INTRODUCTION TO ALGEBRAIC CONCEPTS FOR COMPUTER FOUNDATIONS

George Epstein
Computer Science Department
Indiana University
Bloomington, Indiana 47401

TECHNICAL REPORT No. 18

INTRODUCTION TO ALGEBRAIC CONCEPTS
FOR COMPUTER FOUNDATIONS

GEORGE EPSTEIN

OCTOBER, 1974

INTRODUCTION TO ALGEBRAIC CONCEPTS FOR COMPUTER FOUNDATIONS

George Epstein
Computer Science Department
Indiana University
Bloomington, Indiana 47401

Part I. Introduction to Lattice Theory

I. Introduction

The operation "$\wedge$" in a lattice is the "AND gate" of logical computer design which picks the lowest of the input voltages as its output; the operation "$\vee$" in a lattice is the "OR gate" of logical computer design which picks the highest of the input voltages as its output. These operations correspond to .AND. and .OR. in most high-level programming languages. The following introduction to lattice theory will be of value to computer scientists interested in foundations of the logical design of computer structures, both in hardware and software, and related computer science.

II. Partially Ordered Sets

We begin by considering an arbitrary set or collection of objects P in which there is defined an equivalence relation $(=)$ and a binary relation $(\leq)$ whose ultimate nature depends on the set P and the purposes or semantics at hand, and which have the following properties:

(1) For all $a \in P$, $a \leq a$ i.e., the relation is reflexive.

(2) If $a \leq b$ and $b \leq a$, then $a = b$, i.e., the relation is antisymmetric.

(3) If $a \leq b$ and $b \leq c$, then $a \leq c$, i.e., the relation

is transitive. Such a set is called a partially ordered set w.r.t. the relation symbolized by $\leq$. We use the expression partially ordered since it is not required that at least one of $a \leq b$, $b \leq a$ must be true for every pair of elements a and b of P . If neither $a \leq b$ nor $b \leq a$, the elements a and b are said to be not comparable.

Since the name "partially ordered set" is somewhat long to read and write we shall abbreviate it henceforth to poset.

As an example, consider any set of positive integers and let $a \leq b$ mean "a is a divisor of b" . Then (1), (2), and (3) are all satisfied. That is, every set of positive integers is a poset w.r.t. the relation "is a divisor of." Note that there may well be integers a and b such that neither divides the other in such a set.

It is also easy to give an example of a set which is not a poset. Consider the set of all complex numbers $Z = X + Yi$ where X and Y are real. Then $|Z| = \sqrt{X^2 + Y^2}$. Let the relation $W \leq Z$ mean $|W| \leq |Z|$, where $\leq$ has its usual meaning. Then $W \leq W$ and also $W \leq Z$, $Z \leq V \Rightarrow W \leq V$. However, from $W \leq Z$ and $Z \leq W$ we cannot conclude $Z = W$ in the usual sense of "=" . E.g., $|2 - i| = |1 + 2i|$ but $2 - i \neq 1 + 2i$.

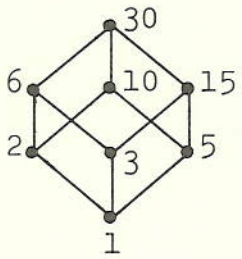
In a poset P we may have $a \leq b$ but $a \neq b$. In this case we write $a < b$. If $a < b$ and there exists no x in P such that $a < x < b$ we say b covers a .

When in addition to the three properties given, we have the further property that for every pair a and $b \in P$ $a < b$, $a = b$, or $b < a$ for every pair of elements a and b of P ,

then P is a completely ordered set or totally ordered set. The real numbers and the usual relation $\leq$ provide the most familiar example.

5.2 Hasse Diagrams of Posets

When a finite poset P contains a reasonably small number of elements, it can be represented conveniently by a figure. The elements of P are represented as points or small circules. If b covers a , we draw b on a higher level than a and connect b to a by a line. (Such a figure is called a Hasse diagram after the German algebraist Helmut Hasse.) For example, consider the poset consisting of the integers 1, 2, 3, 5, 6, 10, 15, 30, which are all the positive integral divisors of 30, and let $\leq$ mean "is a divisor of." Then the Hasse diagram is as follows:

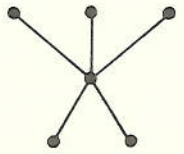


The Hasse diagrams serve to aid us in visualizing what we are working with, and also, as linear graphs, suggest tools, definitions, and theorems which may be of use.

