DISCRETE MATH AND THEORY 1

Vagul Mahadevan
University of Virginia
2023

Contents

1 Sets

It's hard to overstate the importance of sets in mathematics. Sets underlie all of mathematics, and a good conceptual understanding of them is a necessary foundation to approach higher math. Fortunately, you probably already have some intuitive understanding of how sets work–for instance, in geometry, when you made a statement like, "all squares are rectangles, but not all rectangles are squares," you were really making a statement about the *set* of squares and how it relates to the *set* of rectangles. Here, we will add some formalism to your understanding of sets in a framework called **naive set theory**.

Let us begin with a definition:

Definition. A **set** is an *unordered* collection of *unique* objects. Each of these objects is called an **element** or a **member** of the set. We often write out sets with curly braces and commas. For instance:

$$\{1, 2, 3\}$$

is the set containing 1, 2, and 3. We can write $1 \in \{1, 2, 3\}$ to denote that 1 is in the set, and we can also write $5 \notin \{1, 2, 3\}$ to denote that 5 is not in the set.

You can think about a set as a bag with a bunch of unique items in it. We don't care about the order in which you list the items in the bag; it will still contain the same items. We discard any duplicate items because all we care about is whether or not an item is in the set, not how many times a particular item is in the set. The next definition should clarify why this is the case.

Definition. Two sets A and B are **equal** if both of these are true:

- every element in A is also an element of B
- every element in B is also an element of A

Put simply, two sets are considered the same if they have exactly the same elements. This is why order doesn't matter; we can say

$$\{\text{ball}, \text{cookie}, \text{bottle}\} = \{\text{bottle}, \text{cookie}, \text{ball}\}$$

because the two sets have the exact same elements.

We can also construct sets using a rule to determine what elements will be in our set. This is also called **set-builder notation**.

Example. Let $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Let

$$T = \{x : x \in S \text{ and } x \text{ is even}\}.$$

What are the elements of T?

In English, the definition of T is saying, "T is made up of elements that are both in S and even." The part to the left of the colon tells us what to put in our new set, and the part to the right of the colon tells us the rule it needs to satisfy to end up in the new set. For the example, to find out what elements should be in T, we look at each element in S and put it in T if that element is even. Following this procedure, we see that $T = \{2, 4, 6, 8\}$. If, when constructing a set using set-builder notation, you put the same element into the set multiple times, just keep going and make sure to discard any duplicate elements at the end.

It turns out that there is a special set that contains no elements:

> **Definition.** The **empty set** contains 0 elements. We denote it as $\emptyset$ or $\{\}$.

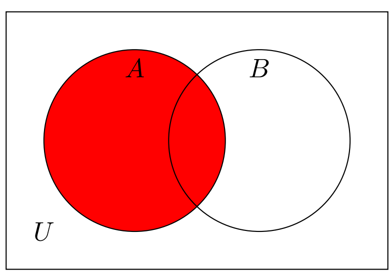
As we continue to add set definitions, properties, and operations, a good way to check your understanding is to consider how they relate to the empty set. The empty set often turns out to be a counterexample to many rules you may instinctively come up with.

It also turns out that sets can be infinite. These include some sets you are already familiar with:

> **Definition.** Here are some important sets:
> - The **natural numbers**: $\mathbb{N} = \{0, 1, 2, \ldots\}$
> - The **integers**: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
> - The **positive integers**: $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
> - The **rational numbers**: $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}^+\}$
> - The **real numbers**: $\mathbb{R}$ contains all the rational and irrational numbers

As you just saw with $\mathbb{Z}^+$, we can add a plus or minus to the end of these symbols to indicate that we want just the positive or negative ones. For example, $\mathbb{R}^-$ would be the negative reals.

Another common way of representing sets is with a **Venn diagram**. Here is an example:



The red circle represents the set A, the mostly-unfilled circle represents B, and the entire box represents the set U. Anything inside the red circle would be an element of A. Venn diagrams can provide a visual, intuitive way to represent sets, and they will help in demonstrating many of the set operations you will see very soon.

1.1 The Subset Relation

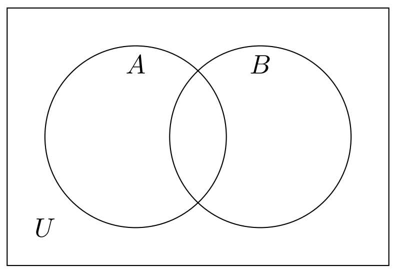
Remember the statement I was talking about earlier, that "all squares are rectangles, but not all rectangles are squares?" We can state this more formally with our set-theoretic language by saying that "the set of squares is a **subset** of the set of rectangles."

