# Problems and Comments on Boolean Algebras

# Rosen, Fifth Edition: Chapter 10; Sixth Edition: Chapter 11

## Boolean Functions

## Section 10. 1, Problems: 1, 2, 3, 4, 10, 11, 29, 36, 37 (fifth edition); Section 11.1, Problems: 1, 2, 5, 6, 12, 13, 31, 40, 41 (sixth edition)

The notation "+" for *OR* is bad and misleading. Just think that in the context of boolean functions, the author uses $+$ instead of $\vee$. The integers modulo $2$, that is $\mathbb{Z}_2 = \{0,1\}$, have an addition where $1+1=0$ while $1 \vee 1 = 1$.

A set $A$ is *partially ordered* by a binary relation $\leq$, if this relation is *reflexive,* that is $a \leq a$ holds for every element $a \in S$, it is transitive, that is if $a \leq b$ and $b \leq c$ hold for elements $a, b, c \in S$, then one also has that $a \leq c$, and $\leq$ is anti-symmetric, that is $a \leq b$ and $b \leq a$ can hold for elements $a, b \in S$ only if $a = b$.

The subsets of any set $S$ are partially ordered by set inclusion. that is the power set $(P(S), \subseteq)$ is a partially ordered set. A partial ordering on $S$ is a *total ordering* if for any two elements $a, b$ of $S$ one has that $a \leq b$ or $b \leq a$. The natural numbers $(\mathbb{N}, \leq)$ with their ordinary ordering are totally ordered.

A *bounded lattice* $L$ is a partially ordered set where every **finite subset** has a l*east upper bound* and a *greatest lower bound.* The least upper bound of the empty subset is defined as $0$, it is the smallest element of $L$. This makes sense because **any element of $L$ is an upper bound for the empty set**. If there were an element $x$ in $L$ which would not be an upper bound then we would have an element in $x \in \emptyset$ such that $not(x \leq a)$. But there is no element in $\emptyset$. Similarly, every element of $L$ is a lower bound of $\emptyset$. Thus the greatest lower bound of $\emptyset$ must be the largest element of $L$.

A *lattice* is a partially ordered set where every **two element subset** has a least upper bound and a greatest lower bound. It is then easy to see that in a lattice every **finite non-empty subset** has a least upper bound and a largest lower bound. However, there might be no smallest or largest element. Lattices which have a smallest and largest element are called *bounded*.

In a c*omplete lattice* every subset has a least upper bound and a largest lower bound. In analysis, a least upper bound is also called *supremum* and a largest lower bound *infimum.*

In a lattice, we define the least upper bound of two elements $a$ and $b$ as their *join* $\vee$ and their largest lower bound as their *meet* $\wedge$. Thus, meet and join are binary operations.

Meet and join operations are commutative and associative. By the very definition we

have that if $u \geq x$ and $u \geq y$ then $u \geq x \vee y$ because $x \vee y$ is the smallest upper bound of $x$ and $y$. Also the idempotency laws, that is $x = x \vee x = x \wedge x$ are trivial.

Important for algebra is the lattice $\mathbb{N}$ of natural numbers where $\leq \; = \; |$ indicates divisibility: $a \leq b \leftrightarrow a|b \leftrightarrow \exists k \; (k \cdot a = b)$. We have that the largest lower bound of two elements $n, m$ is the *greatest common divisor* and the *least upper bound* is the lowest common multiple:

$$n \wedge m = \gcd(n, m) \text{ and } \; n \vee m = \operatorname{lcm}(n, m)$$

Indeed, the greatest common divisor $d$ of $n$ and $m$ divides $n$ and divides $m$, $d|n$ and $d|m$. That is, $d$ is a lower bound for $n$ and $m$, and if $e$ is a lower bound for $n$ and $m$, then $e$ divides $n$ and $m$ and therefore $e$ divides $d$.

A lattice is distributive if meet distributes over join and join distributes over meet:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \text{ and } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

The lattice $(\mathbb{N}, |)$ is distributive. This is not so easy to prove.

If $X$ is any set, the powerset $P(X)$ of $X$ is the set of all subsets $A$ of $X$. It is a bounded lattice where $A \leq B$ means that $A$ is a subset of $B$, that is $A \subseteq B$. The empty set $\emptyset$ is the smallest element and $X$ is the largest element of $P(X)$. Meet is intersection and join is union. It is very easy to see that this lattice is distributive.

