Sets 1

Today:

- ☐ Basics
- ☐ Set theory in first-order logic
- ☐ Operations on sets
- ☐ Identities
- ☐ Paradoxes of naive set theory

1 Basics

You've seen sets before, probably since grade school, often introduced with examples like:

$$S = \{\texttt{apples}, \texttt{oranges}, \texttt{bananas}\}$$

This is a set with three elements, a fact which we would denote $|S| = 3$. What exactly *are* those three elements? Well, I really don't know. Maybe `apples` is *itself* a set—the set of all things presently on earth that you might like to call an apple. Or maybe `apples` is an abstract *concept*, and this set S is a set containing three concepts. A set of concepts. Interesting. Or maybe `apples` is just supposed to be a sequence of six letters, what we call a *string*—here, the letter `a`, then `p`, then another `p`, then `l`, then `e`, then `s`. In that case `apples` has nothing to do with any physical apple, and nothing to do with he concept of an apple—it is *just* a sequence of characters. Maybe.

One thing I *do* know is that

$$\texttt{apples} \in S,$$

which we read as the point "apples" being *in* the set S, or *an element of* the set S. We can call the things in set its *elements*, or its *members*, or its *points*. We might represent it by a diagram, a circle or a box where we make a point, perhaps label it, one point for each item in our set.

What about the set

$$S' = \{\texttt{oranges}, \texttt{apples}, \texttt{oranges}, \texttt{bananas}\}?$$

This is the *same* set as before: $S = S'$. That's because there's no notion of a set containing an item multiple times; rather, something is in the set or it is not. Well, I shouldn't say that there no such notion—just that it's not the notion of a *set*. It's a different notion, which is called a *multiset*.

Also, there is no notion for the *order* of items in a set; it doesn't matter what order you list things inside the curly brackets. It'll just give you a different way of writing the same set.

Here are some other sets you know and love.

$$\begin{aligned}
\mathbb{B} &= \{0,1\} \quad \textit{The boolean domain} \\
\text{Digits} &= \{0,1,2,3,4,5,6,7,8,9\} \quad \textit{The set of decimal digits} \\
\mathbb{N} &= \{0,1,2,\ldots\} \quad \textit{The set of natural numbers} \\
\text{Primes} &= \{2,3,5,7,11,13,\ldots\} \quad \textit{The set of prime numbers} \\
\mathbb{Z} &= \{\ldots,-2,-1,0,1,2,\ldots\} \quad \textit{The set of integers} \\
\mathbb{Q} &= \{p/q : p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\} \quad \textit{The set of rationals} \\
\mathbb{R} &= \textit{The set of real numbers}
\end{aligned}$$

There are lots of ways to specify any given set. All the following mean the same thing:

$$\begin{aligned}
P &= \{n : n \text{ is a prime number}\} \\
&= \{2,3,5,7,11,13,\ldots\} \\
&= \{n \in \mathbb{N} \colon (\forall a \in \mathbb{N})(\forall b \in \mathbb{N})(a \cdot b = n \rightarrow a = 1 \vee b = 1\}
\end{aligned}$$

Or you could just as well say it in English, "Let P be the set of all primes."

The following notation might be familiar from calculus: writing $[a,b]$, $[a,b)$, $(a,b]$, and (a,b) for intervals of real numbers, $a,b \in \mathbb{R}$, $a \leq b$. A bracket indicates that you include that endpoint; a parenthesis means that you don't.

I'm also fond of the notation $[a..b]$ for the set of *integers* between a and b, inclusive (assume again that $a \leq b$).

I like the set $\mathbb{Z}_n = [n] = [0..n-1] = \{0,1,\ldots,n-1\}$. We will learn more about this set later. We will also ascribe operations to it. But don't think that the operations somehow come with the set. If we are thinking of $\mathbb{N}$ as a set of integers, then this *thing*, as a set, knows nothing of successor, addition, multiplication, or whatever.

2 Set Theory in First-Order Logic

We can treat set theory in first order logic. We will only need two things:

- A binary predicate that we denote $\in$
- A constant symbol that we denote $\emptyset$.

That's it! It is *very* spare. All the rest of the things we do to sets or say about sets—we can actually write them using only the vocabulary above.

A very sensible alternative notation for $\emptyset$ would be $\{\ \}$. But it is rarely used.

We write the $\in$ predicate in infix, but don't let that fool you. It takes in two values, which are sets, and it returns a boolean value.

Wait—what do you mean that $\in$ takes two arguments, which are sets? Surely the *second* input is a set, but the first?

There is no problem with sets containing other sets. The set $\{\mathbb{N}, \emptyset, 4, \text{apple}, \{2,4\}\}$ is a perfectly valid set, some of whose elements happen to be sets.

Don't confuse $\emptyset$ with, say $\{\emptyset\}$. The first is a set with no elements. The second is a set with one element. We can even define natural numbers in such a manner, letting $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$, and so on, with $n = \{0, 1, \ldots, n-1\}$.

In *naive* set theory—which is what we will study—we let things be in sets that are not themselves sets. So it's alright for apples to be in sets, where apples, whatever you regard them as, are not sets. In formal treatments of set theory, however, we develop *axioms* to understand set theory and, at least in most famous of these axiom systems, nothing will ever reside in a set that is not itself a set.

3 Operations on Sets

Introduce the following operations, defining each with first-order logic and illustrating each diagrammatically, using a *Venn Diagram*.