III. Properties of Posets

We shall use the words under and over for the relations $\leq$ and $\geq$ of a partial ordering, with the latter terms being an obvious dual version of the former.

We define a maximal element of a poset P as one which is under no other element of P and a minimal element as one which is over no other. The poset in the diagram to the left has 2 minimal elements and 3 maximal ones. We have Theorem 1: A non-empty, finite poset P contains at least one maximal element and at least one minimal element.



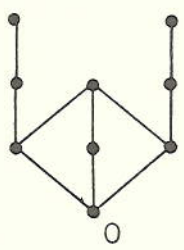
For let a be any element $\in P$. Then if a is not maximal, $\exists b \in P \ni a \in b$. If b is not maximal $\exists c \ni a < b < c$. Since P is finite, this chain must eventually terminate. The last element of the chain is then maximal since it is under no other.

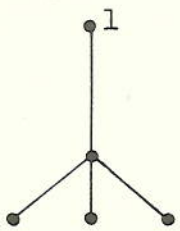
If a poset P contains an element Z which is under every other element of P, then Z is called a zero-element of P. Similarly, if P contains an element U which is over every other element of P, U is called a unit element of P. We have

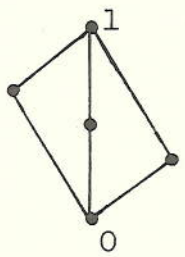
Theorem 2: A poset has at most one zero element and at most one unit element.

For if Z_1 and Z_2 are both zero elements, then $Z_1 \leq Z_2$ and also $Z_2 \leq Z_1$. Hence $Z_1 = Z_2$. Similarly for unit elements.

The zero element is customarily denoted by 0 and the unit element by 1, provided they exist. A poset may have a 0, or a 1, or both, as these examples show:

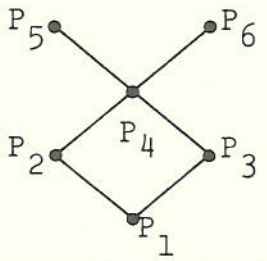






In a poset with a zero element, each element which covers 0 is called an atom. Similarly, in a poset with a unit element, each element covered by 1 is called an antiatom.

Consider now a subset Q of a poset P. There may exist an element $a \in P \ni$ for all $b \in Q$, $b \leq a$. Such an element is called an upper bound of Q.



E.g., in the figure to the left, let $Q = \{P_1, P_2, P_3\}$. Then P_4, P_5, P_6 are all upper bounds of Q. The upper bound P_4 obviously has a minimal sort of property in this respect. This suggests the following definition: if a is an upper bound of a subset Q of a poset P, and if a is under every upper bound of Q, then a is called a least upper bound of Q. Here P_4 is the least upper bound of $\{P_1, P_2, P_3\}$.

In analogous fashion, a lower bound of a subset Q of a poset P is defined as an element $b \in P$ $b \leq a$ for all $a \in Q$. If $Q = \{P_5, P_6\}$ in the preceding figure, then P_1, P_2, P_3, P_4 are all lower bounds for the subset Q. Here P_4 has an obvious maximal property which is reflected in this definition: if b is a lower bound of a subset Q of a poset P, and if b is over every lower bound of Q, then b is the greatest lower bound of Q.

Referring again to the figure, we see that the subset $\{P_1, P_2, P_3, P_4\}$ has the greatest lower bound (g.l.b.) P_1 and the least upper bound (l.u.b.) P_4. The set $\{P_4, P_5, P_6\}$ has g.l.b. P_4 but no upper bound at all. Note that a g.l.b. or l.u.b. of a subset of a poset may or may not belong to the subset, as the case may be. We have

Theorem 3: The l.u.b. (g.l.b.) of a subset Q of a poset P is unique if it exists.

For if a_1 and a_2 are both least upper bounds, then $a_1 \leq a_2$ and $a_2 \leq a_1$. Hence $a_1 = a_2$. Ditto for the g.l.b.

