Chapter 4 Boolean algebras and Propositional Logic

Section 4.1 Boolean algebras

Let $(A, \leq)$ be a lattice, let $x, y \in A$. We say that y is a *complement of* x if

$$x \vee y = \top , \quad x \wedge y = \bot .$$

The concept comes from the algebra of sets. If $(A, \leq) = (\mathcal{P}(B), \subseteq)$, the lattice of subsets of B, then to say that Y is a complement of X in the lattice-theoretic sense just introduced is the same as to say that Y is the complement of X in the simple sense: $Y = B - X$ (see Chapter 1, Section 1.2, p. 12: "laws for complements").

If y is a complement of x, then x is a complement of y: the definition essentially symmetric in x and y, since $y \vee x = x \vee y$ and $y \wedge x = x \wedge y$.

The complement is not necessarily unique. E.g., in both displayed lattices on p. 90 of Chapter 3, both x and z are complements of y. However,

in a distributive lattice, the complement is unique: if y *and* z *are both complements of the same element* x, *then* $y = z$.

Indeed,

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$$

by the distributive law. But

$$x \vee y = \top \text{ and } x \wedge z = \bot$$

by the assumption on y and z. Substituting, we get

$$\top \wedge z = \bot \vee (y \wedge z) ,$$

that is, by $\bot \vee u = u$ (see p. 85, Chapter 3),

$$z = y \wedge z ,$$

which means (see the laws on p. 85, Chapter 3)

$$z \leq y .$$

The roles of z and y are completely symmetric; hence, by interchanging them in the above argument, we get

$$y \leq z .$$

Of course, we can now conclude that $z = y$, as promised.

The complement does not necessarily exist in a lattice even if the lattice is distributive. E.g., any *total* ordering with a maximal and a minimal element is a distributive lattice (*exercise*; show that, in this case, $x \wedge y = \min(x, y)$, where $\min(x, y) = x$ when $x \leq y$, and $\min(x, y) = y$ when $y \leq x$; and $x \vee y = \max(x, y)$, with $\max(x, y)$ defined similarly to $\min(x, y)$). However, if x is an element in such a total order which is not the maximal, nor the minimal, element, then x cannot have a complement; if y is any element, then $x \vee y = \max(x, y) = \top$ implies that $y = \top$, and $x \wedge y = \min(x, y) = \bot$ implies that $y = \bot$, thus $x \vee y = \top$ and $x \wedge y = \bot$ cannot hold at the same time.

A *Boolean algebra* is a distributive lattice in which every element has a complement. Since in a Boolean algebra, the distributice law holds, by what we saw above, the complement of any given element is uniquely determined; the complement of x is denoted by $-x$, or also by $\bar{x}$, or even $\neg x$.

A *complete Boolean algebra* is a complete lattice in which every element has a complement; that is, a complete lattice which is a Boolean algebra at the same time.

Let us note that in any distributive lattice, the **dual** version of the **distributive law** also holds:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) ;$$

here, we reversed the roles of the operations $\wedge$ and $\vee$ with respect to the original version of the distributive law. For the proof, we start by the right-hand side, apply the (first form of the) distributive law to it twice, and use the absorption laws at two places, until we arrive at the left-hand side:

$$(x \vee y) \wedge (x \vee z) = \underbrace{((x \vee y) \wedge x)}_{= x} \vee ((x \vee y) \wedge z) = x \vee ((x \wedge z) \vee (y \wedge z)) =$$

$$= x \vee \underbrace{(x \wedge z)}_{= x} \vee (y \wedge z) = x \vee (y \wedge z)$$

Since lattices can be described by operations and identities, without mentioning the ordering relation (namely, by saying that the items $\top$,$\bot$, $\wedge$, $\vee$ satisfy the associative, commutative, absorption, idempotent and identity laws), we can alternatively describe Boolean algebras by the lattice operations $\top$,$\bot$, $\wedge$, $\vee$, together with the operation of complementation, $-$, and require that these satisfy the lattice identities just mentioned, the distributive law (ensuring that the lattice is distributive), and the two **laws of complements**:

$$x \vee (-x) = \top , \quad x \wedge (-x) = \bot .$$

It turns out that this latter definition is slightly redundant. Alternatively, we have:

Boolean algebras may equivalently be defined by the following laws:

the **associative laws**:

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z$$

$$x \vee (y \vee z) = (x \vee y) \vee z$$

the **commutative laws**:

$$x \wedge y = y \wedge x$$

$x \vee y = y \vee x$

both **distributive laws**

$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

the **identity laws:**

$x \wedge \top = x$, $\qquad x \vee \bot = x$.

the laws of complements:

$x \vee (-x) = \top$, $\quad x \wedge (-x) = \bot$.

The original definition, which says that a Boolean algebra is an *ordered set with certain properties*, namely:

the top and bottom elements exist;
the meet and join of any two elements exist;
the complement of any element exists;
the *first* distributive law ($x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$) holds),

is preferable, however.

The powerset-lattice $\mathcal{P}(B)$ is a complete Boolean algebra. We pointed out before that it is a complete distributive lattice; and above, we pointed out that any $X \varepsilon \mathcal{P}(B)$ has a complement, namely $-Y = B - Y$. Following this example, in any Boolean algebra, we denote the unique complement of x by $-x$.

By what we said about the symmetry in the relation " y is a complement of x " translates into the statement that

$$--x = x,$$

"the law of double negation".

In the case of the powerset-algebra $\mathcal{P}(B)$, in Section 1.2 we talked about the difference $X - Y$ of two sets $X, Y \varepsilon \mathcal{P}(B)$. It is clear that $X - Y = X \wedge (-Y)$. Generalizing this operation, we define, in any Boolean algebra,

$$x - y \underset{\text{def}}{=} x \wedge (-y) ;$$

$x - y$ is called the *difference* of x and y. One can easily verify that

$$x - y = x - (x \wedge y) ,$$

and

$$(x - y) \vee (x \wedge y) = x , \quad (x - y) \wedge (x \wedge y) = \bot .$$

(*exercise*).

Note that, in the case of a powerset algebras, the last two equalities mean that x is the disjoint union of $x - y$ and $x \cap y$, which is an obvious fact. Another useful fact about the difference is this:

$$x \leq y \iff x - y = \bot .$$

Indeed, if $x \leq y$, then $x - y = x \wedge (-y) \leq y \wedge (-y) = \bot$, that is, $x - y = \bot$. On the other hand, if $x - y = \bot$, then $x \wedge (-y) = \bot$, hence,

$$x = x \wedge \top = x \wedge (y \vee -y) = (x \wedge y) \vee (x \wedge (-y)) = (x \wedge y) \vee \bot = x \wedge y ;$$

which means that $x \leq y$.

Let us verify **De Morgan's laws**

$$-(x \wedge y) = (-x) \vee (-y) , \qquad -(x \vee y) = (-x) \wedge (-y)$$

in any Boolean algebra; these laws were stated in Section 1.2 for sets. To prove the first law, we show that the element $(-x) \vee (-y) = -x \vee -y$ is the complement of $x \wedge y$; that is,

$$(x \wedge y) \vee (-x \vee -y) = \top \qquad (1)$$

and

$$(x \wedge y) \wedge (-x \vee -y) = \bot \ . \qquad (2)$$

Using distributivity in its dual form, we have

$$(x \wedge y) \vee (-x \vee -y) =$$

$$= (x \vee (-x \vee -y)) \wedge (y \vee (-x \vee -y))$$

$$= ((x \vee -x) \vee -y) \wedge ((y \vee -y) \vee -x)$$

(by associativity and commutativity)

$$= (\top \vee -y) \wedge (\top \vee -x)$$

$$= \top \wedge \top \qquad \text{(since } \top \vee \text{anything} = \top \text{)}$$

$$= \top \quad \text{(idempotence)} \ .$$

The proof of (2) is, essentially, the "dual" of that of (1): "interchange $\vee$ and $\wedge$ ". In fact, (2) is a *consequence* of (1), the latter applied in the "dual algebra". Let us explain the use of duality in some generality first.

Note that

if $(A, \leq)$ *is a Boolean algebra, then so its converse* $(A, \geq)$.

(the *converse* was mentioned in section 2.3; of course, $x \geq y$ means the same as $x \leq y$.) In fact, if $(A, \leq)$ is a lattice, then $(A, \geq)$ is also a lattice, in which the join operation is the same as the meet operation in $(A, \leq)$, the meet in $(A, \geq)$ is the join in $(A, \leq)$. Since $(A, \leq)$ is distributive, the dual distributive law holds in $(A, \leq)$, which means that the original law of distributivity holds in $(A, \geq)$ (and of course, as a consequence, also the dual law holds in $(A, \geq)$). In other words, $(A, \geq)$ is a distributive lattice. Finally, note that the top element of $(A, \geq)$ is the bottom element of $(A, \leq)$, and the bottom of $(A, \geq)$ is the

top of $(A, \leq)$; therefore, if we take x and its complement $-x$ in $(A, \leq)$, the two equations defining complements *when read in* $(A, \geq)$ become

$$x \wedge -x = \bot \ , \quad x \vee -x = \top$$

that is, $-x$ is again the complement of x in $(A, \geq)$.

We have shown that if $(A, \leq)$ is a Boolean algebra, then so is its converse $(A, \geq)$, and in fact, the top, bottom, meet, join and complement in the converse are the same as, respectively, the bottom, top, join, meet and complement in the original algebra. Thus, if we have shown some identity involving these operations to hold in any Boolean algebra, then the *dual identity* , obtained by changing top, bottom, meet, join to bottom, top, join and meet, respectively, and leaving complements alone, is again true in any Boolean algebra: the meaning of an equality in a Boolean algebra is the same as the meaning of its dual in the converse algebra.