**Proposition** *Let D be a distributive lattice. Then one has that:*

$$a \wedge x = a \wedge y \text{ and } a \vee x = a \vee y \text{ implies that } x = y.$$

**Proof** In any lattice we have that $x = x \vee y$ holds in case that $y \leq x$. Indeed, if $u = x \vee y$, then $u \geq x$. But we also have $x \geq x$ and $x \geq y$. That is, $x \geq u$ because $u$ is the least upper bound of $x$ and $y$. That is $u = x$. Actually, we have that $x = x \vee y$ is equivalent to $x \geq y$. Similarly, $x = x \wedge y$ is equivalent to $x \leq y$.

The proof of the proposition is based on a chain of calculations. Notice that $x \leq a \vee x$.

$$x = x \wedge (a \vee x) = x \wedge (a \vee y) = (a \wedge x) \vee (x \wedge y) = (a \wedge y) \vee (x \wedge y) \leq y$$

Hence, $x \leq y$. By symmetry, $y \leq x$, thus $x = y$.

**Definition** *In a bounded lattice an element c is called a* ***complement*** *of a in case that*

$$a \wedge c = 0 \text{ and } a \vee c = 1$$

**Corollary** *Let D be a bounded distributive lattice. Then an element x can have at most one complement, called $x^*$. If x has complement $x^*$ then $x^*$ has complement x.*

**Proposition** *Let D be a bounded distributive lattice. If x has complement $x^*$ and y has complement $y^*$ then $x \wedge y$ and $x \vee y$ have complements and*

$$(x \wedge y)^* = x^* \vee y^* \text{ and } (x \vee y)^* = x^* \wedge y^*$$

*These are called the* ***De Morgan laws****.*

**Proof** $(x \wedge y) \wedge (x^* \vee y^*) = (x \wedge y \wedge x^*) \vee (x \wedge y \wedge y^*) = 0 \vee 0 = 0$ *and* $(x \wedge y) \vee (x^* \vee y^*) = (x \vee x^* \vee y^*) \wedge (y \vee x^* \vee y^*) = 1 \wedge 1 = 1$. *Thus, $x^* \vee y^*$ must be the complement of $x \wedge y$. The other law has a similar proof.*

**Definition** *A bounded distributive lattice is called a* ***boolean*** *lattice if every element has a*

*complement.*

**Remark** *$x \wedge y = 0$ iff $y \leq x^*$. That is, the complement $x^*$ of $x$ is the largest element whose meet with $x$ is zero. Similarly, if $x \vee y = 1$, then $y \geq x^*$, that is, $x^*$ is the smallest element whose join with $x$ is one.*

**Proof** *Recall that in any lattice, $x \leq y$ is equivalent to $x \wedge y = x$, as well as to $x \vee y = y$. Now, from $x \wedge y = 0$ we get $(x \wedge y) \vee y^* = 0 \vee y^* = y^*$. By distributivity this yields $(x \vee y^*) \wedge (y \vee y^*) = y^*$ which is $(x \vee y^*) \wedge 1 = y^*$, or $(x \vee y^*) = y^*$. Hence $x \leq y^*$. By symmetry of our condition $x \wedge y = 0$ we also get $y \leq x^*$. Conversely, if we have $y \leq x^*$, then $x \wedge y \leq x \wedge x^* = 0$. Thus $x \wedge y = 0$.*

A boolean lattice is also an algebra with two commutative binary operations, namely meet and join. Both have units, namely $0$ is the unit for join, $x \vee 0 = x$, and $1$ is the unit for meet, $x \wedge 1 = x$. If one stresses this algebraic structure, versus partial order, then one calls the boolean lattice a **boolean algebra**. See Definition 1 on page 707, (page 755, sixth ed.) From the algebraic structure one can discover the lattice structure by defining $x \leq y$ iff $x \wedge y = x$.

**Exercise** *Prove that for a boolean lattice one has that $x \leq y$ iff $x^* \geq y^*$.*

An algebraic structure $\mathbf{A} = (A, +, -, 0, *, 1)$ is called a *ring*, if $+$ is a binary operation on the set $A$ which is commutative and associative, $0$ is the additive unit for $+$, that is $a + 0 = a$, $-$ is a unary operation on $A$ which is inverse to $+$, that is $a + (-a) = 0$. The multiplication is associative, but not necessarily commutative, and $1$ is the unit for $*$, that is $a * 1 = 1 * a = a$. Multiplication is distributive over addition, both ways. That is $a * (b + c) = a * b + a * c, (b + c) * a = b * c + c * a$. The $n \times n$ –matrices form a classical example of a ring.

A ring is boolean if every element is idempotent, that is $a * a = a$ holds for every $a$.

