7 Boolean algebra

Definition 7.1 *A Boolean algebra is a set S, containing 2 special elements the 'zero' (0) and 'unity' (1), and equipped with operations of addition (+), multiplication (∗) (both between pairs of elements) and complementation (′) (of single elements), and satisfying the following axioms.*

Commutative laws

$$x * y = y * x \quad x + y = y + x$$

Associative laws

$$x * (y * z) = (x * y) * z \quad x + (y + z) = (x + y) + z$$

Distributive laws

$$x * (y + z) = (x * y) + (x * z) \quad x + (y * z) = (x + y) * (x + z)$$

Behaviour of 1 and 0

$$x * 1 = x \quad x + 0 = x$$

Behaviour of complements

$$x * x' = 0, \quad x + x' = 1$$

The symbols we've used, i.e. $0, 1, +, *, '$, aren't a part of the definition. We could just as easily use other symbols.

NB. Maybe the associative law is a bit puzzling. What it actually tells us is that it's fine to add more than two things together, or multiply more than two things together. We interpret a sum of three things as being the sum of two of them and then the sum of that sum with the third thing. The associative law for addition tells us that, so long as we respect the order of the three things, then we can do whichever sum we like first. (And then, in fact, the commutative law tells us that the order wasn't important either.) So basically, it's fine to add any number of elements of a Boolean algebra together, or to multiply any number of elements together.

In fact we've seen examples of this situation, using other symbols, earlier in this course.

- For any set $\mathcal{U}$, the set of all subsets of $\mathcal{U}$ is a Boolean algebra, for which multiplication is given by $\cap$, addition by $\cup$, complementation by ^{c}, 1 by $\mathcal{U}$, and 0 by $\emptyset$.
- For any set (say $\{p, q, r\}$) of propositional variables, the set of all propositional formulae in these variables is a Boolean algebra, for which multiplication is given by $\wedge$, addition by $\vee$, complementation by $\neg$, the zero by FALSE and the unity by TRUE.

- The set $\{0, 1\}$ forms a Boolean algebra, in which 0 is the zero and 1 the unity when we define

$$0 + 0 = 0, 1 + 1 = 1, 0 + 1 = 1 + 0 = 1,$$
$$0 * 1 = 1 * 0 = 0 * 0 = 0, 1 * 1 = 1,$$
$$0' = 1, 1' = 0$$

  NB. Notice that $1 + 1 = 1$ NOT $1 + 1 = 0$. This all makes sense if we think of 1 as TRUE, 0 as FALSE, $+$ as 'or', $*$ as 'and', and $'$ as 'not'.

- For any of these examples (indeed for any Boolean algebra) we get a second Boolean algebra (the 'dual' of the first) by swapping the definitions of multiplication and addition, and interchanging the unity and the zero, while leaving complementation alone. This explains the duality we already observed in set theory and propositional calculus. It follows from the fact that the axioms occur in pairs.

NB. The idempotent laws, which we observed for sets and in propositional logic, aren't included in the axioms, but in fact they follow from them. i.e. we always have

$$x + x = x, \quad x * x = x$$

for any element x of a Boolean algebra.

And we can deduce the uniqueness of x' as an inverse. For given

$$x + y = 1, \quad x * y = 0$$

we have

$$y = 1*y = (x+x')*y = x*y+x'*y = 0+x'*y = x'*x+x'*y = x'*(x+y) = x'*1 = x'$$

It's useful to study Boolean algebras 'abstractly', because we have so many examples. Anything which we can observe about Boolean algebras in general can be applied to any examples we can find.

In fact any finite Boolean algebra (where finite means that S is finite) is equivalent to the following one, known as the Boolean algebra of all Boolean expressions in a finite set $X = \{a, b, c, d, \ldots\}$ of variables. So we shall simply study this one. Remember, anything we prove about this Boolean algebra can be translated into a statement about any of the examples given above.

Definition 7.2 *The Boolean algebra of all expressions in a set $X = \{a, b, c, d, \ldots\}$ of n variables is defined to be the set of all sums of products of those variables, together with 0 and 1. We use $+$ to denote addition, juxtaposition to denote multiplication, and $'$ to denote complementation, and require all the axioms for a Boolean algebra above to hold.*

Using the axioms we can tidy any element of the Boolean algebra up until it is a sum of products of distinct variables from X together with its set of complements, where no variable and its complement both appear in the same product.

Examples.

Let $X = \{a, b, c\}$,

$$\begin{aligned}(a+b')(b+c')(c+a') &= (a+b')(bc+ba'+c'c+c'a') = (a+b')(bc+a'b+a'c') \\ &= abc+aa'b+aa'c+b'bc+b'ab+b'a'c \\ &= abc+b'ac = abc+a'b'c\end{aligned}$$

$$\begin{aligned}(a+b+c)(a'+b'+c') &= a(a'+b'+c')+b(a'+b'+c')+c(a'+b'+c') \\ &= aa'+ab'+ac'+ba'+bb'+bc'+ca'+cb'+cc' \\ &= ab'+ac'+a'b+bc'+a'c+b'c \\ &= ab'+a'b+ac'+a'c+bc'+b'c\end{aligned}$$

The ordering of the terms, and within the terms, in the final expression, has been chosen for aesthetic reasons only!

7.3 *Disjunctive normal form.*

We can do something else with the second example above.

Since $ab' = ab'1 = ab'(c+c') = ab'c + ab'c'$ etc., we can rewrite the final expression as

$$ab'c+ab'c'+a'bc+a'bc'+abc'+ab'c'+a'bc+a'b'c+abc'+a'bc'+ab'c+a'b'c$$

which then simplifies (reordering, and then using the idempotent law to exclude duplicates of any term) as

$$abc'+ab'c+ab'c'+a'bc+a'bc'+a'b'c$$

This expression is of course more complicated than the final expression above. What makes it interesting is that it is a sum of terms each of which is a product involving every element of X or its complement exactly once.

The end result of the first example is already a sum of products of this type.

The products like this are called the atoms (or sometimes the minterms) of the Boolean algebra. Any element of the Boolean algebra can be written as a sum of distinct atoms in one way only. This expression for the element is known as its disjunctive normal form (or minterm normal form). It's sometimes useful to be able to put an element into this form, e.g. it allows us to see whether two elements of the Boolean algebra are the same or not.

More examples.

Let $X = \{a, b, c, d\}$ To put ab into disjunctive normal form, we write

$$ab = ab(c+c')(d+d') = abcd+abcd'+abc'd+abc'd'$$

To put $ab'+ac'$ into disjunctive normal form we write

$$\begin{aligned}ab'+ac' &= ab'(c+c')(d+d')+a(b+b')c'(d+d') \\ &= ab'cd+ab'cd'+ab'c'd+ab'c'd'+abc'd+abc'd'+ab'cd+ab'c'd' \\ &= ab'cd+ab'cd'+ab'c'd+ab'c'd'+abc'd+abc'd'\end{aligned}$$