Definition. Let A and B be sets.

- A is a **subset** of B, notated $A \subseteq B$, if every element of A is an element of B.
- A is a **proper subset** of B, notated $A \subset B$, if $A \subseteq B$ and $A \neq B$.
- B is a **superset** of A, notated $B \supseteq A$, if $A \subseteq B$.
- B is a **proper superset** of A, notated $B \supset A$, if $A \subset B$.

Note that $\emptyset \subseteq S$ for any set S.

In the following Venn diagram, we can see that A and B are both subsets of U. Anything that is inside A or B is inside U, so any element of A or B is also an element of U.



It's important to understand the difference between a set being a *member* of another set and a set being a *subset* of another set. If we have $A \subseteq B$, this *does not* guarantee that $A \in B$. Similarly, if we have $A \in B$, then we *cannot* immediately conclude $A \subseteq B$.

The subset relation has a lot of interesting properties. For instance, say we have two sets, A and B, such that $A \subseteq B$ and $B \subseteq A$. This means that every element of A is an element of B, and every element of B is an element of A. I hope this sounds familiar; it's our definition of set equality! If $A \subseteq B$ and $B \subseteq A$, then it must be that $A = B$. In the next exercise, you'll explain why several other properties of the subset relation are true. Don't overthink them!

Exercise 1.1. Let A, B, and C be sets. Explain why each of the following are true:

1. $A \subseteq A$ (reflexivity).
2. If $A \subseteq B$ and $B \subseteq A$, then $A = B$ (antisymmetry - we just did this one).
3. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$ (transitivity).
4. If $A \subset B$, then $A \subseteq B$.

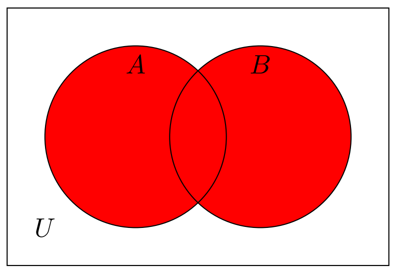
Due to properties 1, 2, and 3 from the exercise above, the subset relation ($\subseteq$) is a **partial order**. Don't worry about what that means just yet; we'll discuss relations and the properties they can possess later on. For now, just make sure you have a good intuitive understanding of why the above properties hold true for the subset relation.

1.2 Set Operations

The subset relation gave us a way to compare sets. We'll now look at some operations that we can use to generate new sets.

Definition. Let A and B be sets.
- The **union** of A and B, notated $A \cup B$, is the set containing every element that is in A, or B, or both.
- The **intersection** of A and B, notated $A \cap B$, is the set containing every element that is both in A and in B.
- If $A \cap B = \emptyset$, then we say A and B are **disjoint**.

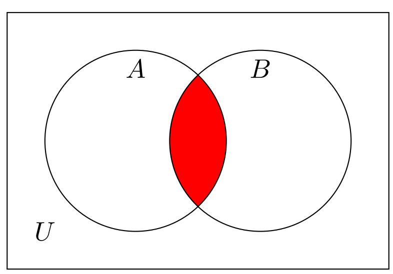
We can think of two sets as two bags with items in them. If you dump the contents of the two bags into a third bag, that third bag would be like the union of the two sets. We can also visualize the union of two sets with a Venn diagram:



The red region in the diagram covers anything that's in A or in B, so the region corresponds to $A \cup B$. Finally, let's also define the union of two sets with set builder notation:

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

The intersection of two sets contains the elements that the two sets have in common. Here is a Venn diagram representing intersection:



The red region where the circles overlap covers anything that's in both sets, so it represents $A \cap B$. I'll leave it to you to formally define intersection in the following exercise.

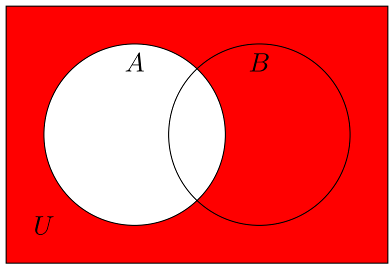
Exercise 1.2. Let A and B be sets. Define $A \cap B$, the intersection of A and B, using set-builder notation.

