Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Lecture 7: Boolean and Abstract Algebra
Winter 2019

1 Boolean Algebras

Recall from your study of set theory in CISC 102 that a **set** is a collection of items that are related in some way by a common property or rule. There are a number of operations that can be applied to sets, like $\cup$, $\cap$, and $^{\mathsf{C}}$. Combining these operations in a certain way allows us to develop a number of identities or laws relating to sets, and this is known as the algebra of sets.

In a classical logic course, the first thing you typically learn about is **propositional calculus**, which is the branch of logic that studies propositions and connectives between propositions. For instance, "all men are mortal" and "Socrates is a man" are propositions, and using propositional calculus, we may conclude that "Socrates is mortal". In a sense, propositional calculus is very closely related to set theory, in that propositional calculus is the study of the set of propositions together with connective operations on propositions. Moreover, we can use combinations of connective operations to develop the laws of propositional calculus as well as a collection of rules of inference, which gives us even more power to manipulate propositions.

Before we continue, it is worth noting that the operations mentioned previously—and indeed, most of the operations we have been using throughout these notes—have a special name. Operations like $\cup$ and $\cap$ apply to pairs of sets in the same way that $+$ and $\times$ apply to pairs of numbers. A general operation $\star$ that applies to pairs of things is called a **binary operation**, and it is really no more than a simple function.

Definition 1 (Binary operation)**.** A binary operation $\star$ on a set A is a function $\star : A \times A \to A$.

In the same sense, a **unary operation** is a function from a set to itself.

Now, recalling our interesting connection between two foundational areas of mathematics, we might ask ourselves what the common link is between sets and logic. More specifically, what are the core aspects of both areas that relate the two? Clearly, both areas deal with sets, both areas have operations that can be applied to sets, and both areas combine operations in such a way as to develop laws that govern their use.

If we distill all three of these traits down to their simplest forms, we get what is known as a **Boolean algebra**. Boolean algebras were first introduced by the English mathematician George Boole in the mid-1800s in two now-classic books, *The Mathematical Analysis of Logic* and *The Laws of Thought*.

Definition 2 (Boolean algebra)**.** A Boolean algebra is a set B together with two binary operations $*$ and $+$, a unary operation $^-$, and elements $\mathsf{0}$ and $\mathsf{1}$ such that, for all $x, y, z \in B$, the following properties hold:

1. Identity laws: $x * \mathsf{0} = x$ and $x + \mathsf{1} = x$.
2. Complement laws: $x * \overline{x} = \mathsf{1}$ and $x + \overline{x} = \mathsf{0}$.
3. Commutative laws: $x * y = y * x$ and $x + y = y + x$.
4. Associative laws: $x * (y * z) = (x * y) * z$ and $x + (y + z) = (x + y) + z$.
5. Distributive laws: $x * (y + z) = (x * y) + (x * z)$ and $x + (y * z) = (x + y) * (x + z)$.

We often informally refer to the operation $*$ as "or", $+$ as "and", and $^-$ as "not". Note that, in this context, the symbols $*$ and $+$ do not refer to the usual multiplication and addition operations!

The elements $\mathsf{0}$ and $\mathsf{1}$ are sometimes referred to as the "bottom" and "top" elements, respectively. They can be thought of as the least and greatest elements under consideration in a Boolean algebra.

Although the five properties listed in Definition 2 are all that are required for a set to be a Boolean algebra, we can use the same properties to derive further properties of Boolean algebras. Just like with the algebra of sets, we can prove that Boolean algebras have their own versions of the idempotent law, null law, involution law, and absorption law. We can even prove that De Morgan's laws hold for Boolean algebras.

Notice that we have been consistent in using the indefinite article when referring to Boolean algebras: we say "*a* Boolean algebra" and not "*the* Boolean algebra". This is because many Boolean algebras exist, and we can create new Boolean algebras as long as we choose a set and operations that abide by the properties listed in Definition 2. We have already seen two examples of Boolean algebras: sets and propositional calculus.

