zero symbols, i.e. $|\varepsilon| = 0$.
- A *prefix* of a sequence is any number of leading symbols of that sequence, and a *suffix* is any number of trailing symbols (any number means 'zero included').

- *Concatenation* (operation)
  Let $x = a_1 \dots a_k$, $y = b_1 \dots b_l$. Then
  $$x \circ y = a_1 \dots a_k b_1 \dots b_l.$$
  We usually write xy instead of $x \circ y$.
- Properties of concatenation:
  1. $x(yz) = (xy)z$
  2. $\varepsilon x = x\varepsilon = x$

  Fact. A triple $(\Sigma, \circ, \varepsilon)$ is a *monoid*, or *semigroup* (a concept discussed later).
- Power operator: $x^0 = \varepsilon$, $x^1 = x$ and $x^k = \underbrace{x \dots x}_{k}$.
- Recursive definition of power:
  $$x^0 = \varepsilon$$
  $$x^{k+1} = x^k x.$$
- Function $h : \Sigma^* \to \mathbb{N}$ defined by $h(z) = |z|$ is a *homomorphism* from $(\Sigma^*, \circ, \varepsilon)$ to $(\mathbb{N}, +, 0)$.

- Let Σ be a finite alphabet. Then we define Σ^* as:

$$\Sigma^* = \{a_1 \ldots a_k \mid a_i \in \Sigma \wedge k \geq 0\},$$

  i.e. the set of all sequences, including ε, built from the elements of Σ.
- A (*formal*) *language* over Σ is any subset of Σ^*, including the empty set $\emptyset$ and Σ^*.

Semigroups

Definition

A semigroup is an algebra $(S, \circ)$ where $\circ$ is a binary associative operator.

Example

- $(\Sigma^*, \circ)$, where $\circ$ is a string concatenation, is a semigroup (an important one).
- $([0, 1], \cdot)$, where "$\cdot$" is a multiplication is a semigroup.
- $(S, \uparrow)$, where S is any nonempty subset of the real numbers and $b \uparrow c$ is the maximum of b and c, is a semigroup.
- $(\{b, c\}, \circ)$, where $\circ$ is defined by $b \circ b = c \circ b = b$ and $b \circ c = c \circ c = c$. This is a finite semigroup (since S is finite).
- Let X be a set. $(Rel(X), \circ)$, where $Rel(X)$ is the set of all binary relations over X and $\circ$ is a composition of relations, is a semigroup.

Definition

Let T be a subset of carrier S of semigroup $(S, \circ)$. Suppose T is closed under $\circ$. Then algebra $(T, \circ)$ is called a subsemigroup of $(S, \circ)$.

Monoids

Definition

- A monoid $(S, \circ, 1)$ is a semigroup $(S, \circ)$ with an identity 1.
- If $\circ$ is also symmetric, the monoid is called Abelian
- A subalgebra of a monoid that contains the identity of the monoid is called a submonoid.

Example

- $(\Sigma^*, \circ, \varepsilon)$, where $\circ$ is a string concatenation, is a monoid. This monoid is not Abelian.
- $([0,1], \cdot, 1)$, where "$\cdot$" is a multiplication is an Abelian monoid.
- $(S, \uparrow)$, where S is any nonempty subset of the real numbers and $b \uparrow c$ is the maximum of b and c, is not a monoid, since $\uparrow$ has no identity in $\mathbb{R}$.
- $(\mathbb{N}, \uparrow, 0)$ in an Abelian monoid. Note that $0 \uparrow b = b \uparrow 0 = b$ for all $b \in \mathbb{N}$.
- Let X be a set. $(Rel(X), \circ, id_X)$, where $Rel(X)$ is the set of all binary relations over X and $\circ$ is a composition of relations, is a monoid. This monoid is not Abelian.

