Boolean Algebras

Definition and examples

A **Boolean algebra** (B,∨,∧,¬) is an algebra, that is, a set and a list of operations, consisting of a nonempty set B, two binary operations x∨y and x∧y, and a unary operation ¬x, satisfying the equational laws of Boolean logic.

Example 1. The algebra ({0,1},∨,∧,¬) defined by (i) $0 ∨ 0 = 0$ and otherwise $x ∨ y = 1$, (ii) $1 ∧ 1 = 1$ and otherwise $x ∧ y = 0$, and (iii) $¬0 = 1$, and $¬1 = 0$.

One of the simpler ways to define the equational laws of Boolean logic is as those equations holding identically of Example 1, where ``identically'' means ``for all values of its variables.'' For example $x = x ∨ x$ holds for all elements x of **2**, which is easily verified by trying both values of x, namely $0 ∨ 0 = 0$ and $1 ∨ 1 = 1$. On the other hand although $x = x ∨ y$ holds for three of the four possible combinations of values of x and y, it fails when $x = 0$ and $y = 1$, and so $x = x ∨ y$ is not a Boolean identity.

In this way our first example can serve not only to illustrate the concept but also to complete the definition of Boolean algebra by defining Boolean logic.

Example 2. The algebra (B,∪,∩,~) where B is a nonempty set of sets including the empty set, ∪ is union, ∩ is intersection, and for any set X in B, ~X is the *relative complement* of X, defined as the set of all elements each appearing in some element of B but not in X. An algebra of this form has been called a *field of sets* (as distinct from a number field such as the field of rationals) by G. Birkhoff, who proved that every Boolean algebra is isomorphic to a field of sets. Example 2 is therefore the most general example possible of a Boolean algebra, up to isomorphism.

When n variables occur in any such equation, there are only 2^n cases to check in order to decide if that equation is a Boolean identity. It follows that a computer can decide with 2^n evaluations of such pairs of terms whether or not an equation with n variables is a Boolean identity. Whether this can be decided much faster, specifically in time polynomial in n (e.g. $57n^{14}+13n^3+4$ steps) was famously shown by Steve Cook in 1970 to be equivalent to the question of whether P=NP, namely whether every problem solvable in nondeterministic polynomial time is also solvable in deterministic polynomial time.

The operations ∨, ∧, and ¬ and constants 0 and 1 constitute a *basis* for the set of all Boolean operations on **2**. This means that every Boolean operation can be represented by a term built up using those operations, for example the ternary operation $x ∨ (y ∧ z)$.

This would seem like a definition of ``Boolean operation'' until we notice that actually *every* finitary operation on **2** can be built in this way. For example there are 16 binary operations on **2**, all of which can be expressed with terms written using only ∨, ∧, ¬, 0, and 1. Likewise there are $2^{2^3} = 256$ ternary Boolean operations. In general there are 2^{2^n} Boolean operations of finite arity n. This gives a very simple definition of a Boolean operation, namely as any finitary operation on the two-element set {0,1}.

In a class of algebras defined as all the models of a set of equations it is usually the case that some algebras of the class satisfy more equations than just those needed to qualify them for the class. The class of Boolean algebras is unusual in that, with a single exception, every Boolean algebra satisfies exactly the Boolean identities and no more. The exception is the one-element Boolean algebra, which necessarily satisfies every equation, even $x = y$, and is therefore sometimes referred to as the inconsistent Boolean algebra.

Underlying partial order

Underlying every Boolean algebra is a partially ordered set (B,≤). The *partial order* relation is defined by $x \leq y$ just when $x = x \wedge y$, or equivalently when $y = x \vee y$. Given a set X of elements of a Boolean algebra, an upper bound on X is an element y such that for every element x of X, $x \leq y$, while a lower bound on X is an element y such that for every element x of X, $y \leq x$.

A sup (supremum) of X is a least upper bound on X, namely an upper bound on X that is less or equal to every upper bound on X. Dually an inf (infimum) of X is a greatest lower bound on X. The sup of x and y always exists, being $x \vee y$, and likewise their inf, namely $x \wedge y$. The empty sup is 0 (the bottom element) and the empty inf is 1 (top). It follows that every finite set has both a sup and an inf. Infinite sets may or may not have a sup and/or an inf.

Any partial order (B,≤) such that every pair x,y of elements has both a sup and an inf is called a *lattice*. We write $x \wedge y$ for the sup and $x \wedge y$ for the inf. The lattice is said to be *distributive* when $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, or equivalently when $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, since either law implies the other in a lattice.

