

# CM10196

## Topic 2: Sets, Predicates, Boolean algebras

Guy McCusker

1W2.1

### Sets

Most of the things mathematicians talk about are built out of *sets*.

The idea of a set is a simple one: a set is just a collection of things that we can talk about together.

Examples include:

- ▶ the set of all students in a class
- ▶ the set of all cows in farms in the UK
- ▶ the set of all cows in farms in the UK which are infected with foot-and-mouth disease (this one is a *subset* of the previous one)
- ▶ the set of *natural numbers*  $0, 1, 2, \dots$
- ▶ the set of *integers*  $\dots, -2, -1, 0, 1, 2, \dots$

### Sets

A set is determined completely by its elements: all that matters is whether an element is in a set or not.

A set doesn't keep its elements in any particular order, and an element cannot appear more than once in a set.

For small, finite sets, it is common to describe a set by listing its elements, surrounded by braces (curly brackets), like this:

$$S = \{a, b, c, d, e, f, g\}.$$

We could also have written  $\{g, f, e, d, c, b, a\}$  and we'd have described the same set.

## Some notation

If an element  $a$  belongs to a set  $S$ , we say  $a$  is a *member of* or *element of*  $S$ , and write  $a \in S$ .

If  $a$  is not an element of  $S$  we write  $a \notin S$ .

There's a special set called the *empty set* which has no elements. It is written  $\emptyset$ .

## Set theory and the foundations of mathematics

Some mathematicians would like to build the whole of mathematics out of a simple, agreed collection of basic ideas and structures.

Set theory is the most commonly used starting point for this task, which is called *foundations of mathematics*.

It is far from simple. Around 100 years ago, Frege believed he had a solid foundation for mathematics based on his theory of sets, until Russell showed that his theory is inconsistent via *Russell's Paradox*.

The best way to provide foundations for mathematics is still under vigorous debate.

## Russell's Paradox

Russell's paradox concerns the important question: what kinds of collections can we reasonably say are sets.

It is vital in mathematics to allow some sets to contain other sets. For instance, let's say that a set of natural numbers is an *initial segment* if it is of the form

$$\{0, 1, \dots, n\}$$

for some  $n$ . Then we could form the set of all initial segments:

$$\{\emptyset, \{0\}, \{0, 1\}, \{0, 1, 2\} \dots\}$$

## Russell's Paradox

If we can form sets of sets, presumably some sets will be able to contain themselves as elements.

This isn't crazy: compare it with the idea of a web-page which lists all web pages related to Python programming. This page is clearly related to Python programming, so it should list itself.

So:

- ▶ Sets can contain other sets as elements
- ▶ Some sets can contain themselves.

## Russell's Paradox

Let  $U$  be the set of all sets which do not contain themselves. That is, a set  $S$  is an element of  $U$  if  $S \notin S$ . If  $S \in S$ , then  $S$  is not an element of  $U$ .

Is  $U \in U$ ?

## Russell's Paradox

Either  $U \in U$  or  $U \notin U$ . (Remember the law of excluded middle:  $X \vee \neg X$ .)

If  $U \in U$ , then by the definition of  $U$ ,  $U$  is a set which is not a member of itself. That is to say,  $U \notin U$ . That's impossible.

So it must be that  $U \notin U$ . That is,  $U$  is not a member of itself. So by definition of  $U$ ,  $U \in U$ . That's impossible too.

The resolution of the paradox is that *you can't just form sets arbitrarily*:  $U$  cannot be a set.

This seriously upset Frege.

## How to fix set theory?

To create a working theory of sets, we need to allow only certain things to be called sets.

Logic to the rescue!

Modern-day set-theory regards a set as being defined by a logical *predicate*. A predicate is a “proposition with a variable”: something like

*x is a number*

If we plug in various values for  $x$ , we get propositions which are either true or false:

- ▶ 11 is a number
- ▶ 3.141 is a number
- ▶ Patrick McGooohan is a number

## Predicates

We won't go into the details of formal set-theory much, but we will use the idea of a predicate.

There are lots of important predicates like

$x < 3$   
 $x$  is a prime number  
 $x$  is an odd number  
 $x = y$

and so on.