Now, the dual of the identity (1) is

$$(x \vee y) \ \wedge \ (-x \wedge -y) \ = \top .$$

This is not quite the same as (2). However, since it is true for all values of the variables, we may replace x with $-x$, y with $-y$, and still have a true identity:

$$(-x \vee -y) \ \wedge \ (--x \wedge --y) \ = \top .$$

Since $--x = x$, $--y = y$, we get

$$(-x \vee -y) \ \wedge \ (x \wedge y) \ = \top ,$$

which is, up to commutativity, the same as (2).

We have shown the first De Morgan identity. The second one is the dual of the first one; therefore the second one holds as well.

Recall the notion of *isomorphism* from Chapter 2, Section 2.1. Recall that two isomorphic relations are "essentially the same" as far as "mathematically interesting" properties are concerned. For instance, it is easy to see that for two isomorphic relations, if one of them is a

lattice, so is the other; if one of them is a Boolean algebra, so is the other.

We are going to show that

Theorem

every finite Boolean algebra is isomorphic to a powerset algebra $(\mathcal{P}(B), \subseteq)$;

Paraphrasing, we may say that, up to isomorphism, all *finite* Boolean algebras are represented as powerset algebras.

In yet other words, we may say that the notion of Boolean algebra completely captures the notion of subset and the operations of union and intersection on subsets, at least as far as *finite* sets are concerned.

It should be noted, however, that there are many *infinite* Boolean algebras, even complete ones, that are very different from powerset algebras.

Towards proving the theorem, let us define an *atom* in any Boolean algebra, or in any order for that matter, to be any element on the *second level* in the order. This means, in the case of a Boolean algebra, that an atom a is not the bottom element, but there is no x such that $\bot<x<a$. In other words, a is an atom iff $x\neq\bot$, and from $x\leq a$ it follows that either $x=\bot$, or $x=a$. An atom is "indivisible" (which is the original meaning of the word "atom"): it does not have any "proper part".

Recall the notion of *height* of an element introduced in Section 3.1 in any *finite* order. Assume that our Boolean algebra is finite. Then an atom is an element whose height is exactly 2 ; the unique element of height 1 is $\bot$.

Note that the atoms in $(\mathcal{P}(B), \subseteq)$ are exactly the singletons $\{u\}$, with $u\in B$. In other words, the elements of the set B are, in a sense, represented in the set-algebra $(\mathcal{P}(B), \subseteq)$, namely by the atoms of the algebra. We claim that

in any finite Boolean algebra $(A, \leq)$, *every element is the join of the atoms below it*:

$$x = \bigvee \{a \varepsilon A \mid a \leq x \ \& \ a \text{ is an atom}\} . \tag{3}$$

Certainly, since A is a finite set, the join is the join of a finite set, therefore, it exists. To prove the equality, let us denote the join on the right-hand side by y. Since y is the join of some elements each of which is $\leq x$, we have that $y \leq x$. Now, consider the element

$$z = x - y .$$

What we want is that $z = \bot$; indeed, if $z = x - y = \bot$, then $x \leq y$; and since $y \leq x$ is true, the desired equality $x=y$ follows.

Now, assume that $z \neq \bot$, to derive a contradiction. In that case, the height, in the sense of Section 3.1, of z is at least 2. But then, as we noted in Section 3.1, there is at least one element b of height exactly 2 which is under z; in other words, there is an atom b such that $b \leq z$. Before proceeding, let us mark down this last, frequently used, conclusion:

In a finite Boolean algebra, every non-bottom element has at least one atom below it.

Now, since $b \leq z$, we have that

$$b \wedge y \leq z \wedge y = \bot ,$$

that is,

$$b \wedge y = \bot .$$

(Thus, in particular, if n is the number of atoms $\leq x$)

If a_i for $i < n$ are all the distinct atoms $\leq x$, then

$$y = a_0 \vee a_1 \vee \ldots \vee a_{n-1} ,$$

and so

$$\bot = b \wedge y = b \wedge (a_0 \vee a_1 \vee \ldots \vee a_{n-1}) =$$

$$= (b \wedge a_0) \vee (b \wedge a_1) \vee \ldots (b \wedge a_{n-1}) ;$$

thus, $b \wedge a_i \leq \bot$, and $b \wedge a_i = \bot$ for all $i<n$. But this means that

the atom b is different from each of the atoms a_i ;

if we had $b=a_i$, then $b \wedge a_i = b \neq \bot$. On the other hand, since $z \leq x$ and $b \leq z$, we have that $b \leq x$ and b is an atom; by the definition of the a_i's as all the atoms below x says that

the atom b is equal to a_i for some $i<n$.

The last two displayed sentences contradict each other. We have shown that $z \neq \bot$ leads to a contradiction; therefore, we have $z = \bot$, and thus $y=x$ as desired.

Let us point out another fact concerning atoms. In any Boolean algebra,

any two distinct atoms are disjoint, and any two disjoint atom are distinct:
if a, b *are atoms, then*

$$a \neq b \iff a \wedge b = \bot . ;$$

This is almost obvious. Suppose first that $a \neq b$. Since a is an atom, and $a \wedge b \leq a$, the only possibilities for $a \wedge b$ are $a \wedge b = \bot$ and $a \wedge b = a$. But the latter means that $a \leq b$; since $a \neq \bot$, and b is an atom, this means $a = b$, which we assumed was not the case. So, $a \wedge b = \bot$ must be the case. Conversely, assume $a \wedge b = \bot$. Since $a \neq \bot$, $a=b$ would mean $a \wedge b = a \neq \bot$. Thus, $a \neq b$.

Note that, in the case of the complete powerset-algebra $(\mathcal{P}(B), \subseteq)$, the atom $\{u\}$ is $\leq$ the set $X \in \mathcal{P}(B)$ just in case $u \varepsilon X$; thus, the atoms that are $\leq X$ correspond exactly to the elements of X. The equality (3) says, in this case, that any set X is the union of all singletons $\{u\}$ with $u \varepsilon X$, an obvious fact.

Let now $(A, \leq)$ be any finite Boolean algebra, let B the set of all atoms of $(A, \leq)$. We

define two mappings

$$A \underset{g}{\overset{f}{\rightleftarrows}} \mathcal{P}(B)$$

as follows:

$$x \overset{f}{\longmapsto} \{a \in A \mid a \leq x \ \&\ a \text{ is an atom}\}$$

and

$$\bigvee X \overset{g}{\longmapsto} X \quad .$$

In words: with any element x of the given Boolean algebra, f associates the set of atoms below x; with any set X of atoms, g associates the join of X.

We claim that the mappings f is an *isomorphism* of orderings, with g its inverse (which then becomes an isomorphism itself):

$$(A, \leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathcal{P}(B), \subseteq) \ ;$$

$$g \circ f = 1_A \ , \quad f \circ g = 1_B \ . \tag{4?}$$

Recall what we have to show, besides (4), for our claim; see (1) on page 37 in Section 2.1. We have to have

$$x \leq y \iff f(x) \subseteq f(y) \tag{4'?}$$

The most difficult part is (4?); we will grant this for the moment, and prove the rest; in this we will use (4); finally, we will prove (4).

First, we show

$$x \leq y \implies f(x) \subseteq f(y) \qquad (4.1?)$$

and

$$X \subseteq Y \implies g(X) \leq g(Y) \qquad (4.2?)$$

for all $x, y \in A$ and $X, Y \in \mathcal{P}(B)$.

If $x \leq y$, and $a \leq x$, then clearly, $a \leq y$. This implies directly that the implication (4.1) holds. (4.2) is the same as to say that

$$X \subseteq Y \implies \bigvee X \leq \bigvee Y$$

which is clear (why?). To see (4'), the left-to-right implication in (4') is (4.1); for the other implication:

$$f(x) \subseteq f(y) \underset{\uparrow\,(4.2)}{\implies} g(f(x)) \leq g(f(y)) \underset{\uparrow\,(4)}{\implies} x \leq y \,.$$

Now, for (4). The first equality under (4) is exactly the assertion under (3) (why?). Finally, let us show that $f \circ g = 1_B$. This means that for any set X of atoms, if $x = \bigvee X$, then

$$\{a \in A \mid a \leq x \;\&\; a \text{ is an atom}\} = X \,.$$

Now, clearly, the right-hand side is contained in the left-hand side (why?). Conversely, to show that the left-hand side is contained in the right-hand side, let a be an atom such that $a \leq x$, to show that $a \in X$. Since $x = \bigvee X$, we have $a \leq \bigvee X$, that is $a \wedge \bigvee X = a$. Let $X = \{b_i \mid i < n\}$. We have

$$a = a \wedge (b_0 \vee b_1 \vee \ldots \vee b_{n-1}) = (a \wedge b_0) \vee (a \wedge b_1) \vee \ldots \vee (a \wedge b_{n-1}) \,. \qquad (5)$$

In particular, each $a \wedge b_i \leq a$. Since a is an atom, either $a \wedge b_i = \bot$ or $a \wedge b_i = a$. It cannot be that for all i , $a \wedge b_i = \bot$, since then the union on the right-hand side of (5) would be $\bot$, and $a \neq \bot$. Therefore, for at least one i , $a \wedge b_i = a$. But then $a \leq b_i$, and thus, since b_i is an atom, and $a \neq \bot$, we must have $a = b_i$. This means that a is an element of X , which was our goal to show.

This completes the proof of the **Theorem**.

One consequence of the theorem is that a finite Boolean algebra $(A, \leq)$ must have a cardinality which is a power of 2 ;

$$|A| = 2^n \text{ for some } n \in \mathbb{N} ;$$

in fact,

if the cardinality of the set of atoms of a Boolean algebra A is n, *then* $|A| = 2^n$.