- Sets are Boolean algebras because we can take $B = \{\text{elements of a given set}\}$, $* = \cup$, $+ = \cap$, $^- = {}^{\mathsf{C}}$, $\mathsf{0} = \emptyset$, and $\mathsf{1} = \mathcal{U}$.
- Propositional calculus is a Boolean algebra because we can take $B = \{\text{propositions}\}$, $* = \vee$, $+ = \wedge$, $^- = \neg$, $\mathsf{0} = \mathsf{F}$, and $\mathsf{1} = \mathsf{T}$.

Let's take a look at a few more examples.

Example 3. The simplest example of a Boolean algebra consists of the set $B = \{0, 1\}$ together with the operations $*$, $+$, and $^-$, where each operation is defined as follows:

x	y	$x * y$
0	0	0
0	1	1
1	0	1
1	1	1

x	y	$x + y$
0	0	0
0	1	0
1	0	0
1	1	1

x	$\overline{x}$
0	1
1	0

Each of the above tables are known as **truth tables**. The two-element Boolean algebra has particular applications in logic and electrical engineering, so it is usually the most familiar example to computer scientists.

Example 4. Given a set A, let $\mathcal{P}(A)$ denote the power set of A. The set $B = \mathcal{P}(A)$ together with the operations $* = \cup$, $+ = \cap$, and $^- = {}^{\mathsf{C}}$ and the elements $\mathsf{0} = \emptyset$ and $\mathsf{1} = A$ form a Boolean algebra.

Example 5. Given a squarefree natural number n, let

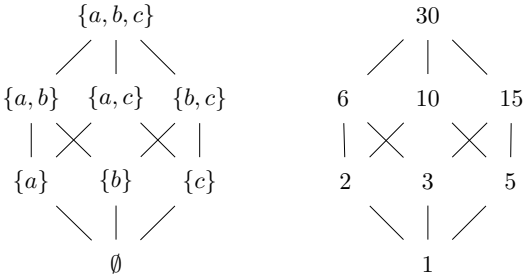
$$B = \{\text{set of positive divisors of } n \mid a \sqsubseteq b \text{ if } a \text{ divides } b \text{ for } 1 \leq a, b \leq n\}.$$

Then the partially-ordered set $(B, \sqsubseteq)$ together with the operations $* = \operatorname{lcm}(a, b)$, $+ = \gcd(a, b)$, and $^- = n/a$ and the elements $\mathsf{0} = 1$ (that is, the number one) and $\mathsf{1} = n$ form a Boolean algebra.

Remark. In Example 5, we defined n to be a **squarefree** natural number. This means that n is not divisible by any square natural number greater than 1. To see why we require n to be squarefree in order to have a Boolean algebra, consider what would happen if n were not squarefree; say, if $n = 20$. Then, for instance, we would have $10 + \overline{10} = \gcd(10, (20/10)) = \gcd(10, 2) = 2$, which contradicts the complement law of a Boolean algebra.

To help with identifying the underlying structure of a Boolean algebra, we may draw it as a graph where (roughly speaking) following two edges "upward" from distinct vertices in the graph denotes an application of the $*$ operation and following two edges "downward" from distinct vertices in the graph denotes an application of the $+$ operation. Moreover, the "lowermost" and "uppermost" vertices of the graph are the bottom element $\mathsf{0}$ and the top element $\mathsf{1}$, respectively. Such graphs are called **lattices**.

In what follows, the Boolean algebras corresponding to the elements of the power set $\mathcal{P}(\{a, b, c\})$ (from Example 4) and the positive divisors of the number $n = 30$ (from Example 5) are drawn as lattices.



2 Abstract Algebra

Studying Boolean algebras and their applications to various areas of computer science and mathematics serves as great motivation for the topic of this section. (Of course, given that the topic at hand has the word "abstract" in its name, any sort of motivation is great.) By now, we have become familiar with concepts like sets, binary operations, associativity, and commutativity. Keep these concepts in mind as we go forward.