**Exercise** *In a boolean ring* $\mathbf{A}$ *one has*

1. $a = -a$, *that is* $a + a = 2a = 0$.
2. $\mathbf{A}$ *is commutative.*

Hint: Calculate $(a + b)^2$ !

A boolean ring $\mathbf{A} = (A, +, -, 0, \cdot, 1)$ becomes a boolean algebra $\mathbf{B} = (A, \wedge, \vee, ^*, 0, 1)$ by defining

$$a \wedge b = a \cdot b, a \vee b = a + b + a \cdot b,\ a^* = 1 + a.$$

The $0$ of the ring $A$ serves also as the $0$ of the boolean algebra $\mathbf{B}$ and the $1$ of $\mathbf{A}$ serves as $1$ of $\mathbf{B}$.

A boolean algebra $\mathbf{B}$ becomes a boolean ring by defining

$$a \cdot b = a \wedge b,\ a + b = (a \wedge b^*) \vee (a^* \wedge b), -a = a^*$$

$0$ and $1$ of $\mathbf{B}$ serve as $0$ and $1$ of $\mathbf{A}$.

We state this just for reference. The proofs are not difficult but quite lengthy and somewhat tricky.

For us it is best to think in terms of boolean lattices.

Overbars like $\overline{x}$ are a bit cumbersome to type. They are decorations and difficult to

read. I prefer $x^*$.

It is a very important fact that the classes of logically equivalent propositional formulas form a boolean lattice **PROP**. For example, the class of all tautologies is the unit $1$, and the class of contradiction is the $0$ in that algebra.

Recall that for any set $X$, the powerset $\mathbf{P}(X)$ is the prototype of a boolean algebra. For subsets $A, B$ of $X$, the join $A \vee B$ is the union $A \cup B$, the meet $A \wedge B$ is the intersection $A \cap B$, $A^*$ is the complement $X \backslash A$, the zero $0$ is the empty set $\emptyset$, and the unit $1$ is the set $X$

It is a very remarkable fact that every **finite** boolean algebra can be identified with a powerset algebra.

**Definition** *An element a of a boolean algebra A is called an atom if* $a > 0$ *and if b is such that* $a \geq b \geq 0$ *then one has that* $b = a$ *or* $b = 0$. *In other words, an atom is a minimal element in* $A \backslash \{0\}$.

**Proposition** *Let A be a* ***finite*** *boolean algebra. Then for every element* $b > 0$ *of A one has some atom a such that* $b \geq a$.

**Proof** *If b is not already an atom, then one has some element* $b_1$ *such that* $b > b_1 > 0$. *If* $b_1$ *is an atom, we are done. Otherwise there is some* $b_2$ *such that* $b_1 > b_2 > 0$. *If* $b_2$ *is an atom, we are done. Otherwise we continue this process. Because A is finite, we must find at some point an atom a such that* $b > a$.

**Proposition** *If* $b > 0$ *is any element in the boolean algebra A and a any atom, then either* $b \geq a$ *or* $b^* \geq a$.

**Proof** *We have* $b \wedge a \leq a$. *Because a is an atom, we must have* $b \wedge a = a$ *or* $b \wedge a = 0$. *This is* $b \leq a$ *or* $b \leq a^*$.

**Proposition** *Let* $\mathbf{A}$ *be a finite boolean algebra. Then every element* $a \in \mathbf{A}$ *is the join of all atoms c where* $c \leq a$ :

$$a = \vee\{c | c \text{ an atom}, c \leq a\}$$

**Proof** *Let* $b = \vee\{c | c \text{ an atom}, c \leq a\}$. *Clearly,* $b \leq a$. *Assume* $b < a$, *then* $b^* \wedge a > 0$ *because* $b^* \wedge a = 0$ *is equivalent to* $a \leq (b^*)^* = b$. *Hence there is an atom* $c \leq b^* \wedge a$. *For this atom c we have* $c \leq a$ *as well as* $c \leq b^*$. *But for any atom* $c \leq a$ *we have* $c \leq b$. *This contradicts* $c \leq b^*$. *Thus* $b = a$.