This is clear, since two isomorphic algebras have underlying sets of the same cardinality, and $|\mathcal{P}(B)| = 2^{|B|}$.

Thus, we have Boolean algebras of cardinalities $1 = 2^0$ (the degenerate Boolean algebra, the power-set of the empty set; $\mathcal{P}(\emptyset) = \{\emptyset\}$), $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, $16 = 2^4$, . . ., but none of powers in between.

Section 4.2 Generating Boolean subalgebras

A *Boolean subalgebra*, or more simply, a *subalgebra*, of a Boolean algebra $(A;\leq)$ is a subset that contains the top and bottom elements of A, and with any elements x and y, it contains $x\wedge y$, $x\vee y$ and $-x$ as well.

A *sublattice* was defined similarly in section 3.2, but with reference to complements removed. Thus, a subalgebra of a Boolean algebra is a sublattice of the ambient Boolean algebra, which is also closed under taking complements. A subalgebra of a Boolean algebra is again a Boolean algebra, with operations inherited from the ambient algebra.

Consider the figures on pages 62 and 63 in Section 3.1, Chapter 3. The one on page 62 is the Hasse diagram of $\mathcal{P}(\{0, 1, 2\})$, the Boolean algebra of all subsets of the set $\{0, 1, 2\}$. The one on page 63 is an isomorphic copy of the previous one; in particular, a Boolean algebra. Let us call this A, or more completely, $(A, \leq)$. Its underlying set is $A=\{0, 1, 2, 3, 4, 5, 6, 7\}$.

Now, the set $X = \{0, 1, 6, 7\}$ is a subset of A; and in fact it is a subalgebra of $(A, \leq)$. Indeed, the top and bottom elements, $\top=7$ and $\bot=0$, of A, are in X. The meet and join of any two elements of X are again in X: there is only one pair of incomparable elements, 1 and 6, in X, and $1\wedge 6=0\in X$, $1\vee 6=7\in X$. Finally, $\neg 1 = 7 \in X$, $\neg 7 = 1 \in X$. X is a Boolean algebra on its own right; the top and bottom elements of it are the same as those of A; meets, joins and complements are computed in it as in A. For instance, the equations $1\wedge 6=0\in X$, $1\vee 6=7$, $\neg 1=7$, $\neg 7=1$ are right when understood either in $(A, \leq)$ or in $(X, \leq)$.

On the other hand, the set $Y=\{0, 1, 2, 4\}$ is not a subalgebra of A since the top element of A, 7, is not in Y. On the other hand, note that on its own right, Y, with the ordering inherited from A, *is* a Boolean algebra: it is isomorphic to $\mathcal{P}(\{1, 2\}), \subseteq)$. For instance, Y has a top element, but it is 4, not 7, the top element of A.

The subset $Z=\{0, 2, 6, 7\}$ is a sub*lattice* of A, but not a subalgebra, since $2\in Z$, but $\neg 2 = 5$ is not in Z.

For any Boolean algebra $(A, \leq)$, the subset $\{\bot, \top\}$ consisting of the top and bottom

elements alone is always a subalgebra. The reason is that the operations $\wedge$, $\vee$ and $-$, when applied to $\bot$ or $\top$, result in $\bot$ or $\top$ again. In particular,

$$\top \wedge \bot = \bot, \qquad \top \vee \bot = \top, \qquad \neg\top = \bot, \qquad \neg\bot = \top.$$

The last two relations are particularly important. They directly follow from the first two, by the very meaning of what "complement" ($\neg$) means.

The whole of a Boolean algebra itself is a subalgebra. In fact, the latter is the maximal subalgebra; the set $\{\bot, \top\}$ is the minimal subalgebra.

Given any Boolean algebra $(A, \leq)$ and an arbitrary subset X of A, we have the subalgebra of $(A, \leq)$ *generated* by X. This may be defined as the least (smallest) subalgebra of $(A, \leq)$ containing X. Let us consider this carefully.

Consider the set $\mathtt{Subalg}(A, \leq)$ of all subalgebras of $(A, \leq)$. E.g., the set A is always in it; and so is the set $\{\bot, \top\}$. When the algebra is A on page 63 of Chapter 3, the set $\mathtt{Subalg}(A, \leq)$ consists of five elements:

$$\begin{aligned}\mathtt{Subalg}(A, \leq) = \{&\{0, 7\} = \{\bot, \top\},\\ &\{0, 1, 6, 7\},\\ &\{0, 2, 5, 7\},\\ &\{0, 3, 4, 7\},\\ &A\}\end{aligned}$$

To see this, note that a subalgebra must be of size 2, 4 or 8, by what we learned in the last section. The one of size 2 is $\{\bot, \top\}$, the one of size 8 is A; the ones of size 4 are given by a pair of elements (x, y) which are different from $\bot$ and $\top$, and which are complements of each other: $\neg x = y$. There are three such pairs: 1 and 6; 2 and 5; 3 and 4.

$\mathtt{Subalg}(A, \leq)$ is a subset of the power-set $\mathcal{P}(A)$; we claim that

$\mathtt{Subalg}(A, \leq)$ *is closed under intersection in* $\mathcal{P}(B)$:

when X_1 , X_2 , ... X_k are subalgebras of $(A, \leq)$, then the intersection $\bigcap_{i=1}^{k} X_i$ is again a subalgebra of $(A, \leq)$. (In fact, even an infinite intersection may be taken.)

The proof of this is quite easy once one decides to do it. Moreover, the essence of the matter has nothing to do with Boolean algebras. What is essential is only that we have a set A , some distinguished elements of it, in this case $\bot$ and $\top$, and a couple of operations on the set, in this case $-$ (unary) , $\wedge$, $\vee$ (both binary). The set $\mathtt{Subalg}(A, \leq)$ is, in the general case, replaced by the set S of all subsets that contain the distinguished elements, and which are closed under the operations. S is a subset of $\mathcal{P}(A)$, and, we assert, S is closed under intersection; the intersection of any number of elements of S is again a member of S .

For the sake of concreteness, let us return to the Boolean case. Consider the fact that the intersection of the second and third subalgebra of A in the example above is the first subalgebra; the assertion at hand says in this case that the intersection of any two members of that five-element set of sets is again a member of that five-element set.

Let us prove the assertion for $\mathtt{Subalg}(A, \leq)$ as stated above. To say that $\bigcap_{i=1}^{k} X_i$ is a subalgebra is to say, among others, that $\bot$ and $\top$ belong to $\bigcap_{i=1}^{k} X_i$. But this is clear since $\bot$ and $\top$ belong to each X_i . Further, we should see that $\bigcap_{i=1}^{k} X_i$ is closed under the operations $\wedge$, $\vee$, $-$; e.g., if x and y are in $\bigcap_{i=1}^{k} X_i$, then so is $x \wedge y$. But if x and y are in $\bigcap_{i=1}^{k} X_i$, then they are in X_i for each i ; since each X_i is a subalgebra, $x \wedge y \in X_i$; since this holds true for all i , $x \wedge y \in \bigcap_{i=1}^{k} X_i$ as required. The argument for $\vee$ and $-$ is identical. We have proved our claim.

Now, let X be an arbitrary subset of A , $(A, \leq)$ a Boolean algebra. Then we may look at the intersection of *all* subalgebras of $(A, \leq)$ containing X :

$$\langle X \rangle = \bigcap \{ Y \mid X \subseteq Y \ \& \ Y \text{ is a subalgebra of } (A, \leq) \} .$$

As an intersection of *some* subalgebras, $\langle X \rangle$ is again a subalgebra. Since X is a subset of each member of the set whose intersection is $\langle X \rangle$, it is clear that $X \subseteq \langle X \rangle$; $\langle X \rangle$ is a subalgebra containing X. But also, $\langle X \rangle$ is the *least* subalgebra containing X: whenever Y is a subalgebra of $(A, \leq)$, and $X \subseteq Y$, then necessarily, $\langle X \rangle \subseteq Y$: this is clear, since Y is *a particular member of the set whose intersection is* $\langle X \rangle$. We conclude that

$\langle X \rangle$, *the intersection of all subalgebras containing* X, *is the least subalgebra containing* X.

We call $\langle X \rangle$ the *subalgebra generated by* X. It may happen that $\langle X \rangle = A$, the generated subalgebra is the whole algebra; in this case, we say that X *generates the algebra* $(A, \leq)$.

Let us look at the example of $(A, \leq)$ on page 63 of Chapter 3 again. Let $X = \{1, 6\}$. Looking at the list of all subalgebras of A given above, we see that the ones containing $\{1, 6\}$ are A itself, and $\{0, 1, 6, 7\}$; the intersection of these two is the smaller one, $\{0, 1, 6, 7\}$;

$$\langle \{1, 6\} \rangle = \{0, 1, 6, 7\}.$$

Let us note a curious aspect of the definition of $\langle X \rangle$. $\langle X \rangle$ itself is a subalgebra containing X, hence, $\langle X \rangle$ itself belongs to the set whose intersection is $\langle X \rangle$! This seems to make the definition through intersection pointless; the definition of $\langle X \rangle$ seems to refer to $\langle X \rangle$ itself, among all subalgebras containing X. However, before we considered the intersection, we did not know that the least subalgebra containing X existed; the definition through the intersection is necessary to have a hold on the thing theoretically.

In general, it would very difficult to find the subalgebra generated by a subset by following the definition. The definition requires the consideration of all subalgebras containing the given set X. Of course, once we have one, say Y, then there is no need to consider any but the ones that are contained in Y; $\langle X \rangle$ will be contained in Y. If Y is large, it is of little help. We, of course, have A itself as one of the subalgebras containing X; taking this as Y does not cut down on the subalgebras we have to consider for getting $\langle X \rangle$.