Abstract algebra is the study of algebraic structures. An algebraic structure is a set together with a collection of operations on that set. Naturally, with such a vague description, we can come up with all manner of algebraic structures. Indeed, we have already seen one example: Boolean algebras, which are formally known as "lattice structures" due to the fact that we can draw a Boolean algebra as a lattice.

Typically, we classify algebraic structures based on the number of binary operations included in the structure. (There are other metrics for classifying algebraic structures, but here we will focus on binary operations). A set by itself, therefore, is a degenerate algebraic structure with zero binary operations.

When we add one binary operation to a set, then we begin to discover some interesting algebraic structures. We can sub-classify the structures with one binary operation based on the properties of the operation and the elements in the set.

- A set S with a binary operation $\star$ is called a **magma**.
- A set S with an *associative* binary operation $\star$ is called a **semigroup**.
- A set S with an associative binary operation $\star$ and an *identity element* is called a **monoid**.

Identity elements are similar to the `NOP` instruction in an assembly language, in that they do nothing to change elements in the set. For instance, adding 0 to a number does nothing just as multiplying a number by 1 does nothing.

Although magmas aren't very interesting on their own, semigroups and monoids appear commonly in mathematics and computer science. For instance, in formal language theory, the set of nonzero-length binary strings together with the concatenation operation is a semigroup and the set of all binary strings of length zero or greater with the concatenation operation is a monoid.

2.1 Groups

To define the main algebraic structure of interest in this section, called a **group**, we must add one more property to our list. This additional property essentially ensures that we can "undo" actions performed on the set.

Definition 6 (Group)**.** A group $(S, \star)$ is a set S together with a binary operation $\star$ that satisfies the following properties:

1. Closure: for all $a, b \in S$, $a \star b \in S$;
2. Associativity: for all $a, b, c \in S$, $(a \star b) \star c = a \star (b \star c)$;

3. Identity: there exists an identity element $e \in S$ such that, for all $a \in S$, $a \star e = e \star a = a$; and
4. Inverse: for all $a \in S$, there exists an inverse element $a^{-1} \in S$ such that $a \star a^{-1} = a^{-1} \star a = e$.

Example 7. Consider the set $\mathbb{Z}_3 = \{0, 1, 2\}$ together with the operation of addition modulo 3, $\oplus_3$. We can represent this operation in a **Cayley table** as follows:

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The pair $(\mathbb{Z}_3, \oplus_3)$ is a group. We prove this fact informally (but we will soon see a more formal way to prove that something is a group). Closure holds, since every entry in the Cayley table comes from the set $\mathbb{Z}_3$. Associativity holds by a property of addition. The element 0 is the identity element, and each element of $\mathbb{Z}_3$ has an inverse corresponding to the element that produces 0 in the Cayley table.

The **order** of a group is equal to the number of elements in the group's set S. If the order of a group is finite, then we say that the group itself is **finite**. The classification of so-called "finite simple groups" is an active and important area of research in group theory, and the advent of computer-aided proof systems has helped greatly to verify lengthy results in this area.

Note that, in the first property of Definition 6, we do not require that both $a \star b$ and $b \star a$ belong to S for all $a, b \in S$. Indeed, we may define sets and binary operations where $a \star b$ maintains closure and $b \star a$ does not. In the special case where $a \star b = b \star a$—that is, when the binary operation $\star$ is commutative—we give its corresponding group a special name.

Definition 8 (Abelian group)**.** A group $(S, \star)$ is an Abelian group if $\star$ is a commutative binary operation; that is, for all $a, b \in S$, $a \star b = b \star a$.

Abelian groups were named after the Norwegian mathematician Niels Henrik Abel, despite the fact that group theory was not a formal area of study during Abel's lifetime. Abel used concepts related to what would later be called commutative groups in his famous proof that there exists no algebraic solution to general polynomials of degree 5 or greater.