**Theorem** *Let* $Atom(\mathbf{A})$ *be the set of all atoms of the finite boolean algebra* $\mathbf{A}$. *We can define a map* $\alpha$ *from* $\mathbf{A}$ *into the powerset of* $Atom(\mathbf{A})$*:*

$$\alpha : \mathbf{A} \to \mathbf{P}(Atom(\mathbf{A})), a \mapsto \{c | c \text{ an atom}, c \leq a\}$$

For example,

$$\alpha(0) = \emptyset, \alpha(1) = Atom(\mathbf{A})$$

But also,

$$\alpha(a \wedge b) = \alpha(a) \cap \alpha(b), \alpha(a \vee b) = \alpha(a) \cup \alpha(b), \alpha(a^*) = Atom(\alpha) \backslash \alpha(a)$$

The map $\alpha$ is bijective with inverse

$$\beta : \mathbf{P}(Atom(\mathbf{A})) \to \mathbf{A}, S \mapsto \vee\{c | c \in S\}$$

**Proof** Let $c \in \alpha(a \vee b)$, then $c$ is an atom and $c \leq a \vee b$. Thus,

$c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) = c$ where we used distributivity. Because $c$ is an atom, we have $(c \wedge a)$ is either 0 or $c$ and similarly, $(c \wedge b)$ is either 0 or $c$. But we cannot have that $(c \wedge a)$ and $(c \wedge b)$ are both 0. Thus either $(c \wedge a) = c$ or $(c \wedge b) = c$. Hence, $c \leq a$ or $c \leq b$, that is, $c \in \alpha(a)$ or $c \in \alpha(b)$. This is, $\alpha(a \vee b) \subseteq \alpha(a) \cup \alpha(b)$. Of course, an atom $c \in \alpha(a) \cup \alpha(b)$ belongs to $\alpha(a)$ or $a(b)$ and is therefore an atom $c \leq a$ or $c \leq b$ and therefore $c \leq a \vee b$. That is $c \in \alpha(a \vee b)$. This proves $\alpha(a \vee b) = \alpha(a) \cup \alpha(b)$.

$\alpha(a^*) = Atom(\alpha) \backslash \alpha(a)$ says that atoms which are not below $a$ are below $a^*$. But we have already shown this.

**Exercise** *Use $\alpha(a \vee b) = \alpha(a) \cup \alpha(b)$ and $\alpha(a^*) = Atom(\alpha) \backslash \alpha(a)$ in order to show*
$\alpha(a \wedge b) = \alpha(a) \cap \alpha(b)$

In order to show that $\alpha$ and $\beta$ are inverse to each other, let $S$ be any set of atoms and $a = \vee\{c | c \in S\}$. Of course, $S \subseteq a(a)$. Then if $d$ is any atom such that $d \leq a$, that is $d \in a(a)$, we have $d = d \wedge a = d \wedge \vee\{c | c \in S\} = \vee(d \wedge c)$ where each term $d \wedge c$ is either $d$ or 0 because $d$ is an atom. But then we must have $d \wedge c = d$ for at least one $c \in S$. But this shows $d \leq c$, and because also $c$ is an atom, $d = c$ for some $c \in S$. This is $a(\beta(S)) = S$.

According to the previous proposition, we have $a = \vee\{c | c \text{ an atom}, c \leq a\}$, that is $a = \beta(\alpha(a))$.

Thus $\alpha$ and $\beta$ are inverse of each other.

The essence of this theorem is

**Theorem** *Let* **A** *be a finite boolean algebra. Then via the map α, the algebra* **A** *can be identified with the powerset algebra* $\mathbf{P}(Atom(\mathbf{A}))$. *In particular, if* **A** *has n atoms, then* **A** *has* $2^n$ *– many elements.*

Thus finite boolean algebras are essentially powerset algebras. For infinite boolean algebras this is not the case.

**Exercise** *Let S be any infinite set. Then the sets which are either finite, or where the complement is finite, form the boolean algebra* $\mathbf{CF}(S)$ *of finite-cofinite subsets of S. For* $S = \mathbb{N}$, *this algebra is denumerable.*

Hint: That for any set $S$, $\mathbf{CF}(S)$ is a boolean algebra is straight forward and uses facts like that the union of finite sets is finite.

A set is called denumerable if it is infinite and countable, that is its elements can be listed as an infinite sequence as $s_1, s_2, \ldots$

The following indicates a listing of all finite-cofinite sets:

$\emptyset, \mathbb{N}$;

$\{0\}, \mathbb{N} \backslash \{0\}$;

$\{1\}, \{0,1\}, \mathbb{N} \backslash \{1\}, \mathbb{N} \backslash \{0,1\}$;

$\{2\}, \{0,2\}, \{1,2\}, \{0,1,2\}, \mathbb{N} \backslash \{2\}, \mathbb{N} \backslash \{0,2\}, \mathbb{N} \backslash \{1,2\}, \mathbb{N} \backslash \{0,1,2\}$

…

What is the pattern? Where would you place $\{2,5,28\}$?