We make a final definition. In a poset P, partially ordered by $\leq$ we define the dual partial ordering $\geq$ thus: $a \geq b$ iff $b \leq a$. It is easy to verify that (1),(2),(3) hold for $\geq$. The Hasse diagram for P w.r.t. $\geq$ is like that of P w.r.t. $\leq$ except that it is turned upside down.

Since any theorem which is true for every partial ordering is thus true for $\geq$, we have the following principle of duality for posets:

Theorem 4: In every theorem about posets, expressed in terms of the symbol $\leq$, this symbol may be replaced by $\geq$ throughout and another true theorem results.

E.g., a poset P contains at most one zero element, i.e., at most one element $z \ni z \leq a$ for all $a \in P$. Dually then, P contains at most one element $\mu \ni \mu \geq a$ for all $a \in P$.

IV. Lattices

A lattice is defined to be a poset in which every pair of elements has a l.u.b. and a g.l.b.

Theorem 5: In a lattice L, every finite, non-empty subset has an l.u.b. and a g.l.b.

The theorem is true for $n = 1$, the element being its own g.l.b. and l.u.b. It is also true when $n = 2$, by the definition of a lattice.

Suppose now the theorem holds for all subsets containing 1,2, ...,k elements, so that a subset $a_1,a_2,\ldots,a_k$ of L has a g.l.b. and an l.u.b. Then if L contains more than k elements, consider the subset $\{a_1,a_2,\ldots,a_{k+1}\}$ of L .
Let $w = \text{l.u.b.}(a_1,a_2,\ldots,a_k)$. Then let $v = \text{l.u.b.}(w,a_{k+1})$. If now u is any upper bound of all of $a_1,a_2,\ldots,a_{k+1}$, u is in particular $\geq$ each of $a_1,a_2,\ldots,a_k$ and therefore $u \geq w$. Also $u \geq a_{k+1}$ and $\therefore u$ is an upper bound of w and a_{k+1} . Hence $u \geq v$. That is, since $v \geq$ each a_j , v is the l.u.b. of $a_1,a_2,\ldots,a_{k+1}$. The theorem follows for the l.u.b. by the principal of finite induction. A similar argument takes care of the g.l.b.

If L is finite and contains n elements, the induction process stops when $k + 1 = n$.

We say that a lattice is <u>complete</u> iff every non-empty finite or infinite subset of L has an l.u.b. and a g.l.b. Then we have at once

<u>Theorem 6: Every finite lattice is complete</u>

We now define in a lattice L two operations $\vee$: "sup" and $\wedge$:"inf"; $a \vee b = \text{l.u.b.}[a,b]$; $a \wedge b = \text{g.l.b.}[a,b]$.

More generally we define

$$\text{l.u.b.}[a_1,a_2,\ldots,a_k] = a_1 \vee a_2 \vee \ldots \vee a_k = \bigvee_{i=1}^{k} a_i$$

$$\text{g.l.b.}[a_1,a_2,\ldots,a_k] = a_1 \wedge a_2 \wedge \ldots \wedge a_k = \bigwedge_{i=1}^{k} a_i$$

If L is finite and $= [a_1,a_2,\ldots,a_n]$, then the following 2 elements exist:

g.l.b.$[a_1,a_2,\ldots,a_n]$, which we call "0" (Section 5.3)

l.u.b.$[a_1,a_2,\ldots,a_n]$, which we call "1" .

This amounts to giving the special names "0" and "1" to two of the elements of L . We have thus

Theorem 7: Every finite lattice contains a "0" and a "1" , where $0 = \bigwedge_{i=1}^{n} a_i$ and $1 = \bigvee_{i=1}^{n} a_i$. We prove next

Theorem 8: In every lattice, the following properties hold:

(L_1) $a \vee b = b \vee a$; $a \wedge b = b \wedge a$. (commutative)

(L_2) $(a \vee b) \vee c = a \vee (b \vee c)$; $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. (associative)

(L_3) $a \vee a = a$; $a \vee a = a$. (idempotent)

(L_4) $(a \wedge b) \vee a = a$; $(a \vee b) \wedge a = a$. (absorbtive)

(L_1) follows from the symmetrical nature of the definitions of $\vee$ and $\wedge$.