## Notation for propositions

In Boolean formulae, we usually use variables like  $X$ ,  $Y$  etc. to stand for propositions.

In predicates, we use lower-case variables like  $x$ ,  $y$  etc. to stand for the values that we're talking about.

A generic predicate with a variable  $x$  will often be written as  $P(x)$ .

This lets us write formulae which contain predicates as well as propositions, as we will soon see.

## Predicates, quantifiers, propositions

Given a predicate  $P(x)$  with a variable  $x$ , there are various propositions we'd like to talk about, such as:

- ▶  $P(x)$  is true when  $x$  is the number 19.
- ▶  $P(x)$  is true when  $x$  is *any* integer.
- ▶ There is some integer  $x$  which makes  $P(x)$  true.

We write these as follows:

- ▶  $P(19)$ .
- ▶  $\forall x \in \mathbb{Z}.P(x)$ .
- ▶  $\exists x \in \mathbb{Z}.P(x)$ .

Here  $\mathbb{Z}$  means the set of integers.

## Universal quantifier

The symbol  $\forall$  is called the *universal quantifier* and is read as “for all”.

It's a bit like a “big conjunction”: saying  $\forall x \in \mathbb{Z}.P(x)$  is the same as saying

$$\dots \wedge P(-2) \wedge P(-1) \wedge P(0) \wedge P(1) \wedge P(2) \wedge \dots$$

This proposition is true when  $P(x)$  is true for every integer  $x$ .

We say that  $x$  *ranges over* the set  $\mathbb{Z}$ .

The quantifier is useful because in examples like this, we cannot possibly write out the whole “big conjunction”—it's infinitely long.

## Existential quantifier

The symbol  $\exists$  is called the *existential quantifier* and is read as “there exists”.

It can be thought of as a “big disjunction”:  $\exists x \in \mathbb{Z}.P(x)$  is a bit like

$$\dots \vee P(-2) \vee P(-1) \vee P(0) \vee P(1) \vee P(2) \vee \dots$$

## Some examples

The proposition

$$\forall x \in \{-1, 0, 1\}. x + 1 > x$$

says the same thing as the proposition

$$(-1 + 1 > -1) \wedge (0 + 1 > 0) \wedge (1 + 1 > 1).$$

The proposition

$$\exists x \in \{-1, 0, 1\}. x + 1 > x$$

says the same thing as the proposition

$$(-1 + 1 > -1) \vee (0 + 1 > 0) \vee (1 + 1 > 1).$$

## More than one quantifier

If a predicate contains more than one variable, we can meaningfully write propositions with more than one quantifier.

For example:

$$\forall x \in \{-1, 0, 1\}. \exists y \in \{-1, 0, 1\}. x + y = 0.$$

Let's "decode" this into big conjunctions and disjunctions so that we can see what it means.

## More than one quantifier

Decoding the  $\forall$ ,

$$\forall x \in \{-1, 0, 1\}. \exists y \in \{-1, 0, 1\}. x + y = 0.$$

means the same as

$$\begin{aligned} & \exists y \in \{-1, 0, 1\}. -1 + y = 0 \\ \wedge & \exists y \in \{-1, 0, 1\}. 0 + y = 0 \\ \wedge & \exists y \in \{-1, 0, 1\}. 1 + y = 0. \end{aligned}$$

## More than one quantifier

We now have three  $\exists$ s to decode: doing so lets us see that our original proposition means the same as

$$\begin{aligned} & ((-1 + -1 = 0) \vee (-1 + 0 = 0) \vee (-1 + 1 = 0)) \\ \wedge & ((0 + -1 = 0) \vee (0 + 0 = 0) \vee (0 + 1 = 0)) \\ \wedge & ((1 + -1 = 0) \vee (1 + 0 = 0) \vee (1 + 1 = 0)) \end{aligned}$$

## Predicates, variables, propositions

We said that a predicate is a “proposition with a variable.” Our previous example shows that we are going to need to allow more than one variable. So a predicate is a “proposition with *some* variables”.

But we need to be more accurate. We said that something like

$$x > 0$$

is a predicate, whereas

$$\exists x \in \mathbb{Z}. x > 0$$

is a proposition.