Remark. Abelian groups should not be confused with objects that are purple and commute. Those objects are called Abelian grapes.

Just like Boolean algebras and monoids, groups include certain special elements: identity elements and inverse elements. The wording of Definition 6 suggests that there exists only one identity element in a group, while there exists one inverse element for each element in the group's set. Here, we prove these claims formally.

Theorem 9. *Given a group $(S, \star)$, the set S contains exactly one identity element.*

Proof. Suppose that S contains more than one identity element. Take two distinct identity elements $e, e' \in S$ and apply the binary operation $\star$ to these elements. Since e is an identity element, $e \star e' = e'$. Similarly, since e' is an identity element, $e \star e' = e$. Thus, we conclude that $e = e'$, showing that the two identity elements assumed to be distinct are, in fact, equal. □

Theorem 10. *Given a group $(S, \star)$, every element in the set S has exactly one inverse in S.*

Proof. Suppose that some element $a \in S$ has more than one inverse. Take two distinct inverse elements $x, y \in S$. Then

$$a \star x = x \star a = e \text{ and } a \star y = y \star a = e,$$

where $e \in S$ is the identity element. By the associative property of groups, we have

$$x \star (a \star y) = (x \star a) \star y.$$

However, since both $a \star y = e$ and $x \star a = e$, the above equation gives

$$x \star e = e \star y$$
$$x = y.$$

Thus, we conclude that the two inverse elements assumed to be distinct are, in fact, equal. □

Now that we've defined and proved some properties of groups, let's take a look at a few more examples of groups. The first example we will see is the canonical example of a group, and we will even prove this fact to illustrate the formal process of showing that something is a group.

Theorem 11. *The set of integers with addition, $(\mathbb{Z}, +)$, is a group.*

Proof. To show that $(\mathbb{Z}, +)$ is a group, we must show that it satisfies the four properties set out in Definition 6.

1. Closure: Given any two integers $a, b \in \mathbb{Z}$, their sum $a + b$ is also an integer.
2. Associativity: Given any three integers $a, b, c \in \mathbb{Z}$, adding c to the sum $a + b$ gives the same result as adding a to the sum $b + c$, so $(a + b) + c = a + b + c = a + (b + c)$.
3. Identity: The integer $0 \in \mathbb{Z}$ is the identity element since $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$.
4. Inverse: Given an integer $a \in \mathbb{Z}$, the integer $-a \in \mathbb{Z}$ is the inverse element of a, since $a + (-a) = -a + a = 0$. If $a = 0$, then $a^{-1} = 0$, making the identity element its own inverse.

Since all four properties are satisfied, we conclude that $(\mathbb{Z}, +)$ is a group. □

In general, we may prove that any set and binary operation is a group by showing that such a pair satisfies the four properties of a group. For the remaining examples, we will not prove that each pair is a group explicitly, but it is a good exercise to attempt each proof on your own.

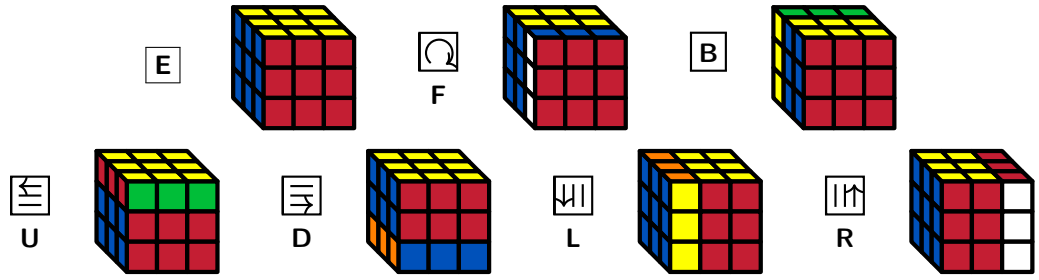
Example 12. The following pairs of sets and binary operations are groups:

- the set of rational numbers with addition, $(\mathbb{Q}, +)$;
- the set of real numbers with addition, $(\mathbb{R}, +)$;
- the set of integers modulo n with addition modulo n, $(\mathbb{Z}_n, \oplus_n)$;
- the Klein four-group K_4, consisting of a set of pairs $S = \{(0,0), (0,1), (1,0), (1,1)\}$ and a binary operation $*$ defined by $(a, b) * (c, d) = (a \oplus_2 c, b \oplus_2 d)$, where $\oplus_2$ is addition modulo 2;

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

- the dihedral group D_{2n}, consisting of symmetries of an n-sided polygon with compositions of rotation/reflection operations;

- the symmetric group S_n, consisting of bijections from an n-element set A to itself with the function composition operation;
- The Rubik's cube group, closely related to the symmetric group S_{48}, with compositions of clockwise/counterclockwise face move operations.



Given all of these examples of things that *are* groups, what are some examples of things that *are not* groups? Fortunately, coming up with examples for the negative case is just as straightforward as for the positive case.

Even though each of $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are groups, the pair $(\mathbb{N}, +)$ is not a group. This is because no element in $\mathbb{N}$ has an inverse, since every element of $\mathbb{N}$ is either zero or positive. In other words, we cannot "undo" the addition of two natural numbers.

Keeping with the sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, if we replace the operation of addition with the operation of multiplication, then we again do not have a group. For instance, the pair $(\mathbb{Z}, \times)$ is not a group because the element $0 \in \mathbb{Z}$ has no inverse. The same reasoning applies for the sets $\mathbb{Q}$ and $\mathbb{R}$.

However, if we remove the troublesome element 0—to get the sets $\mathbb{Z} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$, and $\mathbb{R} \setminus \{0\}$, respectively—then we indeed have a group with the multiplication operation.