(L_2) may be proved thus: Let w = l.u.b.$[(a \vee b),c]$ and let v = l.u.b.$[a,b,c]$. Then $w \geq a \vee b$ and $w \geq c$, i.e., $w \geq a$, b , and c . Hence $w \geq v$ since v is the l.u.b. On the other hand, $v \geq a$ and b and also $v \geq c$. Hence $v \geq a \vee b$ and c . Hence $v \geq w$ since w = l.u.b.$[a \vee b,c]$. Hence $v = w$. Similarly, l.u.b.$[a,(b \vee c)] = v$, and (L_2) follows.

(L_3) is immediate from the definition.

(L_4) is proved thus: $a \wedge b \leq a$, by definition. Then l.u.b.$[a \wedge b,a] = a$ since $a \wedge b$ is below a ; i.e., $(a \wedge b) \vee a = a$. Similarly $a \vee b \geq a$, and hence g.l.b.$[a \vee b,a] = a$ since a is below $a \vee b$; i.e., $(a \vee b) \wedge a = a$.

The converse of the preceding theorem is also true:

Theorem 9: Any set L upon whose elements are defined $=$ and binary compositions $\vee$ and $\wedge$ in L, the latter satisfying (L_1), (L_2), (L_3), and (L_4) is a lattice.

What we have to show is that $\exists$ a relation $\leq$ which has properties (1), (2), and (3), and that w.r.t. this relation, $a \wedge b = \text{g.l.b.}[a,b]$ and $a \vee b = \text{l.u.b.}[a,b]$.

To prove the theorem, we define $a \leq b$ to mean $a \vee b = b$. Then we have:

(P_1): $a \leq a$ because $a \vee a = a$.

(P_2): $a \leq b$ and $b \leq a \Rightarrow a \vee b = b$ and $b \vee a = a$. But $a \vee b = b \vee a$. Hence $a = b$; i.e., (P_2) holds.

(P_3): $a \leq b$ and $b \leq c \Rightarrow a \vee b = b$ and $b \vee c = c \Rightarrow a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c \Rightarrow a \leq c$, so that (P_3) holds.

Now to prove $a \vee b = \text{l.u.b.}[a,b]$ w.r.t. $\leq$ as defined above, we note first that $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$. Hence $a \leq a \vee b$. Similarly $b \leq a \vee b$. Hence $a \vee b$ is an upper bound for a and b.

Now suppose c is any upper bound for a and b. Then $a \leq c$ and $b \leq c$; i.e., $a \vee c = c$ and $b \vee c = c$. Hence $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$, so that $a \vee b \leq c$; i.e., $a \vee b$ is the l.u.b. of a and b.

V. Lattices as Boolean Algebras

Recall that an infinite lattice need not have a 0 or a 1.

Theorem 10: In a lattice L with 0 and 1, for each $a \in L$,

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

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

In fact, $0 \wedge a = \text{g.l.b.}[0,a] = 0$ since 0 is the least element of L. Similarly, $0 \vee a = \text{l.u.b.}[0,a] = a$ since $0 \leq a$. Next $1 \vee a = \text{l.u.b.}[1,a] = 1$ since 1 is the greatest element of L and finally $1 \wedge a = \text{g.l.b.}[1,a] = a$ since $a \leq 1$. Thus 0 and 1 have the expected properties w.r.t. the operations $\vee$ and $\wedge$.

By analogy with our previous experiences, we define a distributive lattice as one in which $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. We have the apparently surprising

Theorem 11: In any lattice L

$[a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)]$ iff $[a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)]$.

Suppose first that $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a,b,c \in L$.

Then $a \vee (b \wedge c) = [a \vee (a \wedge c)] \vee (b \wedge c)$ by L_4

$= a \vee [(a \wedge c) \vee (b \wedge c)]$ by L_2

$= a \vee [c \wedge (a \vee b)]$ by the distributive law assumed in the hypothesis

$= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c]$ by L_4 and L_1

$= (a \vee b) \wedge (a \vee c)$ again by the distributive law assumed in the hypothesis. The other half of the theorem is obtained by a dual proof.