What we really mean is something like

*a predicate is a proposition containing one or more variables which are not bound by a quantifier.*

## Negation and quantifiers

We have seen that  $\forall$  is like a “big conjunction”, and  $\exists$  is like a “big disjunction” .

We have also seen that  $\wedge$  and  $\vee$  are related by the de Morgan laws.

It should not be surprising to discover that  $\exists$  and  $\forall$  are also related by similar laws.

## de Morgan laws for quantifiers

The de Morgan laws for quantifiers are:

- ▶  $\neg(\forall x \in A.P(x)) \equiv \exists x \in A.\neg P(x)$ .
- ▶  $\neg(\exists x \in A.P(x)) \equiv \forall x \in A.\neg P(x)$ .

## de Morgan laws for quantifiers

To see that this make sense, consider a simple example:

$$\neg(\exists x \in \{-1, 0, 1\}.x + 1 = 3.)$$

We can “decode” the  $\exists$  as  $\vee$ , so that this proposition is the same as

$$\neg((-1 + 1 = 3) \vee (0 + 1 = 3) \vee (1 + 1 = 3))$$

which by de Morgan’s law is equivalent to

$$\neg(-1 + 1 = 3) \wedge \neg(0 + 1 = 3) \wedge \neg(1 + 1 = 3).$$

This is the same as

$$\forall x \in \{-1, 0, 1\}.\neg(x + 1 = 3).$$

## The logic of quantifiers

When  $\forall$  and  $\exists$  meet, there is some interesting interplay.

Which of the following things do you think are always true?

- ▶  $\exists x \in A.P(x) \rightarrow \forall x \in A.P(x)$ .
- ▶  $\forall x \in A.P(x) \rightarrow \exists x \in A.P(x)$ .
- ▶  $(\exists x \in A.\forall y \in B.P(x, y)) \rightarrow (\forall y \in B.\exists x \in A.P(x, y))$ .
- ▶  $(\forall y \in B.\exists x \in A.P(x, y)) \rightarrow (\exists x \in A.\forall y \in B.P(x, y))$ .

Are some of them true under certain circumstances and false under others? Hint: think about what happens when the sets  $A$  and  $B$  don’t have very many members (e.g. under two.)

## Equality of sets

The idea of a set is that it is simply the collection of its elements. That means that we should regard two sets as equal if they have the same elements.

Formally:

### Definition

Sets  $A$  and  $B$  are equal (notation:  $A = B$ ) if they have the same elements, i.e.

$$(\forall x \in A. x \in B) \wedge (\forall x \in B. x \in A).$$

i.e. "Every element of  $A$  is an element of  $B$  and vice versa."

## Subsets

If we take just one half of the definition of equality, we get the proposition

$$\forall x \in A. x \in B$$

i.e. "every element of  $A$  is an element of  $B$ ."

This means that the set  $A$  is *contained in*  $B$ , and we say that  $A$  is a subset of  $B$ .

### Definition

A set  $A$  is a subset of  $B$  (notation:  $A \subseteq B$ ) if

$$\forall x \in A. x \in B$$

Note that  $A = B$  if and only if  $A \subseteq B \wedge B \subseteq A$ .

## A remark on notation

Some people use  $A \subset B$  to say that  $A$  is a subset of  $B$ .

I like to write  $A \subseteq B$  because it gives the suggestion that  $A$  can in fact be the same as  $B$ .

Sometimes, people who use  $A \subseteq B$  in this way go on to use  $A \subset B$  to mean that  $A$  is a subset of  $B$  but  $A \neq B$ . Occasionally this is emphasised by writing  $A \subsetneq B$ .

$A$  is sometimes called a *proper subset* of  $B$  in this case.

In this course, if we need to make this distinction, we'll say so explicitly.

## Union of sets

### Definition

Given sets  $A$  and  $B$ , the *union*  $A \cup B$  is defined to be the set

$$\{x \mid (x \in A) \vee (x \in B)\}.$$

The notation above is called a *set comprehension*: it defines a set by means of a predicate.