1. $A \cup B$ — the *union* of sets A and B.
2. $A \cap B$ — the *intersection* of sets A and B.
3. A^c, alternatively written $\overline{A}$ — the (set-theoretic) *complement* of A, which is always relative to some *universe*, call it $\mathcal{U}$.
4. $A \oplus B$ — the *symmetric difference* between two sets — all the points that are in one but not the other. How does this generalize to the symmetric difference of three or more sets?
5. $A - B$, alternatively written $A \setminus B$ — the *set difference* between two sets

Try relating these notions to our first-order logic. For example, how would you say:

> For any pair of sets x and y there is a set $x \cup y$ that contains all of the elements of x and y?

You would write it as:

$$(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow (u \in x \vee u \in y)).$$

Next introduce the *subset* binary relation, $A \subseteq B$. Again, defined logically: $A \subseteq B$ is defined as $(\forall x)(x \in A \to x \in B)$.

And the *superset* binary relation, $A \supseteq B$, defined by $A \supseteq B$ if $B \subseteq A$.

We can do infinite unions and intersections, too. For example, what is

$$\bigcup_{n\in\mathbb{N}} \{2n\} \ ?$$

It's the set of all even natural numbers. Or

$$\bigcap_{a\in\mathbb{R}^+} [0,a] \ ?$$

It's just $\{0\}$. Here $[a,b]$ is all real numbers between a and b, inclusive. We also have interval notation $[a,b)$, $(a,b]$, and (a,b) where we do *not* include the endpoint with the parenthesis.

Another important operation on sets is the powerset of a set:

$$\mathcal{P}(S) \quad = \quad \{A\colon\ A \subseteq S\}$$

That is, $\mathcal{P}(S)$ is the set of all subsets of S.

We have already met the *cardinality* of a set, which, for a finite set, tells you the number of elements in it. We denote this function $|\cdot|$. Looks like absolute value, but has a totally different meaning.

If A is a finite set, what is $|\mathcal{P}(A)|$? It is easily seen to be $2^{|A|}$. In fact, an alternative notation for $\mathcal{P}(A)$ is 2^A, which you might think of as suggestive of the fact just stated.

4 Identities

Lots of simple identities can be proven directly from the definition and by using facts of logic (which, in turn, can invariably be established with truth tables). Like the following:

$$\begin{array}{rcl@{\qquad}rcll}
A \cup A &=& A & A \cap A &=& A \\
A \cup B &=& B \cup A & A \cap B &=& B \cap A \\
A \cup (B \cup C) &=& (A \cup B) \cup C & A \cap (B \cap C) &=& (A \cap B) \cap C \\
A \cup (B \cap C) &=& (A \cup B) \cap (B \cup C) & A \cap (B \cup C) &=& (A \cap B) \cup (A \cap C) \\
A \cup \emptyset &=& A & A \cap \emptyset &=& \emptyset \\
A \cup \mathcal{U} &=& \mathcal{U} & A \cap \mathcal{U} &=& A \\
(A^c)^c &=& A & & & \\
A \cup A^c &=& \mathcal{U} & A \cap A^c &=& \emptyset \\
\mathcal{U}^c &=& \emptyset & \emptyset^c &=& \mathcal{U} \\
(A \cup B)^c &=& A^c \cap B^c & (A \cap B)^c &=& A^c \cup B^c & \textit{De Morgan's laws}
\end{array}$$

Let's prove one of these, say the first listed of De Morgan's laws. To show that, we note that

$$
\begin{aligned}
x \in (A \cup B)^c \quad & \text{iff } \neg(x \in A \cup B) && \textit{Definition of the complement of a set} \\
& \text{iff } \neg(x \in A \vee x \in B) && \textit{Definition of the union of two sets} \\
& \text{iff } \neg(x \in A) \wedge \neg(x \in B) && \textit{De Morgan's law in the logical setting} \\
& \text{iff } x \in A^c \wedge x \in B^c && \textit{Definition of the complement of a set} \\
& \text{iff } x \in A^c \cap B^c && \textit{Definition of the intersection of two sets}
\end{aligned}
$$

and we are done.

5 Paradoxes of Naive Set Theory

Naive set theory, where we describe sets with natural language, where we write things like $\{x\colon\ \cdots\}$ with it being implicit the universe $\mathcal{U}$ from which x is drawn, can sometimes run into trouble. Here are some examples:

- We've already set that sets can contains sets. But can a set contain *itself*? If we casually allow stuff like that, we encounter *Russell's paradox.* Let $S = \{x\colon\ x \notin x\}$. The problem is: *is S itself in S*? We are saying that $S \in S$ iff $S \notin S$. But this makes no sense! Somehow, there must be something illegitimate with our definition of S.

- Consider this example: *let BIG be the largest natural number that can be described with fewer than 200 characters of English text.* I have used 92 characters of English text to define the number BIG. Well, what is wrong with this? Let me try: *Let BIGGER be one more than BIG, where BIG is the largest natural number that can be described with fewer than 200 characters of English text.* I have just used 142 characters. With them, I have defined a number that is bigger than BIG. But BIG was supposed to be the *biggest* number that I could describe with fewer than 200 characters of text.

  What's wrong here is very subtle. It really has to do with English being too imprecise to do what we are expecting it to do. If you're more careful about your descriptive language, you *can* define huge numbers like BIG with this approach. In fact, it's called the "busy beaver function," and you might learn about it in ECS120 or ECS220.

6 Power set

We ended class with a quick definition of the power set of a set, but it was too rushed, so I will go over that again on Tuesday.