There is another approach to the subalgebra $\langle X \rangle$ generated by X that is better from the point of view of calculation, but messier from a theoretical point of view. Let X be an

arbitrary subset of the Boolean algebra $(A, \leq)$. Then, besides the elements of X, all elements of the form

$$\bot,\ \top,\ x \wedge y,\ x \vee y,\ -x, \tag{8}$$

with x and y in X, are in $\langle X \rangle$. Moreover, all elements of the form

$$u \wedge v,\ u \vee v,\ -u,$$

where u and v come from the elements (8) just considered, will also belong to $\langle X \rangle$. E.g., this includes all elements of the form

$$(x \wedge y) \vee (x' \wedge y')$$

with x, y, x', y' from X. Clearly, we can continue in this way, and we may say that

all elements, including the elements of X itself, that can be expressed in terms of $\bot$, $\top$ and the elements of X, using, possibly repeatedly, the operations $\wedge$, $\vee$ and $-$, belong to $\langle X \rangle$.

Now, we claim, the elements mentioned in the last displayed paragraph are *precisely* the elements of $\langle X \rangle$. Since we already know that they all belong to $\langle X \rangle$, we only have to convince ourselves that the set S of these elements *is a subalgebra*: since $\langle X \rangle$ is the least subalgebra, and $S \subseteq \langle X \rangle$, it must then be the case that $S = \langle X \rangle$! But, once we said this, the assertion is clear: the set S contains, by its definition, the elements $\bot$, $\top$; and if u, v belong to S, then they are given as expressions in terms of the elements of X, and $\bot$, $\top$, $\wedge$, $\vee$, $-$, and so, the elements $u \wedge v$, $u \vee v$ are also given as expressions, one level more complicated though, in terms of the elements of X, and $\bot$, $\top$, $\wedge$, $\vee$, $-$, and thus, $u \wedge v$, $u \vee v$ belong to S again. We conclude that

the subalgebra $\langle X \rangle$ consists of all elements, including the elements of X itself, that can be expressed in terms of $\bot$, $\top$ and the elements of X, using, possibly repeatedly, the operations $\wedge$, $\vee$ and $-$.

It is good to realize that this last description of the subalgebra generated by a set is again quite independent of the concrete kind of "algebra" we are considering (in this case, "Boolean

algebra"). E.g., clearly, in the same way, we may talk about the sublattice of a lattice generated by a given set. Besides the definition as an intersection, we get that the sublattice generated by X is given as the Boolean subalgebra in the last description, except that we ignore the references to $-$. There are many other kinds of "algebras" considered in mathematics; the considerations just given apply to all of them.

Consider again this last description of the Boolean subalgebra generated by X. Constructing $\langle X \rangle$ involves collecting all *Boolean expressions* involving elements of X (this is just a short-hand for the elements described). Suppose we collect *some* of them, and we notice that the set of elements we have collected is already closed under the Boolean operations. Then, of course, we may stop, and have the given set equal to $\langle X \rangle$.

Let us reconsider the example of the Boolean algebra A on p. 63, Chapter 3, and its subset $X = \{0, 6\}$. $1 = -6$ and $7 = \top$; 1 and 7 are given as Boolean expressions in terms of X, and so, they belong to $\langle \{0, 6\} \rangle$. But, then we see that the set $X \cup \{1, 7\} = \{0, 1, 6, 7\}$ is already closed under the operations $\wedge$, $\vee$ and $-$ and it contains $\bot$ and $\top$ as well (in principle, by looking at all possible $u \wedge v$, $u \vee v$, with u and v from this set; in fact, now we know that $\{0, 1, 6, 7\}$ is a subalgebra of A since it appears in $\mathtt{Subalg}(A, \leq)$ above.); therefore, we conclude again that

$$\langle \{0, 6\} \rangle = \{0, 1, 6, 7\} .$$

Next, we give a theorem that describes the Boolean subalgebra $\langle X \rangle$ of any Boolean algebra generated by a set X in more explicit terms. This description will be quite specific to Boolean algebras; one does not have a similar description e.g. for the sublattice generated by a subset.

Let $(A, \leq)$ be a Boolean algebra, $X \subseteq A$. We consider the specific elements of A which are of the form

$$y_1 \wedge y_2 \wedge \ldots \wedge y_n$$

where each y_i is either x, or $-x$, with $x \in X$. These elements are called the *meet-expressions based on* X, or more simply, the *meets based on* X. The top element, $\top$, as the empty meet, is always, by definition, a meet based on X. Likewise, as the meet of the one-element set $\{x\}$, any element x of X is a meet based on X, and so is the

complement of any element of X.

If x_1, x_2, x_3, x_4 are elements of X (X may have further elements), then

$$-x_1 \wedge -x_2 \wedge x_3$$

$$x_1 \wedge -x_2 \wedge -x_3 \wedge x_4$$

$$-x_1 \wedge x_2 \wedge x_3 \wedge x_4$$

are examples of meets based on X.

We use an abbreviation to denote meets. We write

$$\overline{x}_1\overline{x}_2x_3\,,\quad x_1\overline{x}_2\overline{x}_3x_4\,,\quad \overline{x}_1x_2x_3x_4$$

for the above three examples, by ignoring the symbol $\wedge$, and putting the minus sign on top of the letters.

Next, still with the given X, we consider *arbitrary joins of X-based meets*. By definition, $\perp$ is always such a join: $\perp$ is the join of the empty set. In the example when $x_1, x_2, x_3, x_4 \in X$,

$$\overline{x}_1x_2x_3 \vee \overline{x}_1x_2x_3x_4 \vee \overline{x}_1\overline{x}_2x_3x_4$$

is another example of such an element. We call these elements the *join-meet expressions* based on X. The theorem promised above is as follows:

The set of all join-meet expressions based on the subset X of any Boolean algebra is identical to the subalgebra generated by X.

To be able to speak more briefly, let us denote the set of join-meet expressions based on X by

$\hat{X}$. We are claiming that

$$\langle X \rangle = \hat{X} .$$

Clearly, every element of $\hat{X}$ is an element of $\langle X \rangle$, $\hat{X} \subseteq \langle X \rangle$ (why?). To see that $\langle X \rangle \subseteq \hat{X}$, we have to see that $\hat{X}$ is a subalgebra containing X, that is, the following facts:

(1) Every element of X is equal to a join-meet expression based on X;

(2) $\perp$ and $\top \varepsilon \hat{X}$;

(3) If u and $v \varepsilon \hat{X}$, then $u \wedge v \varepsilon \hat{X}$, $u \vee v \varepsilon \hat{X}$, $-u \varepsilon \hat{X}$.

(1) and (2) are clear; likewise, the case of join in (3) (why?). Let $u, v \varepsilon \hat{X}$; then $u = \bigvee_{i=1}^{k} u_i$, $v = \bigvee_{j=1}^{\ell} v_j$, with each u_i, v_j a meet based on X. But then, by using the distributive law in its generalized form,

$$u \wedge v = \bigvee_{i=1}^{k} u_i \wedge \bigvee_{j=1}^{\ell} v_j = \bigvee_{\substack{i=1, \ldots, k \\ j=1, \ldots, \ell}} u_i \wedge v_j .$$

Now, notice that the meet of two meets based on X is again a meet based on X. This shows that $u \wedge v$ is a join-meet expression based on X. For use in the next argument, let us note that, as a consequence of the fact that the meet of any two elements of $\hat{X}$ is in $\hat{X}$, the meet of any finitely many elements of $\hat{X}$ belongs to $\hat{X}$ (we already know that $\top \varepsilon \hat{X}$).

Finally, let us turn to complements; assume $u = \bigvee_{i=1}^{k} u_i \varepsilon \hat{X}$, with each u_i a meet based on X; we want to show that $-u \varepsilon \hat{X}$. By the De Morgan law, we have

$$-u = -\bigvee_{i=1}^{k} u_i = \bigwedge_{i=1}^{k} -u_i . \qquad (9)$$

But, each u_i is of the form $u_i = \bigwedge_{p=1}^{q_i} y_p$, with y_p either an element, or a negated (complemented) element of X. By De Morgan's law, now applied to negating a meet rather than a join, we get that $-u_i = \bigvee_{p=1}^{q_i} -y_p$. Here, each $-y_p$ is still either x, or $-x$ for some $x \in X$. Namely, if y_p is x, then $-y_p$ is $-x$, and if y_p is $-x$, then $-y_p$ is $--x = x$. So in particular, each of the $-y_p$'s is a meet expression (of a very simple kind) based on X, hence, their join is a join-meet expression, and so, $-u_i \in \hat{X}$. Now, above we saw that the meet of any finitely many elements of $\hat{X}$ is again in $\hat{X}$. Therefore, by (9), $-u$ belongs to $\hat{X}$ as desired.

This completes the proof of the theorem asserting that $\langle X \rangle$ coincides with the set of all join-meet expressions based on X.

Now, let us consider the special case when X (but not necessarily A) is a finite set; $X = \{x_1, x_2, \ldots, x_n\}$. The *complete meets* based on X are those meet-expressions that use each x_i, straight or negated, exactly once. That is, the complete meets based on X are the expressions of the form $(\overline{})x_1 (\overline{})x_2 \ldots (\overline{})x_n$, with bars present or not present at will. If $n = 4$, then $x_1\overline{x_2}\overline{x_3}x_4$, $\overline{x_1}x_2x_3x_4$ are complete meets based on X, but $\overline{x_1}\overline{x_2}x_3$ is not necessarily one, unless it happens to be equal to one for an individual reason (this last happens, e.g., if $x_4 = \mathsf{T}$; then $\overline{x_1}\overline{x_2}x_3 = \overline{x_1}\overline{x_2}x_3x_4$).