In this case,  $A \cup B$  is defined to be the set of things that satisfy the predicate

$$(x \in A) \vee (x \in B)$$

This just says that the elements of  $A \cup B$  are the elements of  $A$  and the elements of  $B$  taken together.

## Intersection of sets

Similarly, we can make this definition:

### Definition

Given sets  $A$  and  $B$ , the *intersection*  $A \cap B$  is defined to be the set

$$\{x \mid (x \in A) \wedge (x \in B)\}.$$

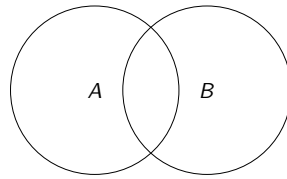
That is, the intersection consists of those things that are in both  $A$  and  $B$ .

## Venn diagrams

It can be useful to visualise these operations. *Venn diagrams* are the common way to do so. Sets are drawn as overlapping circles (or other shapes) and then parts of the diagram can be carved out using intersections and unions.

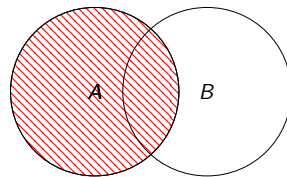
## Venn diagrams

Here are two sets,  $A$  and  $B$ .



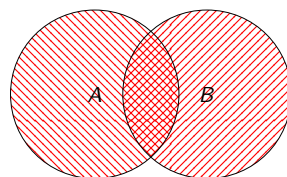
## Venn diagrams

Here the set  $A$  is highlighted.



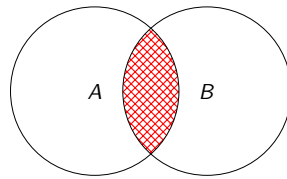
## Venn diagrams

Here the union  $A \cup B$  is highlighted.



## Venn diagrams

Here the intersection  $A \cap B$  is highlighted.



## Examples

Some examples of unions and intersections:

- ▶ If  $E$  is the set of even integers and  $O$  is the set of odd integers, then  $E \cup O = \mathbb{Z}$ .
- ▶ If  $P$  is the set of prime numbers, then  $O \cup P = O \cup \{2\}$ .
- ▶  $E \cap O = \emptyset$ .
- ▶  $E \cap \mathbb{Z} = E$ .
- ▶ If  $A$  is the set of all Computer Science students at Bath, and  $B$  is the set of all people from Norway, then  $A \cap B$  is the set of all Norwegian Computer Science students at Bath.

## Properties of $\cup$ and $\cap$

Since  $\cup$  is defined out of  $\vee$  and  $\cap$  is defined out of  $\wedge$ , union and intersection share a lot of properties with disjunction and conjunction:

**Commutativity**  $A \cup B = B \cup A$  and  $A \cap B = B \cap A$ .

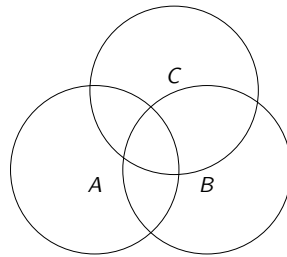
**Associativity**  $A \cup (B \cap C) = (A \cup B) \cap C$  and  $A \cap (B \cup C) = (A \cap B) \cup C$ .

**Distributivity 1**  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

**Distributivity 2**  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

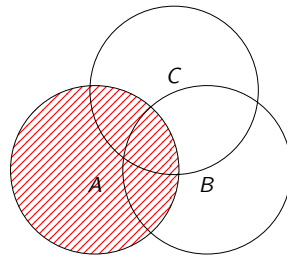
## Distributivity in a Venn diagram

We can convince ourselves the laws are true using pictures.