Next we define a lattice L with 0 and 1 elements to be a complemented lattice iff for each $a \in L \; \exists \; \bar{a} \in L \ni a \vee \bar{a} = 1$ and $a \wedge \bar{a} = 0$. The element $\bar{a}$ is called a complement of a. A simple example of a complemented lattice is the lattice of all the subsets of a set.

Theorem 12: In a distributive lattice with 0 and 1 , the complement is unique.

Suppose in fact $a \vee \bar{a} = 1$, $a \wedge \bar{a} = 0$ and $a \vee b = 1$, $a \wedge b = 0$.

Then $\bar{a} = \bar{a} \wedge 1 = \bar{a} \wedge (a \vee b) = (\bar{a} \wedge a) \vee (\bar{a} \wedge b) = 0 \vee (\bar{a} \wedge b) = \bar{a} \wedge b$.

By a similar computation, $b = b \wedge \bar{a}$; but $b \wedge \bar{a} = \bar{a} \wedge b$, so $b = \bar{a}$ and the complement is unique. We note in passing, however, that it is not an easy matter to decide whether a complemented lattice having unique complements must be distributive or not. At any rate, we are now ready to define a Boolean algebra using these concepts.

Definition: A lattice L with 0 and 1 that is distributive and complemented is a Boolean algebra.

VI. Summary

The above brings the computer scientist to a view of Boolean algebra in terms of lattice theory. For further details or information, see for example, G. Gratzer's "Lattice Theory, First Concepts and Distributive Lattices," Freeman, San Francisco, 1971.

Part II. Introduction to Ring Theory

I. Introduction

The properties of addition and multiplication are of basic importance to the computer scientist. The following introduction to ring theory provides not only a basic understanding of these properties, but also a view of Boolean algebra from the standpoint of this theory.

II. Rings

A ring, R , is a collection or set of elements with two binary operations called addition $\oplus$ and multiplication $\otimes$.

The properties of addition are:

(A.1) Containment

For every $u \in R$, $v \in R$, $u \oplus v \in R$.

(A.2) Associativity

For every $u \in R$, $v \in R$, $w \in r$.

$(u \oplus v) \oplus w = u \oplus (v \oplus w)$

Because of associativity, the parentheses in the above can be removed. Properties (A.1) and (A.2) define an additive semigroup.

(A.3) $u \oplus v = v \oplus u$ for all $u \in R$, $v \in R$

(A.4) For every $u \in R$, there is an element denoted by the symbol 0 such that $u \oplus 0 = u$.

(A.5) For every $u \in R$, there is an element denoted by $(-u)$ such that $u \oplus (-u) = 0$

Properties (A.1) , (A.2) , (A.3) , (A.4) , (A.5) define an additive Abelian group.

The properties of multiplication are:

(M.1) Containment

For every $u \in R$, $v \in R$, $u \otimes v \in R$.

(M.2) Associativity

For every $u \in R$, $v \in R$, $w \in R$.

$(u \otimes v) \times w = u \otimes (v \times w)$.

Properties (M.1) and (M.2) define a multiplicative semigroup. The parentheses in (M.2) can be dropped.

The connecting properties between these operations are:

(C.1) Distributivity on the left:

$u \otimes (v \oplus w) = (u \otimes v) \oplus (u \otimes w)$ for all $u \in R$, $v \in R$, $w \in R$.

(C.2) Distributivity on the right:

$(v \oplus w) \otimes u = (v \otimes u) \oplus (w \otimes u)$ for all $u \in R$, $v \in R$, $w \in R$.

A ring with unit is a ring with an element 1 such that

(V.1) $u \otimes 1 = u$, for all $u \in R$.

(V.2) $1 \otimes u = u$, for all $u \in R$.

A 2-ring with unit is a ring with unit such that

(T.1) $u \otimes u = u$, for all $u \in R$.

Definition: A 2-ring with unit is called a Boolean algebra.

III. Examples

Ex. 1. The ring of positive and negative integers under usual addition and multiplication is a ring with unit in which multiplication is commutative.

Ex. 2. The ring of positive and negative, even integers under usual addition and multiplication is a ring in which multiplication is a ring in which multiplication is commutative, but there is no multiplicative unit.