In the case when X has 4 elements, we may form $2^4 = 16$ of these complete meets; this is the number of ways we can assign positive or negative signs to four elements independently of each other. Of course, there is no guarantee that all the elementary meets are distinct; the actual number of distinct complete meets may be less than 16.

We claim that, in case X is finite,

every meet based on X is the join of some complete meets based on X.

Indeed, note that

$$u = (u \wedge v) \vee (u \wedge -v) ,$$

or in an abbreviated form,

$$u = uv \vee u\overline{v} .$$

Namely, the distributive law, read backwards, says that

$$(u \wedge v) \vee (u \wedge -v) = u \wedge (v \vee -v) = u \wedge \mathsf{T} = u .$$

Using this equality, any meet-expression can be "completed" to read as a join of complete meet-expressions. E.g., suppose $X = \{x_1, x_2, x_3, x_4\}$, and let $u = x_1\overline{x_2}$. Then

$$\begin{aligned} x_1\overline{x_2} &= x_1\overline{x_2}x_3 \vee x_1\overline{x_2}\,\overline{x_3} \\ &= x_1\overline{x_2}x_3x_4 \vee x_1\overline{x_2}x_3x_4 \vee x_1\overline{x_2}\,\overline{x_3}x_4 \vee x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4} . \end{aligned}$$

Thus, if X is a finite set, then every meet-expression, and hence, every join-meet expression, based on X , is the join of complete meets based on X , and we get that

for a finite subset X *of a Boolean algebra, the subalgebra* $\langle X \rangle$ *generated by* X *is the set of all joins of complete meets based on* X .

We obtain an estimate of the cardinality of $\langle X \rangle$.

The subalgebra generated by a set of cardinality n *is at most* $2^{(2^n)}$.

The reason is that the number of complete meets based on X is at most 2^n ; we have at most $2^{(2^n)}$ sets of complete meets of which to form joins.

In particular,

in any Boolean algebra, a finite set generates a finite subalgebra.

This is not obvious on the basis of the definitions alone, and in fact, it does not hold true for many other kinds of "algebras" in mathematics; the sublattice generated by a finite subset of a lattice is not always finite.

The last result, together with the one from the last section that says that every finite Boolean algebra is isomorphic to a power-set algebra, allows us to make an inference of a general "logical" nature. We ask ourselves about *all possible identities* holding for the Boolean operations on sets. Certainly, since the power-set algebras are particular Boolean algebras, any identity that can be derived from the Boolean identities will hold for sets. But, is the converse true? That is, could there be an identity, say $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$, made up of the variables $x_1, \ldots, x_n$, and the Boolean operations $\top$, $\bot$, $\wedge$, $\vee$, $-$, which *does* hold whenever the x_i mean subsets of a fixed set A, and $\top$, $\bot$, $\wedge$, $\vee$, $-$ mean A, $\emptyset$, $\cap$, $\cup$ and $A-(\ )$, respectively, but which *does not* follow from the axioms for Boolean algebras? If such an identity existed, one could argue that the concept of Boolean algebra is "incomplete".

The answer to this question is "no"; such an identity cannot exist. In other words, if an identity holds in power-set algebras, then it holds in all Boolean algebras;

the concept of Boolean algebra is "complete" as far as identities for the Boolean operations on sets are concerned.

To see this, suppose that the identity $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$ holds in power-set algebras; let A be an arbitrary Boolean algebra, and $x_1, \ldots, x_n$ particular elements in A; we want to see that

$$p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) \qquad (9')$$

holds in A. Take $B \underset{\text{def}}{=} \langle \{x_1, \ldots, x_n\} \rangle$, the subalgebra of A generated by the given elements. It is enough to show that (9') holds in B, since the operations in B are the same as in A, except that they are restricted to a smaller set. But by what we proved, B is a finite Boolean algebra, and thus, it is isomorphic to $\mathcal{P}(C)$ for a finite set C. But, we assumed that (9') was true for any elements $x_1, \ldots, x_n$ in any algebra of the form $\mathcal{P}(C)$. Since B is isomorphic to $\mathcal{P}(C)$, (9') must hold in B for any elements $x_1, \ldots, x_n$ in B, in particular, also for the originally selected elements $x_1, \ldots, x_n$. And this is what we wanted to prove.

Next, let us point out that, for X a finite set,

the atoms of the Boolean algebra $\langle X \rangle$ are exactly those complete meet-expressions based on X which are not equal to $\perp$.

To see this, let Y be the set of all the complete meet-expressions based on X *that are not equal to* $\perp$. Still, every element of $\langle X \rangle$ is a join of elements of Y; the bottom can always be omitted from every join. Now, assume a is an atom in $\langle X \rangle$; it is a non-empty join of elements of Y; but, then for at least one $y \in Y$, $y \leq a$; since $y \neq \perp$, we must have that $a = y$. We have proved that every atom of $\langle X \rangle$ must be an element of Y. Conversely, let $y \in Y$, and

$$y = y_1 y_2 \cdots y_n$$

with $y_i = x_i$, or $-x_i$, where x_i $(i = 1, \ldots, n)$ are all the elements of X. We want to see that y is an atom in $\langle X \rangle$. Then, since $y \neq \perp$, as we noted above, there is an atom a of $\langle X \rangle$ below y, $a \leq y$. We just saw that a must belong to Y,

$$a = a_1 a_2 \ldots a_n,$$

where each $a_i = x_i$, or $-x_i$. We must have $a_i = y_i$; otherwise, $y_i = x_i$, and $a_i = -x_i$, or vice versa; thus, $a_i \wedge y_i = x_i \wedge -x_i = \perp$. But then $a \wedge y \leq a_i \wedge y_i = \perp$, and so, $a = a \wedge y = \perp$, contradicting that a is an atom. We thus have that, for each i, $a_i = y_i$; which of course implies that $a = a_1 a_2 \ldots a_n = y_1 y_2 \cdots y_n = y$. Since a is

an atom, and $y=a$, y is an atom as asserted.

Knowing the atoms of the Boolean algebra $\langle X\rangle$ gives us all the elements of that algebra, by the proposition proved in the previous section, according to which, in a finite Boolean algebra, each element is the join of the atoms below it. This now tells us again that every element of $\langle X\rangle$ is the join of some complete meets based on X. Note, however, that to reach the conclusion about the atoms of $\langle X\rangle$, we first had to prove the statement in the previous sentence -- thus, we did not do anything superfluous!

Let $X=\{x_1, x_2, \ldots, x_n\}$, with the x_i's (distinct) elements of the Boolean algebra $(A, \leq)$. Let us look at the subalgebra $\langle X\rangle$ generated by X more closely, with the exact determination of its cardinality in mind. Among the 2^n formal expressions

$$(\bar{x}_1)\ (\bar{x}_2)\ \ldots\ (\bar{x}_n),$$

where each letter x_i is either negated or non-negated, there are some which are equal to $\perp$; let us say that their number is k. The remaining 2^n-k expressions represent atoms. Moreover, it is clear that any two formally different expressions that are not equal to $\perp$ are *different* atoms: here, "formally different" means that at least one x_i appears in one unnegated, in the other negated. The reason is that the two expressions are disjoint, as a consequence of x_i and $-x_i$ being disjoint. Therefore, the algebra $\langle X\rangle$ has exactly 2^n-k atoms. But then, by what we learned in the previous section, we know that the cardinality of $\langle X\rangle$ is: $|\langle X\rangle| = 2^{(2^n-k)}$. In fact, $\langle X\rangle$ is isomorphic to a power-set algebra $\mathcal{P}(Y)$, where Y is a set of cardinality 2^n-k; Y can be taken to be what it denoted above: the non-bottom complete meets based on X.

When $k=0$, we say that the values $x_1, x_2, \ldots, x_n$ are *independent*. A set of elements of a Boolean algebra are independent if all the complete meet expressions based on them are different from the bottom element. This is equivalent to saying that the subalgebra generated by $x_1, x_2, \ldots, x_n$ is of cardinality $2^{(2^n)}$.

We can give a very neat description of *all* the finite Boolean subalgebras of a given Boolean algebra by looking at the above things a bit longer. Looking at any *finite* Boolean algebra, we know that every element, hence in particular the top element $\top$, is the join of the atoms below it, that is, all the atoms in the algebra. To repeat:

in any finite Boolean algebra, the top element $\top$ is the disjoint join of the set of all atoms in the algebra.

(Of course, a "disjoint join" means a join of pairwise *disjoint* elements, elements such that for any two distinct ones of them, say x and y, we have $x \wedge y = \bot$.)

If $x_1, x_2, \ldots, x_n$ are non-bottom elements of a Boolean algebra, which are pairwise disjoint and whose join is $\top$, we say that $\{x_1, x_2, \ldots x_n\}$ *is a partition of* $\top$. Of course, the expression comes from the fact that a partition of $\top$ in $\mathcal{P}(B)$ is the same thing as a partition of the set B in the usual sense.

Now, if C is a finite subalgebra of the Boolean algebra $(A, \leq)$, the atoms of C are disjoint in C, hence, *they are disjoint in the sense of* $(A, \leq)$ *as well*, since meet and bottom element are the same in $(C, \leq)$ and $(A, \leq)$. Also, for a similar reason, the join of the atoms of C is the top $\top$ of $(A, \leq)$ (which is the same as the top of $(C, \leq)$). We conclude that

the atoms of a finite subalgebra of a Boolean algebra form a partition of the top element of the Boolean algebra.