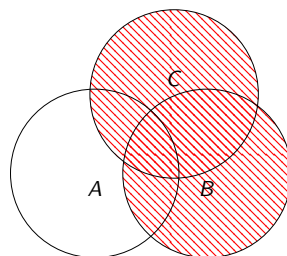
## Distributivity in a Venn diagram

A:



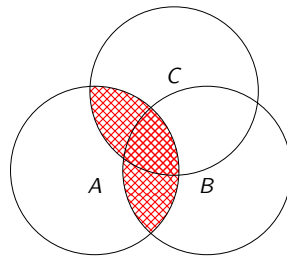
## Distributivity in a Venn diagram

$B \cup C$ :



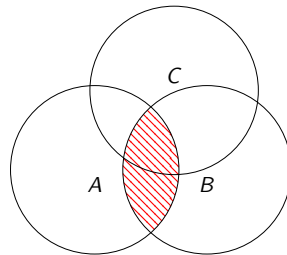
## Distributivity in a Venn diagram

$A \cap (B \cup C)$ :



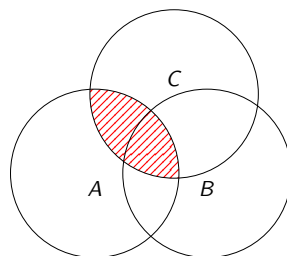
## Distributivity in a Venn diagram

$A \cap B$ :



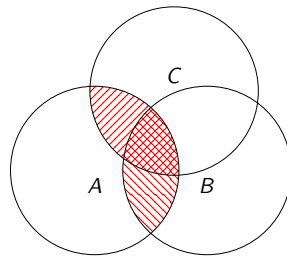
## Distributivity in a Venn diagram

$A \cap C$ :



## Distributivity in a Venn diagram

$(A \cap B) \cup (A \cap C)$ :



## Proofs, not pictures

A real proof of these laws will not rely on pictures, though.

To prove commutativity of  $\cup$ , for instance, we can just unpack the definition and use commutativity of  $\vee$  as follow.

$$\begin{aligned} A \cup B &= \{x \mid x \in A \vee x \in B\} && \text{(definition)} \\ &= \{x \mid x \in B \vee x \in A\} && \text{(commutativity of } \vee \text{)} \\ &= B \cup A. && \text{(definition)} \end{aligned}$$

### Exercise

Prove that the other laws are true, using similar reasoning.

## Set difference

### Definition

Given two sets  $A$  and  $B$ , define  $A \setminus B$  to be the set

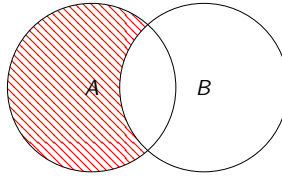
$$\{x \mid x \in A \wedge x \notin B\}.$$

$A \setminus B$  contains all those elements of  $A$  which are not in  $B$  and is called the *difference* of  $A$  and  $B$ .

We read  $A \setminus B$  as "A minus B".

## Venn diagram of set difference

$A \setminus B$  looks like this:



## Complement of a set

Sometimes when working with sets we work with a *universe*  $U$ , which is a big set containing all the elements we're ever going to talk about.

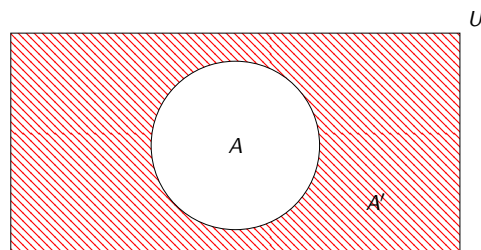
In that case, every set  $A$  we ever work with is a subset of  $U$ .

Under these circumstances, we can define the *complement*  $A'$  of a set:  $A' = U \setminus A$ , so  $A'$  contains everything that  $A$  does not.

Obviously this makes no sense without a universe; but  $A \setminus B$  is sometimes called *relative complement*.

## Venn diagram of complement

The universe  $U$  is usually drawn as a large rectangle surrounding everything else:



## Properties of complement

Complement has certain useful properties, which have something in common with those of *negation* in logic.

- ▶  $A \cap A' = \emptyset$ .
- ▶  $A \cup A' = U$ .
- ▶  $(A \cup B)' = (A' \cap B')$ .
- ▶  $(A \cap B)' = (A' \cup B')$ .

The last two are the *de Morgan laws*.

## Proof of the de Morgan laws

$x \in (A \cup B)'$  is equivalent to  $x \notin (A \cup B)$   
is equivalent to  $\neg(x \in A \cup B)$   
is equivalent to  $\neg((x \in A) \vee (x \in B))$   
is equivalent to  $\neg(x \in A) \wedge \neg(x \in B)$   
is equivalent to  $x \notin A \wedge x \notin B$   
is equivalent to  $x \in A' \wedge x \in B'$   
is equivalent to  $x \in A' \cap B'$

The other de Morgan law can be proved similarly.