Given a lattice with a bottom element 0 and a top element 1, a pair x,y of elements is called *complementary* when $x \wedge y = 0$ and $x \vee y = 1$, and we then say that y is a complement of x and vice versa. Any element x of a distributive lattice can have at most one complement. When every element of a lattice has a complement the lattice is called complemented. It follows that in a complemented distributive lattice, the complement of an element always exists and is unique, making complement a unary operation. Furthermore every complemented distributive lattice forms a Boolean algebra, and conversely every Boolean algebra forms a complemented distributive lattice. This provides an alternative definition of a Boolean algebra, namely as any complemented distributive lattice.

Boolean algebras not isomorphic to power sets

An *atom* of a Boolean algebra is an element x such that there exist exactly two elements y satisfying $y \leq x$, namely x and 0. A Boolean algebra is said to be *atomic* when every element is a sup of some set of atoms (the bottom element is always the empty sup).

Every finite Boolean algebra is atomic, and moreover isomorphic to the power set 2^X of the set X of its atoms, under the operations of union, intersection, and complement, with 0 and 1 realized by respectively the empty set and X. Conversely every finite power set forms a Boolean algebra under union, intersection, and complement.

This converse can be strengthened by dropping ``finite.'' However the converse of this strengthening does not hold: there exist Boolean algebras that are not isomorphic to any power set under union and intersection. The smallest infinite power set is 2^N where N is the set of natural numbers, which Cantor showed to be uncountable. There do however exist countably infinite Boolean algebras, two examples of which we now give.

1. Finite and confinite sets of integers. A cofinite set of integers is one that omits only finitely many integers. The finite sets are clearly closed under finite union and finite intersection, and likewise the cofinite sets are so closed. The complement (with respect to the set of all integers) of a finite set is cofinite and vice versa. The union of a finite set with a cofinite set is cofinite, while their intersection is finite. Hence this set of sets of integers is closed under all the Boolean operations. These operations furthermore satisfy all the Boolean identities. Hence this set of sets forms a field of sets in the above sense of Birkhoff and hence a Boolean algebra. It is atomic (the atoms are the singletons or one-element sets, and every set is the sup of its elements in this algebra) but not complete (any set X of atoms has a sup if and only if the union of X is either finite or cofinite, so in particular the set of even atoms has no sup).

2. The free Boolean algebra on countably many generators. Given countably many variables $v_0, v_1, v_2, \ldots$, this is the set of all abstract terms that can be built up from these variables using the operations $x \wedge y$, $x \vee y$, $\neg x$, and the constants 0 and 1. Any such term will be finite and so use only finitely many variables. Terms are *abstract* in the sense that two terms that always have the same value in **2** are considered to be the same term, e.g. $x \wedge y$ and $y \wedge x$. Without the abstractness requirement, $x \wedge y$ and $y \wedge x$ would be distinct terms whence they

would violate the Boolean identity $x \wedge y = y \wedge x$ when built up from x and y. The abstractness condition ensures that the Boolean identities are always satisfied.

The free countable Boolean algebra is atomless. In particular, for any x there is always a smaller nonzero element, namely $x \wedge v_i$ where v_i is any variable not appearing in the term x. Surprisingly it can be shown that every countable atomless Boolean algebra is isomorphic to the free countable Boolean algebra. Furthermore this algebra is not complete, for example any set X of variables has a sup if and only if the set is finite.

The free Boolean algebra on n generators, n finite, has 2^{2^n} elements. These are the semantically distinct terms that can be built using n variables. When n = 2 this algebra has 16 elements, namely the 16 binary Boolean operations. Because finitely generated Boolean algebras are finite, the class of Boolean algebras is said to be *locally finite*. (Contrast this with finitely generated monoids, e.g. the set of all words on a 2-letter alphabet; the class of monoids is therefore not locally finite.)

Boolean homomorphisms

Just as groups have homomorphisms between them, so do Boolean algebras. A Boolean homomorphism is a function h from one Boolean algebra $(B, \vee, \wedge, \neg, 0, 1)$ to another $(B', \vee', \wedge', \neg', 0', 1')$, such that h(0) = 0', h(1) = 1', $h(x \vee y) = h(x) \vee' h(y)$, and $h(x \wedge y) = h(x) \wedge' h(y)$. From this it follows that $h(\neg x) = \neg' h(x)$ (hint: use $x \wedge \neg x = 0$ and $x \vee \neg x = 1$, along with the uniquess of a solution in y to $x \vee y = 1$, $x \wedge y = 0$).

The category **Bool** of Boolean algebras has as objects all Boolean algebras and as morphisms the homomorphisms between them.

There exists a unique homomorphism from **2** to every Boolean algebra, since any homomorphism must carry bottom to bottem and top to top. A Boolean algebra with this property is called an *initial* Boolean algebra. It can be shown that any two initial Boolean algebras are isomorphic, whence we say *the* initial Boolean algebra.