Here are a couple more operations we'll discuss:

Definition. Let A and B be sets.

- The **complement** of A, notated A^c, is the set containing every element (within some universal set) that is *not* in A.
- The **difference** of A and B, notated $A \setminus B$, is the set containing every element of A that is not in B.

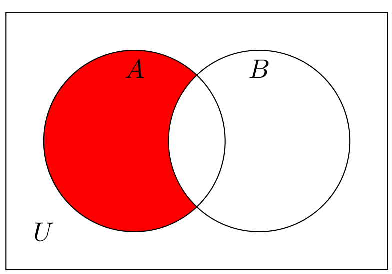
In some sense, the complement of a set is like the opposite or negation of a set. Here is a Venn diagram representing A^c:



You can see that everything outside of the circle representing A is shaded. In addition, the universal set, U, sort of places a bounding box on A^c. The reason we need to either implicitly or explicitly define some kind of universal set is that without it, the complement operation doesn't produce a well-defined set. A^c contains everything not in A, but we need a universal set to make it clear just what ”everything” means. With set-builder notation, A^c looks like this:

$$A^c = \{x : x \notin A \text{ and } x \in U\}.$$

The set difference operation essentially excludes any elements from the first set that are members of the second set. The following Venn diagram represents $A \setminus B$:



Here is $A \setminus B$ in set-builder notation:

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

Notice that we can express a set difference in terms of set complements.

Exercise 1.3. Let A and B be sets. Explain why $A \setminus B = A \cap B^c$.

Here is an example of these operators in action:

Example. Let $A = \{5, 8, 10\}$ and $B = \{3, 5, 10, 11\}$. Evaluate the following;

1. $A \cup B$
2. $A \cap B$
3. $B \setminus A$
4. $A \cap B^c$ (use $\mathbb{N}$ as the universal set here)

1: Putting all the elements of A and B together, we get the set $\{3, 5, 5, 8, 10, 10, 11\}$. After discarding duplicates, we end up with

$$A \cup B = \{3, 5, 8, 10, 11\}.$$

2: The elements which A and B have in common are 5 and 10. So, we have:

$$A \cap B = \{5, 10\}.$$

3: The elements which are in B but not in A are 3 and 11. Therefore, we have:

$$B \setminus A = \{3, 11\}.$$

4: B^c is the set of natural numbers excluding $3, 5, 10$, and 11. The only element that A shares with that set is 8. So,

$$A \cap B^c = \{8\}.$$

Now, here is a similar exercise for you to try:

Exercise 1.4. Let $A = \{2, 4, 6, 8\}$ and B equal the set of positive, even integers. Evaluate the following;

1. $A \cup B$.
2. $A \cap B$.
3. $A \setminus B$.
4. $A^c \cap B$ (use $\mathbb{Z}^+$ as the universal set here).

This exercise is more conceptual:

Exercise 1.5. Let A, B and C be sets. Explain why each of the following is true:

1. $A \cup \emptyset = A$.
2. $A \cap \emptyset = \emptyset$.
3. $A \cup B = B \cup A$ and $A \cap B = B \cap A$ (commutativity).
4. $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$ (associativity).
5. $A^c \cup B^c = (A \cap B)^c$ and $A^c \cap B^c = (A \cup B)^c$ (De Morgan's Laws)
6. $(A^c)^c = A$.
7. A and A^c are disjoint.

1.3 Sequences and the Cartesian Product

Hopefully, by now you've become more familiar with sets and understand that they are unordered and do not have duplicated elements. We'll now introduce a new structure that does not share those properties.

Definition. A **sequence** or **tuple** is an *ordered* list of objects. Unlike sets, a sequence can have repeated elements. We denote sequences using parentheses:

$$(1, 2, 1)$$

is the sequence containing 1, 2, and 1, in that order. A sequence with two elements is often referred to as an **ordered pair**.

To once again reinforce the difference between sequences and sets, the following are true:

$$(1, 2) \neq (2, 1)$$
$$\{1, 2\} = \{2, 1\}$$

Those statements should make it clear that order matters for sequences but not for sets.