## Boolean algebras

We've looked at two areas of mathematics—logic and set theory—and found that there are useful *operators* in each which look quite similar:

**Logic** Conjunction, disjunction, negation.

**Set theory** Intersection, union, complement.

There are also *constants* in the two areas which have aspects in common:

**Logic** True, false

**Set theory** The universe  $U$ , the empty set  $\emptyset$ .

When mathematicians see structures that have something in common, they often like to *generalize*: give a general definition of what the “something in common” is, and prove facts about *any such structure*.

## Boolean algebras

### Definition

A *Boolean algebra* is a set  $A$ , with two binary operations  $\wedge$  and  $\vee$ , a unary operation  $\neg$ , and two constants 0 and 1, such that the following axioms hold:

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

**Commutativity**  $x \vee y = y \vee x$       $x \wedge y = y \wedge x$ .

**Absorption**  $x \vee (x \wedge y) = x$       $x \wedge (x \vee y) = x$ .

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

**Complements**  $a \vee \neg a = 1$       $a \wedge \neg a = 0$ .

## Boolean algebras

Generalizing in this way means that we can prove things about *any Boolean algebra* which will then automatically apply to propositional logic, to set theory, and to any other Boolean algebra we come up with.

That's how mathematics works!

## Example Boolean algebras

### Example

The set  $\{t, f\}$  of truth values is a Boolean algebra.  $\wedge$  is conjunction,  $\vee$  is disjunction,  $\neg$  is negation, 0 is f and 1 is t.

It is easy to check that the required axioms are satisfied. They ought to: the definition of Boolean algebra was motivated by this example.

Before we can introduce the next example we need a definition.

## Powerset

### Definition

Given a set  $A$ , the set  $\mathcal{P}A$  is defined to be

$$\{B \mid B \subset A\}$$

i.e. the set of all subsets of  $A$ .

### Example

$$\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Note that we always have  $A \in \mathcal{P}A$ .

## Example Boolean algebras

### Example

Given a set  $A$ , the powerset  $\mathcal{P}A$  is a Boolean algebra:  $\wedge$  is  $\cap$ ,  $\vee$  is  $\cup$ ,  $\neg$  is complement relative to  $A$  (so  $\neg B = A \setminus B$ ),  $0$  is  $\emptyset$  and  $1$  is  $A$  itself.

Check that the axioms hold!

## Boolean algebras

### Exercise

Show that the following laws are true in any Boolean algebra:

- ▶  $x \vee x = x$        $x \wedge x = x$
- ▶  $x \vee 0 = x$        $x \wedge 1 = x$
- ▶  $x \vee 1 = 1$        $x \wedge 0 = 0$
- ▶  $\neg 0 = 1$        $\neg 1 = 0$
- ▶  $\neg(x \wedge y) = \neg x \vee \neg y$        $\neg(x \vee y) = \neg x \wedge \neg y$
- ▶  $\neg\neg x = x$ .

The first few are not too hard.

## Laws of Boolean algebras

For the last three laws, it can be helpful to show first that *complements are unique*, that is, if  $x \wedge y = 0$  and  $x \vee y = 1$  then  $y = \neg x$ .

To put this another way, if  $y$  and  $z$  are both complements of  $x$ , that is

$$x \wedge y = 0 = x \wedge z \quad x \vee y = 1 = x \vee z$$

then  $y = z$ .

To show this, consider the formula  $y \wedge (x \vee z)$  and use the distributive law.

## The power of mathematics

The power of this generalization is that once we've established that certain properties follow from our axioms, *any* structure that satisfies the axioms will have those properties.

There are lots of other examples of Boolean algebras in mathematics: topological spaces; the set of central idempotents of a ring, ...

The idea of defining a structure (like a Boolean algebra) by operations and axioms and working on these structures in a general way is the core of the subject of *algebra*.

It has a lot in common with computer science: when we program we often define *data structures* and *operations on data*. We can frequently design algorithms in an abstract, general way.

## Hooray for maths

Hooray for maths.