Note however that an atom of a subalgebra is far from necessarily being an atom of the big algebra; an atom of the subalgebra has no non-bottom element *of the subalgebra* under it, but it may have plenty of elements of the big algebra under it.

In particular, we conclude that

the atoms of any finite subalgebra of $\mathcal{P}(B)$ form a finite partition of the set B in the usual sense.

By the *Venn diagram* generated by a system $\{X_1, X_2, \ldots, X_n\}$ of subsets of a fixed set B we mean the partition of the set B whose cells are the *non-empty* complete intersection(=meet)-expressions based on $\{X_1, X_2, \ldots, X_n\}$, that is, all *non-empty* sets of the form

$$(-)X_1 \wedge (-)X_2 \wedge \ldots \wedge (-)X_n,$$

with the minus signs present or not in an arbitrary manner. The cells of the Venn-diagram generated by a system of sets are the atoms of the Boolean subalgebra generated by the given sets. The elements of that generated subalgebra are precisely the unions (joins) of the cells.

We have just seen that any finite subalgebra of a Boolean algebra gives rise to a partition of $\top$. Moreover, the subalgebra is completely given by this partition; it consists of the joins that can be formed using the elements of the partition.

Now, let us consider an *arbitrary* partition $\{x_1, x_2, \ldots, x_n\}$ of $\top$ in a Boolean algebra $(A, \leq)$. What are the atoms of the subalgebra generated by $\{x_1, x_2, \ldots, x_n\}$? Not surprisingly, the elements $x_1, x_2, \ldots x_n$ themselves! Just consider: an expression of the form

$$(-)x_1 \wedge (-)x_2 \wedge (-)x_3 \wedge \ldots \wedge (-)x_n$$

(which is the form any atom of the generated subalgebra will take) must be $\bot$ if there are two or more terms without $-$ in the expression; namely, any two distinct atoms are disjoint, and thus, any intersection in which two distinct atoms and possibly other things are terms is bottom. If all terms have minus signs, we just have

$$-x_1 \wedge -x_2 \wedge -x_3 \wedge \ldots \wedge -x_n$$
$$= -(x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_n) = -\top = \bot;$$

again, we got $\bot$. Therefore, the only way we get a non-bottom element, that is, an atom of the subalgebra, is when we have precisely one term without minus sign in the expression. Now, suppose this term without minus sign is the first one:

$$x_1 \wedge -x_2 \wedge -x_3 \wedge \ldots -x_n. \qquad (10)$$

But, since $x_1 \wedge x_2 = \bot$, we have

$$x_1 = x_1 \wedge \top = x_1 \wedge (x_2 \vee -x_2) = (x_1 \wedge x_2) \vee (x_1 \wedge -x_2) = \bot \vee (x_1 \wedge -x_2) = x_1 \wedge -x_2 .$$

We got that $x_1 \wedge -x_2 = x_1$. So, the element under (10) is

$$x_1 \wedge -x_3 \wedge \ldots -x_n .$$

Of course, by the same argument, $-x_3$, $\ldots -x_n$ can also be taken away, and we get that the element under (10) is just x_1.

Similar conclusion can be drawn if, instead of x_1, another x_i is the one term without a negative sign. We obtain, as promised, that

the atoms of the subalgebra generated by a partition of $\top$ *are precisely the elements of the partition.*

We conclude

the finite subalgebras of a Boolean algebra are in a one-to-one correspondence with the finite partitions of $\top$.

If we take $\mathcal{P}(B)$ to be the Boolean algebra, and if we consider that $\top$ is the set B itself, and a finite partition of B is the same as an equivalence relation with finitely many equivalence classes, we get that

the finite subalgebras of $\mathcal{P}(B)$ *are in a one-to-one correspondence with those equivalence relations on* B *which have finitely many classes.*

Of course, if B itself is finite, we do not have to stipulate that the equivalence relation have finitely many classes. Also, it is easy to see that if X and Y are two Boolean subalgebras of $\mathcal{P}(B)$, and E and F are the corresponding equivalence relation on B, then $X \subseteq Y$ iff $F \subseteq E$. We conclude:

For a finite set B, the lattice of Boolean subalgebras of $\mathcal{P}(B)$ is isomorphic to the converse of the lattice of equivalence relations on B.

Section 4.3. Boolean functions

Let us take another look at the simplest non-trivial Boolean algebra, $\mathcal{P}(\{0\})$, the power-set algebra based on a one-element set, chosen here as $\{0\}$. This has two elements, the empty set $\emptyset$, which is $\bot$ (bottom), and the set $\{0\}$, which is $\top$. Let us write $\mathbf{2}$ for this algebra; thus, $\mathbf{2} = \{\bot,\top\}$, with the total ordering given by $\bot < \top$. It is obvious, either because we are having a two-element total ordering, or because we are having an algebra of sets, that the Boolean operations are as follows:

$$\top \wedge \top = \top \qquad \top \wedge \bot = \bot$$

$$\bot \wedge \top = \bot \qquad \bot \wedge \bot = \bot$$

$$\top \vee \top = \top \qquad \top \vee \bot = \top$$

$$\bot \wedge \top = \top \qquad \bot \wedge \bot = \bot$$

$$-\top = \bot \qquad -\bot = \top .$$

We read $\top$ as **true**, $\bot$ as **false**; we read the operation $\wedge$ as **and**, $\vee$ as **or**, $-$ as **not**. In this way, the two-element Boolean algebra becomes an algebra of *truth-values*, and becomes the basis of *propositional logic*. In propositional logic, we analyze sentences into constituent parts out of which the sentence is built up using the *connectives*: $\wedge$ (conjunction; "and"), $\vee$ (disjunction; "or"), $\neg$ (negation; "not"; the difference to the "minus" sign, $-$, is inessential), and two more: $\longrightarrow$ (conditional; "if ..., then ...") and $\longleftrightarrow$ (biconditional; "if and only if").

We also call a sentence of the form $A \wedge B$ a *conjunction*, its terms A and B the *conjuncts* in the sentence. As indicated in the previous paragraph, the operation of conjunction is the one that forms $A \wedge B$ out of A, B. $A \vee B$ is a *disjunction*; A and B are its *disjuncts*. $A \longrightarrow B$ is a *conditional*; A is its *antecedent*, B its *succedent*. $A \longleftrightarrow B$ is a *biconditional*.

Consider the following sentences:

" n is divisible by 2 , or n is divisible by 3 ."

" n is divisible by 2 , and n is divisible by 3 ."

"If the greatest common divisor of n and 6 is not 1 , then n is divisible by 2 , or n is divisible 3 ."

" n is divisible by 6 if and only if n is divisible by 2 and n is divisible by 3 ."

By denoting the sentence " n is divisible by 2 " by A ;

$A \underset{\text{def}}{\equiv}$ " n is divisible by 2 ";

also

$B \underset{\text{def}}{\equiv}$ " n is divisible by 3 ",

$C \equiv$ " n is divisible by 6 ",

$D \equiv$ " The greatest common divisor of n and 6 is 1 ",

the above sentences may be analyzed, respectively, as

$E \underset{\text{def}}{\equiv} A \wedge B$,

$F \underset{\text{def}}{\equiv} A \vee B$,

$G \underset{\text{def}}{\equiv} (\neg D) \longrightarrow (A \vee B)$,

$H \underset{\text{def}}{\equiv} C \longleftrightarrow (A \wedge B)$.

The truth or falsity of the last four composite sentences depend on the truth-values of their constituents A, B, C and D. (Of course, the truth-value of each of A, B, C and D depend on the value of the n, which we assume to be a fixed, but unspecified, natural number.)

The dependence of the truth-value of E is exactly according to the truth-table given above describing the effect of the operation of $\wedge$ (conjunction) on the two truth-values. That is to say, if A and B are both **true**, so is $E \equiv A \wedge B$; in any other of the three cases concerning the values of A and B: $(\top, \bot)$, $(\bot, \top)$, and $(\top, \bot)$, the value of $A \wedge B$ is **false**. This corresponds to the ordinary use of the connective "and".

The truth-value of $F \equiv A \vee B$ is computed according to the truth-table for $\vee$ (disjunction) given above. E.g., if $n = 6$, or if $n = 2$, or if $n = 3$, $A \vee B$ is **true**; in fact, according to the first three lines of that table, in the given order. However, if $n = 1$, then $A \vee B$ is **false**; this corresponds to the last line of the table. Notice that disjunction as we are describing it here is *non-exclusive "or"*; a disjunction is **true** if, in particular, both disjuncts are **true**. The sentence in question is, in more explicit form,

"Either n is divisible by 2, or n is divisible by 3, or both."

Let us note that in mathematics, "or" (disjunction) is *always* intended as non-exclusive "or". (With exclusive "or", a disjunction would be true just in case *precisely one* disjunct is true.) This may be seen e.g. on the sentence G that is regarded as being true, no matter what n is. If $n = 6$, then the succedent of the conditional, $A \vee B$ is **true** under the non-exclusive interpretation, but not under the exclusive one.

The connective of negation as used in mathematical language, clearly corresponds to the table given for it above. If $n = 5$, then D (with D the sentence denoted by D above) is **true**, and $\neg D$ is **false**; if $n = 2$, then D is **false**, and $\neg D$ is **true**.

The connective of the conditional also corresponds to an operation in the two-element algebra **2** as follows:

$$\top \longrightarrow \top = \top, \qquad \top \longrightarrow \bot = \bot,$$

$$\bot \longrightarrow \top = \top, \qquad \bot \longrightarrow \bot = \top.$$

This table says that a conditional is **true** unless the antecedent is **true**, and the succedent is **false**. In particular, the conditional is **true** whenever the antecedent is **false**, independently of the truth-value of the succedent: "false implies everything".