It is known from set theory, that no powerset algebra can be denumerable One can show that already $P(\mathbb{N})$ is uncountable. Hence, $\mathbf{CF}(\mathbb{N})$ cannot be a powerset algebra.

## Representing Boolean Functions

## Section 10.2, Problems: 1, 3, 4, 5, 9, 10 14 (fifth edition); Section 11.2, Problems 1, 3, 4, 5, 9, 10, 14 (sixth edition)

The logical expression $p \wedge (\neg q) \wedge r$ is *true* if and only if we have that $p = T$ *and* $q = F$ *and* $r = T$. Instead of $(\neg q)$ we can also use the notation $q^*$, and if we perceive logical conjunction as multiplication, then we may drop the $\wedge$ sign. Thus for $p \wedge (\neg q) \wedge r$ we can write $pq^*r$

The two element boolean algebra $\mathbf{B} = \mathbf{B}_2$ consists only of $0$ and $1$ which act like $F$ and $T$. The expression $pq^*r$ is like a formula for a function

$$f(p,q,r) = pq^*r$$

which takes on the value $1$ if and only if $p = 1, q = 0, r = 1$. At all other values for the variables $p, q, r$ the function $f$ takes on the value $0$.

In the following, let $\mathbf{B}$ be the two element boolean algebra, $\mathbf{B}_2 = \{0,1\}$. A **boolean function** of degree $n$ is a map $F : B^n \to B$. It can be given by a table, say

| $x$ | $y$ | $F$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

This function $F$ is of degree $2$ and takes on the value $1$ if and only if for $x = 1, y = 0$ and for $x = 0, y = 1$. We obviously have that

$$F(x,y) = xy^* \vee x^*y$$

Similarly, any boolean function of degree $n$ is given by such a disjunction (the book says sum) of a conjunction (or product) of the variables $x_i$ or $x_i^*$. This is called the **sum-of-products-expansion** or **disjunctive normal form**.

The function $F^*$ has the table

| $x$ | $y$ | $F^*$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

and

$$F^*(x,y) = xy \vee x^*y^*$$

using that $(F^*)^* = F,$ we get by De Morgan's laws that

$$F(x,y) = (xy \vee x^*y^*)^* = (x^* \vee y^*)(x \vee y)$$

Here we have represented $F$ as a conjunction (product) of disjunctions (sums). This can be called a **product-of-sums-expansion** or **conjunctive normal form**.

These normal forms show that every boolean function of degree $n$ is an *algebraic term* in variables $x_1, \ldots, x_n$ using only $^*, \wedge, \vee$. Actually, every boolean function can be expressed in terms of $\wedge$ and $^*$ or in terms of $\vee$ and $^*$. This is because of:

$$a \wedge b = (a^* \vee b^*)^* \text{ and } a \vee b = (a^* \wedge b^*)^*$$

We say that $\{\wedge, \vee, ^*\}$, $\{\vee, ^*\}$, $\{\wedge, ^*\}$ are *functionally complete*. It is quite remarkable that one binary operation can express any propositional combination. The connective *Nand* stands for *not_and. It is also called the Sheffer stroke* $|$. Its truth table looks like:

| $x$ | $y$ | $\|$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

**Exercise** *Find the conjunctive and disjunctive normal form of the connective* $|$.

All propositional connectives are terms in $|$. This is Exercise 14 in the book.

The boolean functions of degree $n$ form a boolean algebra: If $F$ and $G$ are such functions, then the meet of $F$ and $G$ is the function $F \wedge G$ for which $(F \wedge G)(x_1, \ldots, x_n) = F(x_1, \ldots, x_n) \wedge G(x_1, \ldots, x_n)$, and similarly for the other boolean operations.

Now, what are the atoms $A$ of this boolean algebra? First, we must have $A > 0$. Now, $F \geq G$ iff $F(x_1, \ldots, x_n) \geq G(x_1, \ldots, x_n)$ holds for all $(x_1, \ldots, x_n) \in \mathbf{B}^n$. Thus, $A$ is an atom iff $A(x_1, \ldots, x_n) = 1$ for exactly one choice of $(x_1, \ldots, x_n) \in \mathbf{B}^n$, and $0$ elsewhere. Thus, the disjunctive normal form of an atom $A$ has exactly one term, and the disjunctive normal form of $F$ is the representation of $F$ as a join of atoms.

