Sets

Joseph R. Mileti

February 27, 2017

1 Sets, Set Construction, and Subsets

1.1 Sets and Set Construction

In mathematics, a set is a collection of elements without regard to repetition or order. Intuitively, a set is a box where the only thing that matters are the objects that are inside it, and furthermore the box does not have more than 1 of any given object. For example, $\{3, 5\}$ is a set with 2 elements. Since all that matters are the elements, we define two sets to be equal if they have the same elements, regardless of how the sets themselves are defined or described.

Definition 1.1. *Given two sets A and B, we say that $A = B$ if A and B have exactly the same elements.*

Since the elements themselves matter, but not their order, we have $\{3, 7\} = \{7, 3\}$ and $\{1, 2, 3\} = \{3, 1, 2\}$. Also, although we typically would not even write something like $\{2, 5, 5\}$, if we choose to do so then we would have $\{2, 5, 5\} = \{2, 5\}$ because both have the same elements, namely 2 and 5.

We use $\in$ to represent the fact that a particular object is an element of a certain set. For example, we have $2 \in \{2, 5\}$ and $3 \notin \{2, 5\}$. Since sets are mathematical objects, they may be elements of other sets. For example, we can form the set $S = \{1, \{2, 3\}\}$. Notice that we have $1 \in S$ and $\{2, 3\} \in S$, but $2 \notin S$ and $3 \notin S$. As a result, S has only 2 elements, namely 1 and $\{2, 3\}$. Thinking of a set as a box, one element of S is the number 1, and the other is a different box. The empty set is the unique set with no elements. We can write it as $\{\}$, but instead we typically denote it by $\emptyset$. There is only *one* empty set, because if both A and B have no elements, then they have exactly the same elements for vacuous reasons, and hence $A = B$. Notice that $\{\emptyset\}$ does not equal $\emptyset$. After all, $\{\emptyset\}$ has one element! You can think of $\{\emptyset\}$ as a box that has one empty box inside it.

Notice that sets can be either finite or infinite. At this point, our standard examples of infinite sets are the universes of numbers:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- $\mathbb{N}^+ = \{1, 2, 3, \dots\}$.
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- $\mathbb{Q}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.

Beyond these fundamental sets, there are various ways to define new sets. In some cases, we can simply list the elements as we did above. Although this often works for small finite sets, it is almost never a good idea to list the elements of a set with 20 or more elements, and it rarely works for infinite sets (unless there is an obvious pattern like $\{5, 10, 15, 20, \dots\}$). One of the standard ways to define a set S is to carve it out

of some bigger set A by describing a certain property that may or may not be satisfied by an element of A. For example, we could define

$$S = \{n \in \mathbb{N} : 5 < n < 13\}.$$

We read this line by saying that S is defined to be the set of all $n \in \mathbb{N}$ such that $5 < n < 13$. Thus, in this case, we are taking $A = \mathbb{N}$, and forming a set S by carving out those elements of A that satisfy the condition that $5 < n < 13$. In other words, think about going through each of element n, checking if $5 < n < 13$ is a true statement, and collecting those $n \in \mathbb{N}$ that make it true into a set that we call S. In more simple terms, we can also describe S as follows:

$$S = \{6, 7, 8, 9, 10, 11, 12\}.$$

It is important that we put the "$\mathbb{N}$" in the above description, because if we wrote $\{n : 5 < n < 13\}$ then it would be unclear what n we should consider. For example, should $\frac{11}{2}$ be in this set? How about $\sqrt{17}$? Sometimes the "universe" of numbers (or other mathematical objects) that we are working within is clear, but typically it is best to write the global set that we are picking elements from in order to avoid such ambiguity. Notice that when we define a set, there is no guarantee that it has any elements. For example, $\{q \in \mathbb{N} : q^2 = 2\} = \emptyset$ because $\sqrt{2}$ is irrational. Keep in mind that we can also use words in our description of sets, such as $\{n \in \mathbb{N} : n \text{ is an even prime}\}$. As mentioned above, two sets that have quite different descriptions can be equal. For example, we have

$$\{n \in \mathbb{N} : n \text{ is an even prime}\} = \{n \in \mathbb{N} : 3 < n^2 < 8\}$$

because both sets equal $\{2\}$. Always remember the structure of sets formed in this way. We write

$$\{x \in A : \mathsf{P}(x)\}$$

where A is a known set and $\mathsf{P}(x)$ is a "property" such that given a particular $y \in A$, the statement $\mathsf{P}(y)$ is either true or false.