- Any semigroup $(S, \circ)$ can be made into a monoid $(S \cup \{c\}, \circ, c)$ for $c \notin S$ a fresh element that is defined to satisfy $c \circ b = b \circ c = b$ for all elements of $S \cup \{c\}$.
- For example, operator $\uparrow$ can be extended to $\mathbb{R} \cup \{\infty\}$ by $r \uparrow \infty = \infty \uparrow r = r$ for all elements of $\mathbb{R} \cup \{\infty\}$, so that $\uparrow$ has an identity.
- One must be wary of this extension, however, because other properties of the reals $\mathbb{R}$ may not hold for $\mathbb{R} \cup \{\infty\}$. For example, $1 + b > b$ does not hold for $b = \infty$.

Definition

A group is an algebra $(S, \circ, 1)$ in which

(a) $\circ$ is a binary, associative operator,

(b) $\circ$ has the identity 1 in S,

(c) Every element $b \in S$ has an inverse, which we write as b^{-1}.

A symmetric, commutative, or Abelian group is an Abelian monoid in which every element has an inverse.

Definition

A group is an algebra $(S, \circ, 1)$ in which

(a) $\circ$ is a binary, associative operator,

(b) $\circ$ has the identity 1 in S,

(c) Every element $b \in S$ has an inverse, which we write as b^{-1}.

A symmetric, commutative, or Abelian group is an Abelian monoid in which every element has an inverse.

Examples of groups

(a) The *additive group of integers* $\langle \mathbb{Z}, +, 0 \rangle$ is a group. The inverse b^{-1} of b is $-b$.

(b) Let K be the set of multiples of 5. Then $\langle K, +, 0 \rangle$ is a group. The inverse b^{-1} of b is the element $-b$.

(c) Let $n > 0$ be an integer. Define $\oplus$ for operands b and c in $0..(n-1)$ by $b \oplus c = (b + c) \textbf{ mod } n$. Then $M_n = \langle 0..(n-1), \oplus, 0 \rangle$ is a group, called the *additive group of integers modulo* n.

(d) $\langle \mathbb{R}, \cdot, 1 \rangle$ has identity 1 but is not a group, because 0 has no inverse.

(e) $\langle \mathbb{R}^+, \cdot, 1 \rangle$ is a group. The inverse r^{-1} of r in $\mathbb{R}^+$ is $1/r$. $\square$

Theorems for Groups

(18.18) $b = (b^{-1})^{-1}$

(18.19) **Cancellation:** $b \circ d = c \circ d \;\equiv\; b = c$

$d \circ b = d \circ c \;\equiv\; b = c$

(18.20) **Unique solution:** $b \circ x = c \;\equiv\; x = b^{-1} \circ c$

$x \circ b = c \;\equiv\; x = c \circ b^{-1}$

(18.21) **One-to-one:** $b \neq c \;\equiv\; d \circ b \neq d \circ c$

$b \neq c \;\equiv\; b \circ d \neq c \circ d$

(18.22) **Onto:** $(\exists x \mid : b \circ x = c)$

$(\exists x \mid : x \circ b = c)$

Proof of 18.18.

$(b^{-1})^{-1} = 1 \circ (b^{-1})^{-1} = b \circ b^{-1} \circ (b^{-1})^{-1} = b \circ 1 = b$ ∎

Definition

We define integral powers b^n of an element b of a group $(S, \circ, 1)$ as follows:

$$b^0 = 1$$
$$b^n = b^{n-1} \circ b \quad (\text{for } n > 0$$
$$b^{-n} = (b^{-1})^n \quad (\text{for } n > 0$$

Properties of powers of group elements

$$b^m \circ b^n = b^{m+n} \quad (\text{for } m \text{ and } n \text{ integers})$$

$$(b^m)^n = b^{m \cdot n} \quad (\text{for } m \text{ and } n \text{ integers})$$

$$b^n = b^p \;\equiv\; b^{n-p} = 1$$

Definition

A boolean algebra is an algebra $(S, \oplus, \otimes, \sim, 0, 1)$ in which

(a) $\oplus$ and $\otimes$ are associative binary operators;

(b) $\oplus$ and $\otimes$ are symmetric;

(c) 0 and 1 are the identities of $\oplus$ and $\otimes$;

(d) unary operator $\sim$ satisfies $b \oplus (\sim b) = 1$ and $b \otimes (\sim b) = 0$ (for all b); $\sim b$ is called the complement of b;

(e) $\otimes$ distributes over $\oplus$: $b \otimes (c \oplus d) = (b \otimes c) \oplus (b \otimes d)$;

(f) $\oplus$ distributes over $\otimes$: $b \oplus (c \otimes d) = (b \oplus c) \otimes (b \oplus d)$.