There are $2^n$ many atoms and the algebra of boolean functions $F$ of degree $n$ has $2^{2^n}$ –many elements. We denote this boolean algebra as $\mathbf{F}_n$ and it is also called the *free boolean algebra, freely generated by* $n$ *many elements.*

Special boolean functions of degree $n$ are the $n$ projections $P_i, i = 1, \ldots, n$. The projection $P_i$ assigns to the $n-$ tuple $(x_1, \ldots, x_n)$ the value of the $i^{th}$ coordinate. For example, in case that $n = 3$ and $i = 2$, we have that $P_2(0,0,0) = 0$ and $P_2(1,1,1) = 1$. The value of $P_2(x_1, x_2, x_3)$ is $1$ if and only if $x_2 = 1$. For the disjunctive normalform of $P_2$ we have:

$$P_2(x_1, x_2, x_3) = x_1x_2x_3 \vee x_1^*x_2x_3 \vee x_1x_2x_3^* \vee x_1^*x_2x_3^* \equiv x_2$$

If we denote the projections $P_i$ as $\mathbf{x}_i$, then we have in the algebra $\mathbf{F}_3$ of boolean functions of degree $3$ that

$$\mathbf{x}_2 = \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3 \vee \mathbf{x}_1^*\mathbf{x}_2\mathbf{x}_3 \vee \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3^* \vee \mathbf{x}_1^*\mathbf{x}_2\mathbf{x}_3^*$$

This is now an equality in the boolean algebra $\mathbf{F}_3$.
More generally, we see that in the free boolean algebra $\mathbf{F}_n$ every element $F$ admits a **unique** representation as a disjunction of a product (that is a conjunction) of the projections $\mathbf{x}_i$ and their complements.

**Definition** *A homomorphism between boolean algebras* $\mathbf{A}$ *and* $\mathbf{B}$ *is a map* $\varphi : \mathbf{A} \to \mathbf{B}$ *such that*

$$\varphi(0) = 0, \varphi(1) = 1,$$
$$\varphi(a_1 \wedge a_2) = \varphi(a_{1)} \wedge \varphi(a_2), \varphi(a_1 \vee a_2) = \varphi(a_1) \vee \varphi(a_2),$$
$$\varphi(a^*) = \varphi(a)^*$$

Now let $a_1, \ldots, a_n$ be any list of elements in a boolean algebra $\mathbf{A}$. The assignment $\mathbf{x}_i \mapsto a_i$ then can be extended to a map $\varphi : \mathbf{F}_n \to \mathbf{A}$ by replacing in the disjunctive normal form of the element $F$ each $\mathbf{x}_i$ by $a_i$ and $\mathbf{x}_i^*$ by $a_i^*$.

**Exercise** *Show that the map* $\varphi$ *is a homomorphism between the boolean algebras.*

**Hint**: If $F = s_1 \vee \ldots \vee s_k$ and $G = t_1 \vee \ldots \vee t_l$ then $F \wedge G = u_1 \wedge \ldots \wedge u_m$ where the $u_i$ are the common members in the disjunction. This is because $s_i \wedge t_j = s_i$ in case that $s_i = t_j$ or $0$ otherwise. Notice that if $s_i \neq t_j$ at least one of the $\mathbf{x}_v$ occurs in $s_i$ as $\mathbf{x}_v$ but as $\mathbf{x}_v^*$ in $t_j$, or the other way round. It is now easy to see that
$\varphi(F \wedge G) = \varphi(u_1) \wedge \ldots \wedge \varphi(u_m) = (\varphi(s_1) \vee \ldots \vee \varphi(s_k)) \wedge (\varphi(t_1) \vee \ldots \vee \varphi(t_l)) = \varphi(F) \wedge \varphi(G)$. Indeed if $s_i \neq t_j$ then $\varphi(s_i) \wedge \varphi(t_j) = 0$ because the conjunction contains one of the $a_v$ complemented as well as uncomplemented. similar arguments apply to join and complement.

**Definition** *A subset B of a boolean algebra* $\mathbf{A}$ *is called closed if it contains* $0$ *and* $1$ *and if it contains with a the complement* $a^*$ *and with a and b, also* $a \wedge b$ *and* $a \vee b$*..*

A closed subset of a boolean algebra is by itself a boolean algebra. Thus closed subsets are also called *subalgebras.* For any boolean algebra $\mathbf{A}$, the subset $\{0, 1\}$ is the smallest closed subset of $\mathbf{A}$. Somewhat more general, for any $a \in \mathbf{A}$, the subset $\{a, a^*, 0, 1\}$ is the smallest closed subset of $\mathbf{A}$ which contains $a$. For any set $S$, the algebra $\mathbf{CF}(S)$ of finite-cofinite subsets of $S$ is a subalgebra of the powerset algebra $\mathbf{P}(S)$.
For any subset *X* of a boolean algebra $\mathbf{A}$ there is a smallest closed subset which contains *X,* namely the intersection of all closed subsets which contain *X.* This is so because the intersection of closed subsets is closed and the whole algebra, which of course is a closed subset, contains *X*
The set *X* is said to *generate* the boolean algebra $\mathbf{A}$, in case that $\mathbf{A}$ is the smallest closed subset that contains *X.* Of course, $\mathbf{A}$ is trivially generated by its underlying set $A$. For any $\mathbf{A}$, the empty subset $\emptyset$ generates the smallest boolean subalgebra, namely the one consisting only of $0$ and $1$. Important is the