Another way to describe a set is through a "parametric" description. Rather than carving out a certain subset of a given set by describing a property that the elements must satisfy, we can instead form all the elements one obtains by varying a value through a particular set. For example, consider the following description of a set:

$$S = \{3x^2 + 1 : x \in \mathbb{R}\}.$$

Although the notation looks quite similar to the above (in both case we have curly braces, with a : in the middle), this set is described differently. Notice that instead of having a set that elements are coming from on the left of the colon, we now have a set that elements are coming from on the right. Furthermore, we now have a formula on the left rather than a property on the right. The difference is that for a property, when we plug in an element from the given set, we either obtain a true or false value, but that isn't the case for a formula like $3x^2 + 1$. The idea here is that instead of carving out a subset of $\mathbb{R}$ by using a property (i.e. taking those elements that make the property *true*), we let x vary through all real numbers, plug each of these real numbers x into $3x^2 + 1$, and form the set of all possible outputs. For example, we have $4 \in S$ because $4 = 3 \cdot 1^2 + 1$. In other words, when $x = 1$, the left hand side gives the value 4, so we should put $4 \in S$. Notice also that $4 = 3 \cdot (-1)^2 + 1$, so we can also see that $4 \in S$ because of the "witness" -1. Of course, we are forming a set, so we do not repeat the number 4. We also have $1 \in S$ because $1 = 3 \cdot 0^2 + 1$, and we have $76 \in S$ because $76 = 3 \cdot 5^2 + 1$. Notice also that $7 \in S$ because $7 = 3 \cdot (\sqrt{2})^2 + 1$.

In a general parametric set description, we will have a set A and a *function* $f(x)$ that allows inputs from A, and we write

$$\{f(x) : x \in A\}$$

for the set of all possible outputs of the function as we vary the inputs through the set A. We will discuss the general definition of a function in the next section, but for the moment you can think of them as given by formulas.

Now it is possible and indeed straightforward to turn any parametric description of a set into one where we carve out a subset by a property. In our case of $S = \{3x^2 + 1 : x \in \mathbb{R}\}$ above, we can alternatively write it as

$$S = \{y \in \mathbb{R} : \text{There exists } x \in \mathbb{R} \text{ with } y = 3x^2 + 1\}.$$

Notice how we flipped the way we described the set by introducing a "there exists" quantifier in order to form a property. This is always possible for a parametric description. For example, we have

$$\{5n + 4 : n \in \mathbb{N}\} = \{m \in \mathbb{N} : \text{There exists } n \in \mathbb{N} \text{ with } m = 5n + 4\}.$$

Thus, these parametric descriptions are not essentially new ways to describe sets, but they can often be more concise and clear.

By the way, we can use multiple parameters in our description. For example, consider the set

$$S = \{18m + 33n : m, n \in \mathbb{Z}\}.$$

Now we are simply letting m and n vary through all possible values in $\mathbb{Z}$ and collecting all of the values $18m + 33n$ that result. For example, we have $15 \in S$ because $15 = 18 \cdot (-1) + 33 \cdot 1$. We also have $102 \in S$ because $102 = 18 \cdot 2 + 33 \cdot 2$. Notice that we are varying m and n independently, so they might take different values, or the same value (as in the case of $m = n = 2$). Don't be fooled by the fact that we used different letters! As above, we can flip this description around by writing

$$S = \{k \in \mathbb{Z} : \text{There exists } m, n \in \mathbb{Z} \text{ with } k = 18m + 33n\}.$$

1.2 Subsets and Set Equality

Definition 1.2. *Given two sets A and B, we write $A \subseteq B$ to mean that every element of A is an element of B. More formally, $A \subseteq B$ means that for all x, if $x \in A$, then $x \in B$.*

Written more succinctly, $A \subseteq B$ means that for all $a \in A$, we have that $a \in B$. To prove that $A \subseteq B$, one takes a completely arbitrary $a \in A$, and argues that $a \in B$. For example, let $A = \{6n : n \in \mathbb{Z}\}$ and let $B = \{2n : n \in \mathbb{Z}\}$. Since both of these sets are infinite, we can't show that $A \subseteq B$ by taking each element of A in turn and showing that it is an element of B. Instead, we take an *arbitrary* $a \in A$, and show that $a \in B$. Here's the proof.