Ex. 3. The ring of 2 by 2 matrices with positive and negative integers as entries, under usual matrix addition and multiplication, is a ring with unit in which multiplication is not commutative. Further, the product of two elements can be 0 even though neither element is 0 .

Ex. 4. The ring consisting solely of 0 and 1 under binary addition and multiplication is a 2-ring with unit called the "two element Boolean algebra."

Ex. 5. The ring of all subsets of a set, with $S_1 \otimes S_2$ the subset of points common to S_1 and S_2 and $S_1 \oplus S_2$ the subset of points in S_1 or S_2 but not in both S_1 and S_2 , is a 2-ring with unit called the "Boolean algebra of subsets of a set."

IV. Elementary Consequences

(L.1) The element 0 is unique.

Proof: It must be shown that if there is an element $z \in R$ such that $u \oplus z = u$ for all $u \in R$, then $z = 0$.

Consider $z \oplus 0$.

By (A.4) , $z \oplus 0 = z$.

However, by (A.3) , $z \oplus 0 = 0 \oplus z$.

$= 0$ by the assumption .

Hence, $z = 0$.

(L.2) The element $(-u)$ is unique.

Proof: It must be shown that if there is an element $y \in R$ such that $u \oplus (y) = 0$ for any $u \in R$, then $y = (-u)$.

Consider $y \oplus (u \oplus (-u))$.

By (A.5), $y \oplus (u + (-u)) = y \oplus 0$

$= y$ by (A.4).

Consider $(y \oplus u) + (-u)$.

By (A.3), $(y \oplus u) \oplus (-u) = (u \oplus y) \oplus (-u)$

$= 0 \oplus (-u)$ by the assumption

$= (-u) \oplus 0$ by (A.3)

$= (-u)$ by (A.4).

Hence $y = (-u)$ by (A.2).

(L.3) In a ring with unit, the element 1 is unique.

Proof: As in (L.1)

(L.4) In a ring with unit $(-1) \otimes (-1) = 1$.

Initial comments: It must be shown that $(-1) \otimes (-1)$ is the inverse of (-1). Then, because $(-1) \oplus 1 = 1 \oplus (-1)$ by A.3)

$= 0$ by (A.5),

it will follow that $(-1) \otimes (-1) = 1$ by (L.2). However, to show $(-1) \oplus [(-1) \otimes (-1)] = 0$, since

$(-1) \oplus [(-1) \otimes (-1)] = [(-1) \otimes 1] \oplus [(-1) \otimes (-1)]$ by (V.1)

$= (-1) \otimes [1 \oplus (-1)]$ by (C.1)

$= (-1) \otimes 0$ by (A.5),

it will be enough to prove $u \otimes 0 = 0$ for all $u \in R$, since then the above steps can be reversed to obtain a proof.

Proof: $u \otimes 0 = 0$ for all $u \in R$ for

$u = u \otimes 1$ by (V.1)

$= u \otimes (1 \oplus 0)$ by (A.4)

$= (u \otimes 1) \oplus (u \otimes 0)$ by (C.1)

$= u \oplus (u \otimes 0)$ by (V.1)

and $0 = u \otimes 0$

Let $u = 1$. The $0 = (-1) \otimes 0$

$= (-1) \otimes [1 \oplus (-1)]$ by (A.5)

$= [(-1) \otimes 1] \oplus [(-1) \otimes (-1)]$ by (C.1)

$= (-1) \oplus [(-1) \otimes (-1)]$ by (V.1)

and $(-1) \otimes (-1) = 1$ by the above comments. Thus, this basic property follows from the properties of a ring with unit, without using (M.2) , (C.2) , and (V.2) .

(L.5) In a 2-ring with unit (i.e., a Boolean algebra), $v \oplus v = 0$ for all $v \in R$.

Proof: $u = u \otimes u$ for all $u \in R$ by (T.1) .

Hence $(v \oplus v) = (v \oplus v) \otimes (v \oplus v)$

$= [(v \oplus v) \otimes v] \oplus [(v \oplus v) \otimes v]$ by (C.1)

$= [(v \otimes v) \oplus (v \otimes v)] \oplus [(v \otimes v) \oplus v \otimes v]$ by (C.2) twice; $= [v \oplus v] \oplus]v \oplus v]$ by (T.1) four times; and and $v \oplus v = 0$ by (L.1) .