**Example** *In the algebra* $\mathbf{F}_n$*, the set* $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ *of the n projections generates* $\mathbf{F}_n$.

This is because every boolean function $F$ is a "boolean" combination of projections.

**Proposition** *Every finite boolean algebra* $\mathbf{A}$ *is a homomorphic image of a free boolean algebra* $\mathbf{F}_n$ *for some n.*

Assume that the boolean algebra $\mathbf{A}$ is generated by $a_1, \ldots, a_n$. Then there is a unique homomorphism from $\mathbf{F}_n$ onto $\mathbf{A}$. Thus $\mathbf{A}$ can have at most $2^{2^n}$ –many elements.

**Definition** *A bijective homomorphism is called an isomorphism.*

**Proposition** *The inverse map of a bijective homomorphism is homomorphic. One writes* $\mathbf{A} \cong \mathbf{B}$ *in case that there is an isomorphism from* $\mathbf{A}$ *to* $\mathbf{B}$.

This is an easy exercise. Isomorphic boolean algebras have the same cardinal and the same algebraic properties.

**Theorem** *Let* $\mathbf{G}$ *be a boolean algebra which is generated by n elements* $y_1, y_2, \ldots, y_n$ *such that if* $\mathbf{A}$ *is any boolean algebra and* $a_1, a_2, \ldots, a_n$ *any list of elements in* $\mathbf{A}$*, then there is a unique homomorphism form* $\mathbf{G}$ *to* $\mathbf{A}$ *such that* $y_i \mapsto a_i$. *Then* $\mathbf{G} \cong \mathbf{F}_n$.

**Proof** Because there must be a homomorphism from $\mathbf{F}_n$ onto $\mathbf{G}$ and a homomorphism from $\mathbf{G}$ onto $\mathbf{F}_n$, both algebras have the same number of elements and therefore are isomorphic. However, there is a more conceptual argument: There is a unique homomorphism $\alpha : \mathbf{F}_n \to \mathbf{G}, \mathbf{x}_i \mapsto y_i$ and a unique homomorphism $\beta : \mathbf{G} \to \mathbf{F}_n, y_i \mapsto \mathbf{x}_i$. The composition $\alpha \circ \beta$ is a homomorphism $\mathbf{G} \to \mathbf{G}, y_i \mapsto y_i$. Hence $\alpha \circ \beta$ must be the identity on $\mathbf{G}$ and similarly, $\beta \circ \alpha$ must be the identity on $\mathbf{F}_n$. Hence, $\alpha$ and $\beta$ are inverse to each other.

We have that $\mathbf{F}_n$ is the free boolean algebra, freely generated by $n$ elements. Given an infinite set $p_1, p_2, \ldots, p_n, \ldots$ of *propositional variables,* we defined *propositions* as the boolean combinations of such variables. Two such propositions are equivalent, if $p \leftrightarrow q$ is a tautology, that is its truth table is constant $1$. Equivalence classes of propositions form a boolean algebra **PROP**. From an algebraic standpoint, **PROP** is characterized as the free boolean algebra, freely generated by $p_1, p_2, \ldots, p_n, \ldots$. That is, every assignment $p_i \mapsto a_i$ of the propositional variables by elements of an arbitrary boolean algebra $\mathbf{A}$ admits a unique homomorphic extension. If $\mathbf{A}$ is the two element boolean algebra $\{T, F\}$ then a truth assignment on the variables $p_i$ leads to a truth evaluation of the propositions $p$, according to the truth tables.

**Exercise** *The algebra* **PROP** *and the algebra* $\mathbf{CF}(N)$ *of finite-cofinite sets of natural numbers are* ***not*** *isomorphic.*

**Hint**:Are there any atoms in **PRO**?

## Logic Gates

## Section 10.3 Problems: 1-5, 6, 7, 8 (fifth edition); Section 11.3 Problems 1-5, 6, 7, 8(sixth edition)

The design of certain electronic circuits is based on boolean logic. Take for example the boolean function $f(x, y, z) = xy \vee xz \vee yz$. This function takes on the value $1$ if two of the three variables are $1$. This function can be used to model majority voting amongst three individuals.