Proposition 1.3. *Let $A = \{6n : n \in \mathbb{Z}\}$ and $B = \{2n : n \in \mathbb{Z}\}$. We have $A \subseteq B$.*

Proof. Let $a \in A$ be arbitrary. By definition of A, this means that we can fix an $m \in \mathbb{Z}$ with $a = 6m$. Notice then that $a = 2 \cdot (3m)$. Since $3m \in \mathbb{Z}$, it follows that $a \in B$. Since $a \in A$ we arbitrary, we conclude that $A \subseteq B$. □

As usual, pause to make sure that you understand the logic of the argument above. First, we took an arbitrary element a from the set A. Now since $A = \{6n : n \in \mathbb{Z}\}$ and this is a parametric description with an implicit "there exists" quantifier, there must be one fixed integer value of n that puts a into the set A. In our proof, we chose to call that one fixed integer m. Now in order to show that $a \in B$, we need to exhibit a $k \in \mathbb{Z}$ with $a = 2k$. In order to do this, we hope to manipulate $a = 6m$ to introduce a 2, and ensure that the element we are multiplying by 2 is an integer.

What would go wrong if we tried to prove that $B \subseteq A$? Let's try it. Let $b \in B$ be arbitrary. Since $b \in B$, we can fix $m \in \mathbb{Z}$ with $b = 2m$. Now our goal is to try to prove that we can find an $n \in \mathbb{Z}$ with $b = 6n$. It's not obvious how to obtain a 6 from that 2, but we can try to force a 6 in the following way. Since $b = 2m$ and $2 = \frac{6}{3}$, we can write $b = 6 \cdot \frac{m}{3}$. We have indeed found a number n such that $b = 6n$, but we have not

checked that this n is an integer. In general, dividing an integer by 3 does not result in an integer, so this argument currently has a hole in it.

Although that argument has a problem, we can not immediately conclude that $B \not\subseteq A$. Our failure to find an argument does not mean that an argument does not exist. So how can we show that $B \not\subseteq A$? All that we need to do is find just *one example* of an element of B that is not an element of A (because the negation of the "for all" statement $A \subseteq B$ is a "there exists" statement). We choose 2 as our example. However, we need to convince everybody that this choice works. So let's do it! First, notice that $2 = 2 \cdot 1$, so $2 \in B$ because $1 \in \mathbb{Z}$. We now need to show that $2 \notin A$, and we'll do this using a proof by contradiction. Suppose instead that $2 \in A$. Then, by definition, we can fix an $m \in \mathbb{Z}$ with $2 = 6m$. We then have that $m = \frac{2}{6} = \frac{1}{3}$. However, this a contradiction because $\frac{1}{3} \notin \mathbb{Z}$. Since our assumption that $2 \in A$ led to a contradiction, we conclude that $2 \notin A$. We found an example of an element that is in B but not in A, so we conclude that $B \not\subseteq A$.

Recall that two sets A and B are defined to be equal if they have the same elements. Therefore, we have $A = B$ exactly when both $A \subseteq B$ and $B \subseteq A$ are true. Thus, given two sets A and B, we can prove that $A = B$ by performing two proofs like the one above. Such a strategy is called a *double containment* proof. We give an example of such an argument now.

Proposition 1.4. *Let $A = \{7n - 3 : n \in \mathbb{Z}\}$ and $B = \{7n + 11 : n \in \mathbb{Z}\}$. We have $A = B$.*

Proof. We prove that $A = B$ by showing that both $A \subseteq B$ and also that $B \subseteq A$.