In the other direction, there may exist many homomorphisms from a Boolean algebra B to **2**. Any such homomorphism partitions B into those elements mapped to 1 and those to 0. The subset of B consisting of the former is called an *ultrafilter* of B. When B is finite its ultrafilters pair up with its atoms; one atom is mapped to 1 and the rest to 0. Each ultrafilter of B thus consists of an atom of B and all the elements above it; hence exactly half the elements of B are in the ultrafilter.

For infinite Boolean algebras the notion of ultrafilter becomes considerably more delicate. One simpleminded ultrafilter of the Boolean algebra of finite and cofinite sets of integers is the set of cofinite integers, but there are many more. Likewise the powerset of the integers has among its ultrafilters the set of all subsets containing a given integer; there are countably many of these "standard" ultrafilters, which may be identified with the integers themselves, but there are uncountably many more "nonstandard" ultrafilters. These form the basis for nonstandard mathematics, providing representations for such classically inconsistent objects as infinitesimals and delta functions.

Complete Boolean algebras

Recall the definition of sup and inf from the section above on the underlying partial order of a Boolean algebra. A *complete* Boolean algebra is one every subset of which has both a sup and an inf.

A complete homomorphism is one that preserves all sups that exist, not just the finite sups, and likewise for infs. A complete atomic Boolean algebra, or CABA, is a Boolean algebra that is atomic and has all sups and infs. The category CABA of all CABAs and their complete homomorphisms is dual to the category of sets and their functions, meaning that it is equivalent to the opposite of that category (the *abstract* category resulting from reversing all morphisms). However the category Bool of Boolean algebras and their homomorphisms is dual to the category of totally disconnected compact Hausdorff spaces, or Stone spaces.

Gaifman and Hales independently showed in 1964 that free complete Boolean algebras did not exist. This suggests that it is impossible to have an infinitary Boolean logic for lack of terms. However free CABAs (complete atomic Boolean algebras) *do* exist for all cardinalities of a set V of generators, namely the power set algebra 2^{2^V}, this being the obvious generalization of the finite free Boolean algebras.

The nonexistence of complete Boolean algebras can be traced to failure to extend the equations of Boolean logic suitably to all laws that should hold for infinitary conjunction and disjunction, in particular the neglect of distributivity in the definition of complete Boolean algebra. A complete Boolean algebra is called *completely distributive* when arbitrary conjunctions distribute over arbitrary disjunctions and vice versa. A complete and completely distributive Boolean algebra is isomorphic to a CABA, whence there do exist free complete and completely distributive Boolean algebras. This neatly rescues infinitary Boolean logic from the fate the Gaifman-Hales result seemed to consign it to.

Other definitions of Boolean algebra

There are many other definitions of a Boolean algebra besides the ones already encountered. We list four of the more important here. As it would take us too far afield to develop the necessary background for each, we leave a fuller understanding of these as a project to pursue with the help of a suitable search engine.

(Stone) A Boolean algebra is a ring satisfying $x^2 = x$. A ring satisfying this condition is called a Boolean ring, whence a Boolean algebra is a Boolean ring, with the ring multiplication as conjunction and the ring addition as XOR (exclusive-or) or $\oplus$, definable as $x \oplus y = (x \wedge \neg y) \vee (\neg x \wedge y)$, which in the two-element Boolean algebra can be defined as the truth value of $x \neq y$, and which can also be viewed as addition mod 2. Those who are picky about the impact of change of base will argue that a Boolean ring is not itself a Boolean algebra, while acknowledging however that the category of Boolean rings is equivalent to the category of Boolean algebras. Others will argue that the choice of basis should be irrelevant to the concept of Boolean algebra, and that one should compare algebras on the strength of all the operations obtained by composition (called a *clone* for ``closed nest of operations") and not just the basis. From that perspective Boolean rings and Boolean algebras have exactly the same operations in their respective clones, namely all the Boolean operations.

(Lawvere) A Boolean algebra is a product-preserving set-valued functor F:C→Set from the category C of finite power sets and *all* functions between them. Because it preserves products, any such functor is determined by the set F(2) to which F maps the two-element power set 2. This set then serves as the underlying set of the Boolean algebra represented by this functor. The functor then interprets the functions from the finite power sets to the two-element power set as the Boolean operations on F(2). All other functions between finite power sets are then interpreted as tuples of Boolean operations on F(2).

(Stone) A Boolean algebra is the set of all continuous functions from a totally disconnected compact Hausdorff space, or Stone space, to the Sierpinski space (the two-element topological space with three open sets). This is just the reverse direction of the duality mentioned earlier from Boolean algebras to Stone spaces.

(Johnstone) A Boolean algebra is an object of the ind-completion of the category of finite Boolean algebras, aka finite power sets and all meet- and join-preserving functions between them. In this definition Boolean algebras arise as colimits of diagrams of finite Boolean algebras.