Electric circuits use as basic components **logic gates**. Any functionally complete set

suffices. Most circuits are based on the **Inverter**, **And Gate** and the **Or Gate**. The inverter has only one input arrow, And and Or gates can have any number of input arrows. All gates have one output arrow. Inputs can be outputs of other gates. Input as well as output arrows have values which are either $0$ or $1$ and are calculated according to boolean logic.

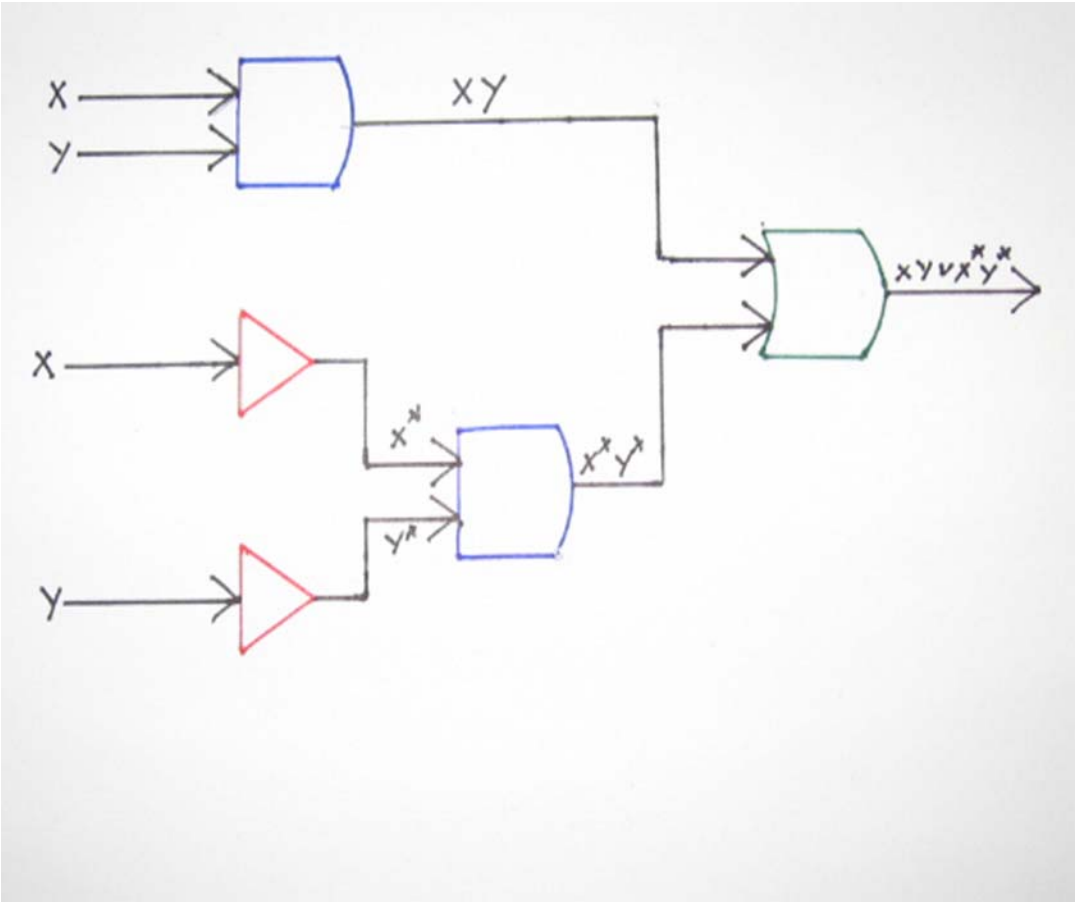
As an example consider the light in a hallway which is controlled by two light switches which can be either up or down. Any change of the position of one switch changes the state of the light which can be either on or off. The following table models the situation:

| $x$ | $y$ | $L$ |
|---|---|---|
| *down* | *up* | *off* |
| *up* | *up* | *on* |
| *up* | *down* | *off* |
| *down* | *down* | *on* |

We can arbitrarily assign boolean values to the position of the switches, say $down = 0, up = 1, off = 0, on = 1$, then $L$ is the boolean function:

| $x$ | $y$ | $L$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

which is given by the expression $L(x,y) = xy \vee x^*y^*$. The logic circuit for this function is:




Logic Gate for two switches controlling a light

Of course, finding the electric wiring for this combinatorial situation is a different matter.