We may verify that this corresponds to the usual mathematical use by considering that the sentence

$$I \stackrel{\equiv}{\text{def}} C \longrightarrow A,$$

that is,

"If n is divisible by 6, then n is divisible by 2",

should be true no matter what the value of n is. If $n = 6$, $n = 2$, $n = 1$, we obtain the sentences

"If 6 is divisible by 6, then 6 is divisible by 2",

"If 2 is divisible by 6, then 2 is divisible by 2",

"If 1 is divisible by 6, then 1 is divisible by 2".

These are of the respective forms

$$\top \longrightarrow \top, \qquad \bot \longrightarrow \top, \qquad \bot \longrightarrow \bot.$$

As said, ordinary mathematical usage attributes the value **true** to these forms, in agreement with the table for the conditional above.

The fact that a conditional is **true** once the antecedent is **false** is also reflected in the general approach to the proof of a conditional, which is that we start by *assuming* that the antecedent is **true**. In fact, we may just as well do so, since if the antecedent is **false**, the whole conditional is automatically **true**, and we can rest in our task of proving the conditional to be **true**.

The conditional can be expressed in terms of negation and disjunction:

$$x \rightarrow y = (-x) \vee y \tag{1}$$

is an identity true for any values of x and y in 2 (verify!). Thus, in principle, the conditional could be dispensed with; sentence G may be paraphrased as

"Either the greatest common divisor of n and 6 is 1, or n is divisible by 2, or n is divisible by 3."

The biconditional has the following truth-table:

$$\top \leftrightarrow \top = \top \qquad \top \leftrightarrow \bot = \bot$$

$$\bot \leftrightarrow \top = \bot \qquad \bot \leftrightarrow \bot = \bot .$$

In other words, the biconditional is **true** just in case its terms have equal truth-values. The biconditional can also be expressed in terms of previous connectives:

$$x \leftrightarrow y = (x \rightarrow y) \wedge (y \rightarrow x) \tag{2}$$

(verify!). In fact, this corresponds to our general attitude towards the proof of a biconditional, which is that it involves the proof of two conditionals.

The equalities (1), (2) may be considered as definitions of the conditional $\rightarrow$ and the biconditional $\leftrightarrow$ as operations in an arbitrary Boolean algebra. In case that algebra is $\mathcal{P}(B)$, then, for sets X and $Y \subseteq B$, we have that

$$X \rightarrow Y \underset{\text{def}}{=} (-X) \cup Y$$

and

$$X \leftrightarrow Y \underset{\text{def}}{=} ((-X) \cup Y) \cap ((-Y) \cup X) .$$

Next, we introduce a general construction on Boolean algebras.

Let $\mathfrak{A} = (A, \leq)$ be any Boolean algebra, I any set. We consider all functions from I into A as the elements of a new Boolean algebra denoted $\mathfrak{A}^I$; read " $\mathfrak{A}$-to-the-power-I ", or more simply, " $\mathfrak{A}$-to-I ". The underlying set of $\mathfrak{A}^I$ is, as we said, A^I , the set of all functions $\xi: I \to A$. The ordering in $\mathfrak{A}$, $\leq^*$, is defined *componentwise* from $\leq$: for $\xi, \zeta \in A^I$,

$$\xi \leq^* \zeta \iff \xi(i) \leq \zeta(i) \text{ for all } i \in I .$$

There are several things to check: firstly, that $\leq^*$ is indeed an order on A^I ; further, that this order has all the requisite properties to make $\mathfrak{A}^I = (A^I, \leq^*)$ a Boolean algebra. In fact, what happens is that the Boolean operations $\top^*$, $\bot^*$, $\wedge^*$, $\vee^*$, and $-^*$ in $\mathfrak{A}^I$ are all computed *componentwise*: for all $\xi, \zeta \in A^I$ and $i \in I$, we have:

$$\begin{aligned} \top^*(i) &= \top , \\ \bot^*(i) &= \bot , \\ (\xi \wedge \zeta)(i) &= \xi(i) \wedge \zeta(i) \end{aligned}$$

(we should have written $\xi \wedge^* \zeta$, but it is not necessary to be that pedantic ...).

$$\begin{aligned} (\xi \vee \zeta)(i) &= \xi(i) \vee \zeta(i) \\ (-\xi)(i) &= -(\xi(i)) \end{aligned}$$

The proof of all these assertions is easy. For instance, the assertion for $\wedge$ is that the function $\eta \in A^I$ for which $\eta(i) = \xi(i) \wedge \zeta(i)$ for all $i \in I$ is, in fact, the meet of ξ and ζ in $\mathfrak{A}^I$. According to a display on page 80 in Section 3.2, the best way to prove this is showing that

for all $\chi \in A^I$,

$$\chi \leq^* \eta \iff \chi \leq \xi \text{ and } \chi \leq \zeta .$$

When we put in the definition of η and that of $\leq^*$, we get

for all $\chi \in A^I$,
$\chi(i) \leq \xi(i) \wedge \zeta(i) \iff \chi(i) \leq \xi(i)$ and $\chi(i) \leq \zeta(i)$,

which, for each $i \in I$, is an instance of the same relation on page 80 in Section 3.2 for the original Boolean algebra $\mathfrak{A}$.

Let us apply the power-construction to the algebra $\mathfrak{A}=2$. The elements of the Boolean algebra $\mathbf{2}^I$ are the functions $I \longrightarrow 2$; for $\xi, \eta \varepsilon \mathbf{2}^I$, $\xi \leq \eta$ iff $\xi(i) \leq \eta(i)$ for all $i \varepsilon I$. Also note that since $\mathbf{2}$ has just two elements $\perp$ and $\top$, and $\perp < \top$, $\xi(i) \leq \eta(i)$ is equivalent to saying that if $\xi(i) = \top$, then $\eta(i) = \top$.

The power-algebra $\mathbf{2}^I$ is in fact a very familiar one: it is isomorphic to the power-set algebra $\mathcal{P}(I)$:

$$\mathcal{P}(I) \cong \mathbf{2}^I .$$

Let us specify the isomorphism, in fact, in both directions:

$$\mathcal{P}(I) \underset{g}{\overset{f}{\rightleftarrows}} \mathbf{2}^I \ ::$$

for $X \varepsilon \mathcal{P}(I)$, $f(X)$ is the function $I \longrightarrow \mathbf{2}$ for which

$$f(X)(u) = \begin{cases} \top & \text{if } u \varepsilon X \\ \perp & \text{if } u \notin X \end{cases}$$

and

for any function $\xi \varepsilon \mathbf{2}^I$, $g(\xi)$ is the subset of I given as

$$g(\xi) = \{u \varepsilon I \mid \xi(u) = \top\}.$$

These functions f and g respect the orders, and they are inverses of each other; these facts are easily checked (*exercises*). In other words, f is an isomorphism $f:\mathcal{P}(I) \xrightarrow{\cong} \mathbf{2}^I$. Note that, for $X \in \mathcal{P}(I)$, $f(X)$ is what we call the *characteristic function of* X.

This representation of power-set algebras provides a direct proof that

any identity that holds in the 2-element algebra $\mathbf{2}$ *holds in any power-set algebra, and hence, in any Boolean algebra whatsoever.*

The reason is that, as it is seen by inspection, an identity that holds in an algebra $\mathfrak{A}$ holds also in a power $\mathfrak{A}^I$ of it; also remember that we said in the previous section that all identities in set-algebras hold in all Boolean algebras.

Seen in the light of the last statement, the definition of "Boolean algebra" is just a summary of what identities hold in the algebra of the two truth-values!

When people talk about "Boolean functions", they mean functions of possibly several variables, all of which range over $\{\top, \bot\}$, and whose values are also in $\{\top, \bot\}$. (Very often (specially in computer science), we write 1 for $\top$, and 0 for $\bot$; but we will stick to the $\top,\bot$-notation.) If the function f in question has n variables $P_1, \ldots, P_n$ [we write P for the variables, since they are seen as "propositions"; in fact, they simply take the values $\top$ and $\top$], then f is a function

$$f : \{\top, \bot\}^n \longrightarrow \{\top, \bot\} ;$$

for any $P_1, \ldots, P_n \in \{\top, \bot\}$, $f(P_1, \ldots, P_n)$ is again an element of $\{\top, \bot\}$.

With the fixed n, note that the number of distinct n-variable Boolean functions is $2^{(2^n)}$. A Boolean function f can be represented by a *truth-table* listing all possible systems of argument-values, and the corresponding function-values. For instance, when $n=3$, the truth-table might be like this (we write P, Q, R *for* P_1, P_2, P_3):

P	Q	R	$f(P, Q, R)$
$\top$	$\top$	$\top$	$\bot$
$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$

(3)

Now, regard the set $\{\top, \bot\}$ as the underlying set of $\mathbf{2}$. Then the n-variable Boolean functions form the underlying set of the power-algebra $\mathbf{2}^I$, where $I=\{\top, \bot\}^n$. In other words, for a fixed n, the n-variable Boolean functions themselves form a Boolean algebra. Let us write $\vec{P}$ to abbreviate $P_1, \ldots, P_n$. The Boolean operations on the power-algebra $\mathbf{2}^{(\{\top, \bot\}^n)}$, *the Boolean algebra of n-variable Boolean functions*, is defined componentwise:

$$(f \wedge g)(\vec{P}) = (f(\vec{P}) \wedge g(\vec{P}),$$

and similarly for the other operations.

We write, more simply, $\mathtt{BF}[n]$ for $\mathbf{2}^{(\{\top, \bot\}^n)}$, the Boolean algebra of n-variable Boolean functions.