- We first show that $A \subseteq B$. Let $a \in A$ be arbitrary. By definition of A, we can fix an $m \in \mathbb{Z}$ with $a = 7m - 3$. Notice that

$$\begin{aligned} a &= 7m - 3 \\ &= 7m - 14 + 11 \\ &= 7(m - 2) + 11. \end{aligned}$$

  Now $m - 2 \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so it follows that $a \in B$. Since $a \in A$ was arbitrary, we conclude that $A \subseteq B$.

- We now show that $B \subseteq A$. Let $b \in B$ be arbitrary. By definition of B, we can fix an $m \in \mathbb{Z}$ with $a = 7m + 11$. Notice that

$$\begin{aligned} a &= 7m + 11 \\ &= 7m + 14 - 3 \\ &= 7(m + 2) - 3. \end{aligned}$$

  Now $m + 2 \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so it follows that $a \in B$. Since $a \in A$ was arbitrary, we conclude that $A \subseteq B$.

We have shown that both $A \subseteq B$ and $B \subseteq A$ are true, so it follows that $A = B$. □

Here is a more interesting example. Consider the set

$$S = \{9m + 15n : m, n \in \mathbb{Z}\}.$$

For example, we have $9 \in S$ because $9 = 9 \cdot 1 + 15 \cdot 0$. We also have $3 \in S$ because $3 = 9 \cdot 2 + 15 \cdot (-1)$ (or alternatively because $3 = 9 \cdot (-3) + 15 \cdot 2$). We can always generate new values of S by simply plugging in values for m and n, but is there another way to describe the elements of S in an easier way? We now show that an integer is in S exactly when it is a multiple of 3.

Proposition 1.5. *We have $\{9m + 15n : m, n \in \mathbb{Z}\} = \{3m : m \in \mathbb{Z}\}$.*

Proof. We give a double containment proof.

- We first show that $\{9m + 15n : m, n \in \mathbb{Z}\} \subseteq \{3m : m \in \mathbb{Z}\}$. Let $a \in \{9m + 15n : m, n \in \mathbb{Z}\}$ be arbitrary. By definition, we can fix $k, \ell \in \mathbb{Z}$ with $a = 9k + 15\ell$. Notice that

$$\begin{aligned} a &= 9k + 15\ell \\ &= 3 \cdot (3k + 5\ell). \end{aligned}$$

  Now $3k+5\ell \in \mathbb{Z}$ because $k, \ell \in \mathbb{Z}$, so it follows that $a \in \{3m : m \in \mathbb{Z}\}$. Since $a \in \{9m+15n : m, n \in \mathbb{Z}\}$ was arbitrary, we conclude that $\{9m + 15n : m, n \in \mathbb{Z}\} \subseteq \{3m : m \in \mathbb{Z}\}$.

- We now show that $\{3m : m \in \mathbb{Z}\} \subseteq \{9m + 15n : m, n \in \mathbb{Z}\}$. Let $a \in \{3m : m \in \mathbb{Z}\}$ be arbitrary. By definition, we can fix $k \in \mathbb{Z}$ with $a = 3k$. Notice that

$$\begin{aligned} a &= 3k \\ &= (9 \cdot (-3) + 15 \cdot 2) \cdot k \\ &= 9 \cdot (-3k) + 15 \cdot 2k. \end{aligned}$$

  Now $-3k, 2k \in \mathbb{Z}$ because $k \in \mathbb{Z}$, so it follows that $a \in \{9m+15n : m, n \in \mathbb{Z}\}$. Since $a \in \{3m : m \in \mathbb{Z}\}$ was arbitrary, we conclude that $\{3m : m \in \mathbb{Z}\} \subseteq \{9m + 15n : m, n \in \mathbb{Z}\}$.

We have shown that both $\{9m+15n : m, n \in \mathbb{Z}\} \subseteq \{3m : n \in \mathbb{Z}\}$ and $\{3m : m \in \mathbb{Z}\} \subseteq \{9m+15n : m, n \in \mathbb{Z}\}$ are true, so it follows that $\{9m + 15n : m, n \in \mathbb{Z}\} = \{3m : m \in \mathbb{Z}\}$. □