- $\oplus$ is often called "sum" or "plus", while $\otimes$ is often called "product" or " times".

Example

- $(\mathbb{B}, \vee, \wedge, \neg, \mathit{false}, \mathit{true})$ is a boolean algebra. It is our model for the propositional calculus, its provides intuition for the general definition.
- $(\mathcal{P}(S), \cup, \cap, \sim, \emptyset, S)$ is a boolean algebra, where S is any nonempty set. We call this a power-set algebra.
- For n in $\mathbb{Z}^+$, let F_n be the set of functions of type $\mathbb{B}^n \to \mathbb{B}$, i.e. the set of boolean functions of n boolean arguments. Let s denote a sequence of n boolean values. Define $\oplus, \otimes$ and $\sim$ by $(f1 \oplus f2)(s) = f1(s) \vee f2(s)$, $(f1 \otimes f2)(s) = f1(s) \wedge f2(s)$, $(\sim f)(s) = \neg f(s)$. Then $(F_n, \oplus, \otimes, \sim, f, t)$ is a boolean algebra. The identity of $\oplus$ is the function f that always yields *false*, and the identity t of $\otimes$ always yields *true*.

Definition

- The *greatest common* divisor b **gcd** c of integers b and c that are not both zero is the greatest integer that divides both. For example 24 **gcd** 30 $= 6$.
- The *least common multiple* b **lcm** c of b and c is the smallest positive integer that is a multiple of both b and c. For example 12 **lcm** 18 $= 36$.

Example

$(\{1, 2, 3, 6]\}, \mathbf{lcm}, \mathbf{gcd}, \sim, 1, 6)$, where $\sim x = \frac{6}{x}$m, is a boolean algebra.

Theorems for Boolean Algebras

(18.49) **Idempotency:** $b \oplus b = b, \quad b \otimes b = b$

(18.50) **Zero:** $b \oplus 1 = 1, \quad b \otimes 0 = 0$

(18.51) **Absorption:** $b \oplus (b \otimes c) = b, \quad b \otimes (b \oplus c) = b$

(18.52) **Cancellation:**
$$(b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \ \equiv \ c = d$$
$$(b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \ \equiv \ c = d$$

(18.53) **Unique complement:** $b \oplus c = 1 \wedge b \otimes c = 0 \ \equiv \ c = \sim b$

(18.54) **Double complement:** $\sim(\sim b) = b$

(18.55) **Constant complement:** $\sim 0 = 1, \quad \sim 1 = 0$

(18.56) **De Morgan:**
$$\sim(b \oplus c) = (\sim b) \otimes (\sim c)$$
$$\sim(b \otimes c) = (\sim b) \oplus (\sim c)$$

(18.57) $b \oplus (\sim c) = 1 \ \equiv \ b \oplus c = b, \quad b \otimes (\sim c) = 0 \ \equiv \ b \otimes c = b$

(18.58) A homomorphic image of a boolean algebra is a boolean algebra.

Partial Order Generated by a Boolean Algebra

Definition

Consider an arbitrary Boolean algebra $(S, \oplus, \otimes, \sim, 0, 1)$. Define the relations $\leq$ and $<$ on S as follows:

$$b \leq c \equiv b \otimes c = b$$

$$b < c \equiv b \leq c \wedge b \neq c$$

Theorem

Relation $\leq$ is a partial order.

Proof.