The most natural examples for Boolean functions are the *Boolean polynomials*: these are the functions that can be written down by repeated use of the basic Boolean operations. For instance, when $n=3$, the following are Boolean polynomials :

$$(\neg(((P \vee \neg R) \wedge (Q \vee \neg R)) \wedge \top)) \vee R$$

$$\neg(R \vee \neg Q) .$$

The fact that the last does not contain the variable P does not make it illegitimate as a three-variable polynomial: this one simply does not depend on P.

Boolean polynomials should be seen as analogs to ordinary (algebraic) polynomials. The differences are that, Boolean polynomials are functions on the truth-values, instead of numbers; and the basic Boolean operations figure in them, instead of the ordinary arithmetical operations $+$, $\cdot$, etc.

A Boolean polynomial is (or, denotes) a Boolean function: substituting definite truth-values for the variables, and using the basic Boolean operations on truth-values, we get a definite value for the polynomial. For instance, here are all the values of the first the two listed polynomials:

P	Q	R	$(\neg(((P \vee \neg R) \wedge (Q \vee \neg R)) \wedge \top)) \vee R$
$\top$	$\top$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$

Calculating the value, for instance in the third line, looks like this:

$$(\neg(((P \vee \neg R) \wedge (Q \vee \neg R)) \wedge \top)) \vee R\,.$$

$$\begin{array}{cccccccccccccccc} \bot & & \top & \top & \top & \bot & \top & & \top & \top & \top & \bot & & \top & \top & \bot & \bot \\ 7 & & & 2 & 1 & & 5 & & & 4 & 3 & & & 6 & & 8 & \end{array}$$

In this, first, we wrote the value of every variable under each occurrence of the variable, including the value $\top$ under the constant $\top$ in the polynomial; next, we proceeded to calculate the values of the part-expressions from the inside out; there are as many as there are *connectives*, occurrences of $\wedge$, $\vee$, and $-$. The numbers indicate the order in which we go through all constituent expressions until we reach the total expression in stage 8; the final result is that above 8, $\bot$.

There is a slight ambiguity in the meaning of the expression "Boolean polynomial". We sometimes mean the formal expression itself, rather than the function denoted by it. However,

the official meaning should remain the function itself; when one wants to refer to the formal notion, one should say "formal polynomial". This remark is relevant in the light of the fact that two formally different Boolean polynomials may be *equal* to each other. In the first of the last two examples, the values in the value-column coincide with the values of R; the polynomial coincides (denotes the same function as) the simple polynomial ("monomial") R.

Of course, this phenomenon is familiar in the case of ordinary (algebraic) polynomials. E.g, the two formal polynomial expressions $(x-y)\,(x+y)$ and x^2-y^2 denote the *same* polynomial. We can see this by using the basic algebraic laws. The situation with Boolean polynomials is similar. Instead of going through the tables of values (which tend to be very large even with a moderate number of variables), we may use the Boolean identities to establish that two formal Boolean polynomials are the same polynomial. For instance, in the example at hand:

$$(\neg(((P \vee \neg R) \wedge (Q \vee \neg R).) \wedge \mathsf{T})) \vee R$$

=	$(\neg(((P \wedge Q) \vee \neg R) \wedge \mathsf{T})) \vee R$	(distributive law)
=	$(\neg(((P \wedge Q) \vee \neg R)\ )) \vee R$	(unit law)
=	$(\neg(P \wedge Q) \wedge \neg\neg R)\ ) \vee R$	(De Morgan)
=	$(\neg(P \wedge Q) \wedge R)\ ) \vee R$	(double negation)
=	R	(commutative law,

absorption)

In fact, what we said about all identities of Boolean algebras being true in **2** means that every time two formal Boolean polynomials are the same function on the truth-values, this fact can be deduced by using the Boolean identities alone.

Note that the Boolean operations on the Boolean polynomials as Boolean functions are performed by formally applying the operation in question. For instance, if the three variable polynomials mentioned above are briefly called f and g, then $f \wedge g$ is

$$(((\neg(((P \vee \neg R) \wedge (Q \vee \neg R))) \wedge \mathsf{T})) \vee R) \wedge \neg(R \vee \neg Q)\ .$$

What this means is that

the Boolean polynomials form a subalgebra of $\mathtt{BF}[n]$.

Consider now the variables P_1 , P_2 , ... P_n themselves as such Boolean functions, in fact, Boolean polynomials. P_i is the function that satisfies

$$P_i(\varepsilon_1, \ldots, \varepsilon_i, \ldots, \varepsilon_n) = \varepsilon_i ;$$

here, each ε_1 , , ε_n is a truth-value, $\top$ or $\bot$. (This is similar as when the single variable say y is regarded as one of the ordinary polynomials in variables x, y, z .) We clearly have that

the particular elements P_i of $\mathtt{BF}[n]$ generate the Boolean subalgebra of Boolean polynomials.

Now, I claim that

the Boolean functions P_1 , P_2 , ... P_n *are independent in the Boolean algebra of all* n*-element Boolean functions.*

What we have to see is that, for any distribution of the values ε_1 , , ε_n in $\{\top, \bot\}$, the meet-expression

$$\varepsilon_1 P_1 \wedge \varepsilon_2 P_2 \wedge \ldots \wedge \varepsilon_n P_n$$

is *different from* $\bot$ in the Boolean algebra of Boolean functions; here, εP means P if $\varepsilon = \top$, and $-P$ if $\varepsilon = \bot$. But if we give the value ε_i to P_i , we get that $\varepsilon_i P_i$ takes the value $\top$: $(P)\,(P{=}\top) = \top$; $(-P)\,(P{=}\bot) = \top$; thus,

$$(\varepsilon_1 P_1 \wedge \varepsilon_2 P_2 \wedge \ldots \wedge \varepsilon_n P_n)\,(P_1{=}\varepsilon_1, \ldots, P_n{=}\varepsilon_n) = \top \wedge \top \wedge \ldots \wedge \top = \top .$$

Since the function takes the value $\top$ at at least one system of arguments, the function is not the $\bot$-function, which is constant $\bot$.

Remember that an independent family of n elements generate a Boolean subalgebra of size $2^{(2^n)}$. It follows that there are exactly $2^{(2^n)}$ distinct Boolean polynomials. But the

whole algebra $\mathtt{BF}[n]$ is of the same size, $2^{(2^n)}$. It follows that

all Boolean functions are (represented by) Boolean polynomials. In fact, all Boolean functions can be written as joins of complete meet expressions in terms of the variables.

The expressions P_i and $\neg P_i$ (or, $\bar{P}_i$) are also called *literals*. The expression of a Boolean function as a join of distinct complete meets of literals is called the *disjunctive normal form* (dnf) of the function. We have that every function has a unique dnf: the complete meets of literals appearing in the dnf are determined as those atoms of $\mathtt{BF}[n]$ that are below the given function.

Applying duality, one also gets a *conjunctive normal form.*

The last-stated fact has concerning the existence of the dnf also has a direct proof, together with a simple method of producing the dnf of a function, based on the truth-table of the function. The result is this. Consider the truth-table of the n-variable Boolean function f. Select those lines in the table in which the value of f is $\mathtt{T}$; say the lines in which this is the case are

$$\ell_1, \ell_2, \ldots, \ell_k .$$

Each line ℓ_j (j=1, . . ., k) has a certain system of the values of the variables. Let us denote the value of P_i in line ℓ_j by ε_{ji} (and not ε_{ij}, because j denotes the "row-number", i the "column-number"). The dnf of f is $\bigvee_{j=1}^{k} \bigwedge_{i=1}^{n} \varepsilon_{ji} P_i$; or in more detail,

$$\begin{array}{ll} & \varepsilon_{11}P_1 \wedge \varepsilon_{12}P_2 \wedge \ldots \wedge \varepsilon_{1n}P_n \\ \vee & \varepsilon_{21}P_1 \wedge \varepsilon_{22}P_2 \wedge \ldots \wedge \varepsilon_{2n}P_n \\ \vee & \ldots \\ \vee & \varepsilon_{k1}P_1 \wedge \varepsilon_{k2}P_2 \wedge \ldots \wedge \varepsilon_{kn}P_n . \end{array}$$

Here we used the convention applied before: $\mathtt{T}P$ is P, $\bot P$ is $\neg P$.

To give an example, consider the function whose truth-table is (3). There are five lines where

the value is $\top$. The dnf is

$$PQ\bar{R} \vee P\bar{Q}R \vee \bar{P}QR \vee \bar{\bar{P}}QR \vee \bar{\bar{P}}\bar{\bar{Q}}\bar{\bar{R}} \ .$$

The proof that this is a correct procedure has to show that the dnf constructed assumes the same values at each system of values for the variables. Now, the dnf is $\top$ if and only if one of its disjuncts is $\top$. But each disjunct corresponds to a line, say ℓ_j, where the value of f is $\top$. The corresponding disjunct is

$$\varepsilon_{j1}P_1 \wedge \varepsilon_{j2}P_2 \wedge \ldots \wedge \varepsilon_{jn}P_n, \tag{4}$$

and this will take the value $\top$ iff each conjunct $\varepsilon_{ji}P_i$ takes the value $\top$, which is the case if and only if P_i takes the value ε_{ji}. This means that the unique system of truth-values where the value of (4) is $\top$ is precisely the one in line ℓ_j! We have concluded that the dnf takes the value $\top$ exactly in the lines ℓ_j, for j=1,...,k, which are also exactly the lines where f is $\top$. This proves that the dnf and f are identical functions.

The dnf of a Boolean function may be extremely large already in case of a moderate number of variables. The problem of *Boolean realization* is to find a possibly small formal Boolean polynomial representing a given Boolean function.