This is a basic property of binary addition.

(L.6) In a 2-ring with unit (i.e., a Boolean algebra), $u \otimes v = v \otimes u$ for all $u \in R$, $v \in R$.

Proof: $u \oplus v = (u \oplus v) \otimes (u \oplus v)$ by (T.1)

$= [(u \oplus v) \otimes u] \oplus [(u \oplus v) \otimes v]$ by (C.1) twice

$= [(u \otimes u) \oplus (v \otimes u)] \oplus [(u \otimes v) \oplus (v \otimes v)]$ by (C.2) twice;

$= [u \oplus (v \otimes u)] \oplus [(u \otimes v) \oplus v]$ by (T.1) twice

$= u \oplus [(v \otimes u) \oplus (u \otimes v) \oplus v]$ by (A.2)

$= u \oplus [(v \otimes u) \oplus (u \otimes v) \oplus v]$ by (A.2)

$= u \oplus [v \oplus ((v \otimes u) \oplus (u \otimes v))]$ by (A.3)

$= (u \oplus v) \oplus [(v \otimes u) \oplus (u \otimes v)]$ by (A.2)

So $0 = (v \otimes u) \oplus (u \otimes v)$ by (L.1)

Hence $u \otimes v = -(v \otimes u)$ by (L.2)

$= v \otimes u$

since $-(w) = w$ by (L.6) and (L.2) .

We say that multiplication is commutative in a 2-ring with unit. This is a familiar property of binary multiplication. Note that because of (A.3) in every ring, addition is commutative.

V. The above brings the computer scientist to a view of Boolean algebra in terms of ring theory. The emphasis here is on an understanding of the basic properties of addition and multiplication. For further details or information, a good beginning is N. McCoy's "Rings and Ideals."

Part III. Boolean Algebra

In Part I a definition of Boolean algebra was given as a particular kind of lattice, that is, as a distributive lattice with 0 and 1 which is complemented. In Part II another definition of Boolean algebra was given as a particular kind of ring, i.e., as a 2-ring with unit. The references given in Part I or Part II form a basis for further investigation along the lines of either of these definitions. Still other beginning approaches are found in many beginning books on computer science such as "Logic and Algorithms" by R.R. Korfhage, Chapter 2. Here we give two exercises which, taken together, establish that the two definitions of Part I and Part II are indeed equivalent.

1) Prove that any distributive lattice with $0,1$ which is complemented is also a 2-ring with unit. In other words, prove that the operation $\oplus$ is definable so that $x \oplus y$ may be given in terms or x,y and the operations $\vee,\wedge,-$; the operation $\otimes$ is definable so that $x \otimes y$ may be given in terms of x,y , and the operations $\vee,\wedge,-$; there is an element z of the lattice which behaves as the 0 of the ring; there is an element μ of the lattice which behaves as the 1 of the ring.

2) Prove that any 2-ring with unit is also a distributive lattice with $0,1$ which is complemented, i.e., prove that (a) the operation $\wedge$ is definable so that $x \wedge y$ may be given in terms of x,y and the operations $\oplus,\otimes$; (b) the operations $\wedge$ is definable so that $x \wedge y$ may be given in terms of x,y and the operations $\oplus,\otimes$; (c) there is an element e of the ring which

behaves as the 1 of the lattice; (d) there is an element r of the ring which behaves as the 0 of the lattice; (e) the operation - is definable so that $\bar{x}$ may be given in terms of x,0,1, and the operations $\oplus, \otimes$.

Further Problems

(i) Express $x \oplus y$ in terms of the operations $\vee, \wedge$, but using the operation - only once. Can this also be done for the important sum-with-carry expression $x \oplus y \oplus c$?

(ii) In a ring with unit where $v \otimes v \otimes v = v$ for all v , give a counter-example which shows that $v \oplus v \oplus v = 0$ need not hold for all v . Show that the integers 0,1,2(modulo 3) form a ring with unit satisfying both of these properties.

(iii) Prove that the NAND or STROKE function defined in a 2-ring with unit by $u/v = (u \otimes v) \oplus 1$ may be used as the sole operation in the proof of (2) above.

Typed by Christopher Charles