Since $b \otimes b = b$ then $b \leq b$, so $\leq$ is reflexive.
$b \leq c \wedge c \leq b \iff b \otimes c = b \wedge b \otimes c = c \iff b = c$, so $\leq$ is antisymmetric.
$b \leq c \wedge c \leq d \iff b \otimes c = b \wedge c \otimes d = c \iff$
$b \times c \otimes d = b \otimes d \iff b \leq d$. Hence $\leq$ is transitive. ∎

Lemma

$b \otimes c = b \iff b \oplus c = c$

Proof.

$(\Rightarrow) \quad b \oplus c = (b \otimes c) \oplus c = c.$

$(\Leftarrow) \quad b \otimes c = b \otimes (b \oplus c) = b.$ ■

Theorem

$b \leq c \iff b \oplus c = c$

Proof.

$b \leq c \iff b \otimes c = b \iff b \oplus c.$ ■

Atoms

- **Intuition**. Consider a Boolean algebra $(\mathcal{P}(S), \cup, \cap, \sim, \emptyset, S)$. The *singletons*, i.e. sets containing only one element, $\{b\}$, for all $b \in S$, can be called *atoms*, as they are not divisible and each non empty set can be built from them.
- Note that only $\emptyset$ is smaller than singletons with respect to the partial order $\subseteq$.

Definition

Consider an arbitrary Boolean algebra $(S, \oplus, \otimes, \sim, 0, 1)$.
An element $a \in S$ is called an atom if the following predicate is satisfied;

$$a \neq 0 \wedge (\forall b : S \mid 0 \leq b \leq a : 0 = b \vee b = a).$$

We then write $atom(a)$.

Properties of atoms of a boolean algebra

$$(18.64) \quad atom.a \;\Rightarrow\; a \otimes b = 0 \vee a \otimes b = a$$

$$(18.65) \quad atom.a \wedge atom.b \wedge a \neq b \;\Rightarrow\; a \otimes b = 0$$

$$(18.66) \quad (\forall a \mid atom.a : a \otimes b = 0) \;\Rightarrow\; b = 0$$

- Let B be a non-empty set. Clearly $B = \bigcup\{\{b\} \mid: b \in B\}$, or equivalently $B = \bigcup_{b \in B}\{b\}$.
- For example, $\{a, b, c, d\} = \{a\} \cup \{b\} \cup \{c\} \cup \{d\}$, $\mathbb{N} = \{1\} \cup \{2\} \cup \{3\} \ldots$, etc.
- Hence each set is a union of all singletons that it contains.
- Singletons are atoms of the Boolean algebra of sets, so each set is a union of all its atoms.
- We can extend this property to all finite Boolean algebras.

Theorem

Any element b of a finite Boolean different than 0 is equal to its "sum" of atoms, i.e. for every $b \in S$

$$b = \bigoplus(a \mid atom(a) \wedge a \oplus b \neq 0 : a).$$

Definition

For every $b \in B$, we define $y(b) = \bigoplus(a \mid atom(a) \wedge a \oplus b \neq 0 : a)$.

Lemma

$b \otimes y(b) = y(b)$

Proof.

Clearly $y(b) \in B$. We have:

$b \otimes y(b) = b \otimes \bigoplus(a \mid atom(a) \wedge a \oplus b \neq 0 : a) =$

$\bigoplus(a \mid atom(a) \wedge a \oplus b \neq 0 : b \otimes a = a) =$

$\bigoplus(a \mid atom(a) \wedge a \oplus b \neq 0 : a) = y(b)$, so we are done. ■

Lemma

$b \otimes \sim y(b) = 0$

Proof.

It suffices to show that for each atom s, $(b \otimes \sim y(b)) \otimes a = 0$. Then by property (18.66), page 37 of this Lecture Notes, we have $b \otimes \sim y(b) = 0$. We have to consider two cases; $b \otimes a = 0$ and $b \otimes a \neq 0$.

Case $b \otimes a = 0$: $(b \otimes \sim y(b)) \otimes a = 0 \otimes \sim y(b) = 0$.