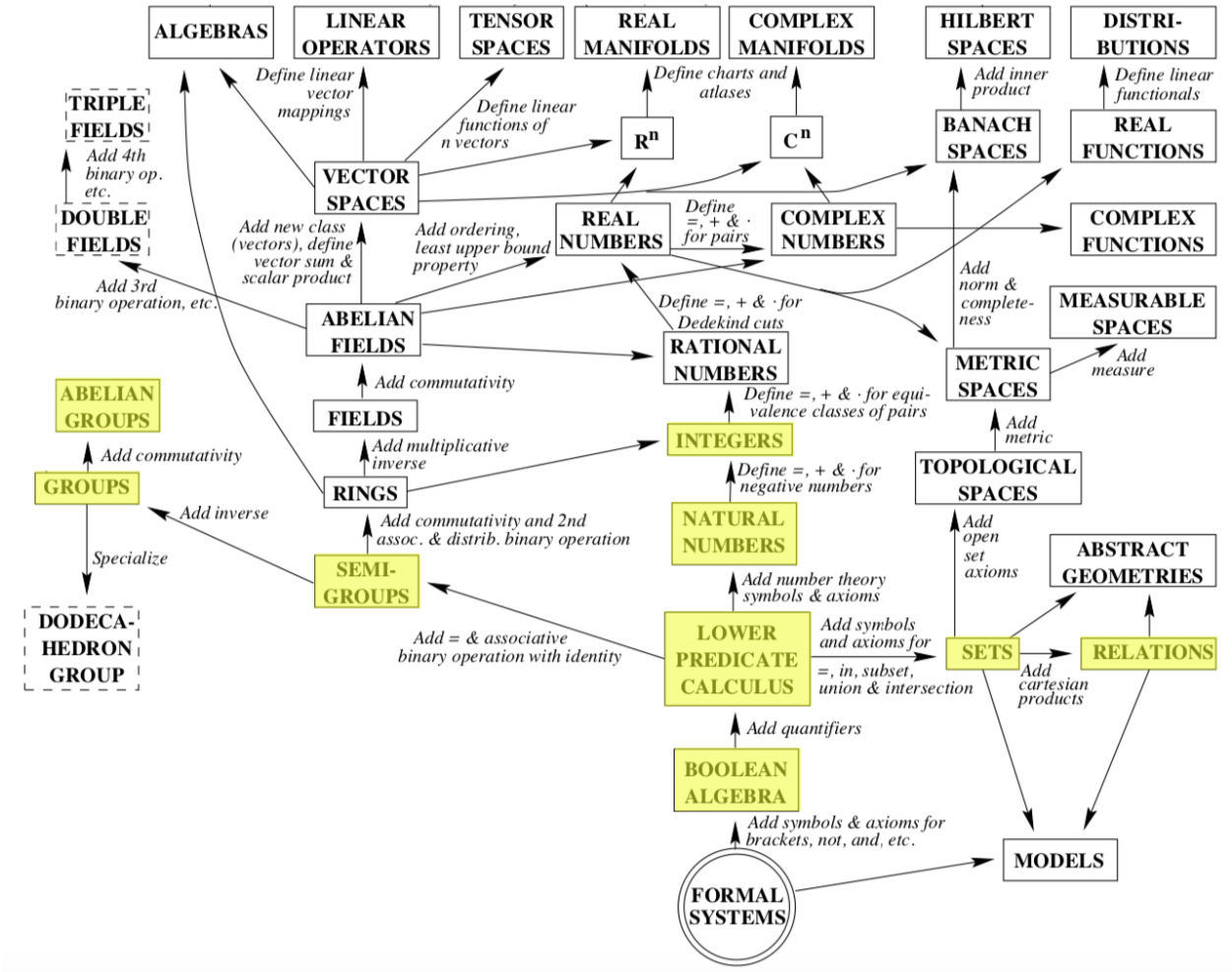
2.2 Beyond Groups

In these notes, we have seen groups (sets with one binary operation) and Boolean algebras (sets with two binary operations and one unary operation). Unfortunately, we don't have the time in this course to investigate what lies between or beyond these two algebraic structures. To summarize the depth of group theory, however, here is a brief overview of other common algebraic structures.

- If we add a second associative operation, $\bullet$, to an Abelian group, and if the second operation $\bullet$ distributes over the first operation $\star$, then we get a **ring**. Informally speaking, rings allow us to perform "addition" and "multiplication" on a set.
- If the second operation of a ring is commutative, then we get an **Abelian ring**.
- If we include multiplicative inverses for every nonzero element in an Abelian ring, then we get a **field**. Informally speaking, fields allow us to perform "addition", "subtraction", "multiplication", and "division" on a set.
- If we combine an Abelian group and a ring, then we get a **module**.
- If we combine an Abelian group and a field, then we get a **vector space**.
- If we combine a module and a ring, then we get an **algebra**.
- If we take an infinite set together with two binary operations, a unary "successor" operation, and a special element 0, then we get an **arithmetic**.

As we go higher and higher in this hierarchy, the structures become more abstract and the number of applications become smaller. Usually, each of the above topics are covered in a course devoted to group theory, such as MATH 210, MATH 310, and MATH 414. If this topic interests you, you might wish to expand your horizons by taking such a course; a little more mathematics never hurt anyone.

For the bird's-eye view of where our course fits into the grand scheme of computing and mathematics, the following diagram (adapted from a figure in a paper by Max Tegmark[1]) illustrates connections between many areas of mathematics. The concepts that we studied in this course and some concepts that you may have studied in other computing or mathematics courses are highlighted in yellow. Many of the non-highlighted concepts are covered in higher-level mathematics courses, though even concepts listed at the highest level of the chart do not constitute the apex of mathematics. If you enjoyed what you learned in this course, consider taking other courses to learn about the other concepts in this chart. You won't regret it!



[1]Max Tegmark. Is "the theory of everything" merely the ultimate ensemble theory?. *Annals of Physics*, 270(1):1–51, 1998.