Case $b \otimes a \neq 0$: We have $(b \otimes \sim y(b)) \otimes a =$
$b \otimes a \otimes \sim \bigoplus(c \mid atom(c) \wedge b \oplus b \neq 0 : c) =$
$b \otimes a \ \ \otimes (\sim a) \otimes \bigotimes(c \mid c \neq a \wedge atom(c) \wedge b \oplus b \neq 0 : \sim c) =$
$b \otimes 0 \otimes \bigotimes(c \mid c \neq a \wedge atom(c) \wedge b \oplus b \neq 0 : \sim c) = 0.$ ∎

Theorem

Any element b of a finite Boolean different than 0 is equal to its "sum" of atoms, i.e. for every $b \in S$

$$b = y(b) = \bigoplus(a \mid atom(a) \wedge a \oplus b \neq 0 : a).$$

Moreover $y(b) = \bigoplus(a \mid atom(a) \wedge a \leq b : a)$, and this representation is unique.

Proof.

We have proven: $b \otimes y(b) = y(b)$ and $b \otimes \sim y(b) = 0$.
We will show that $b = y(b)$.
We have $b = b \otimes 1 = b \otimes (y(b) \oplus (\sim y(b)) =$
$(b \otimes y(b)) \oplus (b \otimes (\sim y(b)) = y(s) \oplus 0 = y(s)$.
Clearly $atom(a) \wedge a \oplus b \neq 0 \;\equiv\; atom(a) \wedge a \leq b$, so
$y(b) = \bigoplus(a \mid atom(a) \wedge a \leq b : a)$, which immediately implies uniqueness. ■

Theorem

A boolean algebra with n atoms has 2^n elements.

Proof.

Since if $|X| = n$ then $|\mathcal{P}(X)| = 2^n$. ∎

Theorem

A finite boolean algebra $A = (S, \oplus, \otimes, \sim, 0, 1)$ *with* n *atoms is isomorphic to algebra* $\hat{A} = (\mathcal{P}(\{1, \ldots, n\}), \cup, \cap, \sim, \emptyset, \{1, \ldots, n\})$.

Proof.

Let label the elements of S with $\{1, \ldots, n\}$, i.e. assume $a_1, \ldots, a_n$ are atoms of S. Clearly A and $\hat{A}$ have the same signature. Define the function $h : S \to \mathcal{P}(\{1, \ldots, n\})$ by, for each $b \in S$,

$$h(b) = \{i \mid: atom(a_i) \wedge a_i \leq b\}.$$

Since the representation of each element of A as a sum is unique, this mapping is well defined, one-to-one, and onto. Clearly $h(0) = \emptyset$ and $h(1) = \{1, \ldots, n\}$, so h preserves constants.

Since $b = \bigoplus(i \mid: atom(a_i) \wedge a_i \leq b)$ we actually have
$h(\bigoplus(i \mid: atom(a_i) \wedge a_i \leq b)) = \{i \mid: atom(a_i) \wedge a_i \leq b\}$! Hence
$h(b \oplus c) = h(\bigoplus(i \mid: atom(a_i) \wedge a_i \leq b) \oplus \bigoplus(i \mid: atom(a_i) \wedge a_i \leq c)) =$
$h(\bigoplus(i \mid: (atom(a_i) \wedge a_i \leq b) \vee (atom(a_i) \wedge a_i \leq c))) =$
$\{i \mid: (atom(a_i) \wedge a_i \leq b) \vee (atom(a_i) \wedge a_i \leq c)\} =$
$\{i \mid: atom(a_i) \wedge a_i \leq b\} \cup \{i \mid: (atom(a_i) \wedge a_i \leq c\} = h(b) \cup h(b)$.
Similarly we can show $h(b \otimes c) = h(b) \cup h(c)$.
Define $c = \sim b$. Hence $b \oplus c = 1$ and $b \otimes c = 0$, i.e.
$h(b \oplus c) = h(b) \oplus h(c) = h(b) \cup h(c) = \{1, \ldots, n\}$ and
$h(b \otimes c) = h(c) \otimes h(c) = h(b) \cap h(c) = \emptyset$. Hence $h(b) = \{1, \ldots, n\} \setminus h(c)$, i.e.
$h(b) = \sim h(c)$. This means h is an isomorphism. ■