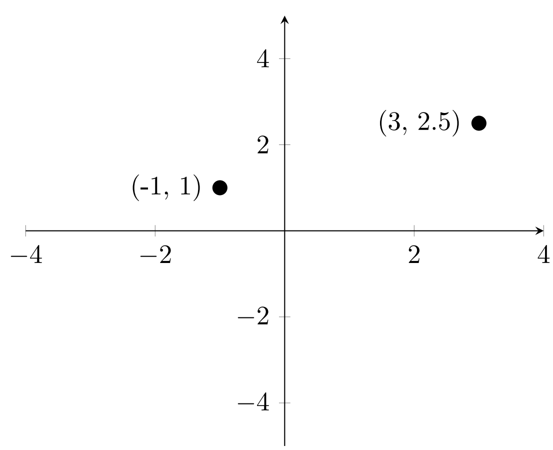
The reason we care about sequences is that they are generated by the next operation we'll discuss.

Definition. The **Cartesian product** of two sets A and B is defined as follows:

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}.$$

The Cartesian product of two sets is the set of all sequences where the first element is in the first set and the second set is in the second set.

You actually are intimately familiar with a certain Cartesian product of sets: $\mathbb{R} \times \mathbb{R}$, also known as $\mathbb{R}^2$. It's what the **Cartesian plane** helps us visualize:



Every point in the Cartesian plane, such as the ones labeled above, can be represented by an ordered pair. The set of all these ordered pairs is $\mathbb{R} \times \mathbb{R}$, since the x and y values in these ordered pairs can be any real numbers.

Let's consider a simpler example:

Example. Let $A = \{2, 4, 6\}$ and $B = \{1, 3, 5, 7\}$. Evaluate $A \times B$. Then evaluate $B \times A$.

The Cartesian product of A and B contains every sequence of length 2 where the first element is in A and the second element is in B. Here it is:

$$A \times B = \{(2, 1), (2, 3), (2, 5), (2, 7), (4, 1), (4, 3), (4, 5), (4, 7), (6, 1), (6, 3), (6, 5), (6, 7)\}$$

On the other hand, the sequences in $B \times A$ have something in B as the first element and something in A as the second:

$$B \times A = \{(1, 2), (1, 4), (1, 6), (3, 2), (3, 4), (3, 6), (5, 2), (5, 4), (5, 6), (7, 2), (7, 4), (7, 6)\}$$

Notice that $A \times B$ and $B \times A$ are not equal–in fact, they have the same sequences but in the opposite order. The fact that they aren't equal demonstrates that the Cartesian product operation is **not commutative**. The question of when $A \times B = B \times A$ is the subject of the next exercise.

Exercise 1.6. Let A and B be sets. When is $A \times B$ equal to $B \times A$?
(Hint: don't forget to consider the empty set)

Sometimes, you might see exponentiation of sets, like how we saw $\mathbb{R}^2$ earlier. This is just a shorthand for a repeated Cartesian product, with the exponent being the number of times to apply the product. To make it clear what this looks like, we'll first define the n-fold Cartesian product:

Definition. The **n-fold Cartesian product** of n sets $S_1, \ldots, S_n$ is defined as follows:

$$S_1 \times \ldots \times S_n = \{(x_1, \ldots, x_n) : x_i \in S_i \text{ for } i \in \{1, \ldots, n\}\}.$$

The resulting set contains all sequences of length n where the ith element of the sequence is in the ith set of the product.

Each sequence in the resulting set has one element from each of the sets in the order in which they were multiplied. So, we can understand $\mathbb{R}^n$ to be the set of all sequences that have n real numbers.

1.4 The Powerset

Definition. The **powerset** of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A. Note that the empty set and A are elements of $\mathcal{P}(A)$.

The powerset's elements are the subsets of the set it came from. Since every set is a subset of itself, and the empty set is a subset of every set, both of those are members of the powerset. Let's look at an example:

Example. Let $A = \{1, 2, 3\}$. What is $\mathcal{P}(A)$?

A good, systematic way to write out the powerset is to list out every subset of size 0, then 1, and so on. Proceeding in this fashion, we get:

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

We'll end this short section with an exercise:

Exercise 1.7. Let A be a set. Explain why $\mathcal{P}(A)$ always has more elements than A.

1.5 Cardinality

Having a way to describe the size of a set is useful. For finite sets, defining this is easy:

Definition. The **cardinality** of a set A, denoted $|A|$, is the number of elements in the set. The cardinality of the empty set is 0.

For instance, the cardinality of the set $\{3, 6, 9\}$ is 3. Let's do a slightly more involved example.

Example. If S is the set containing all the characters that appear in the string "MISSISSIPPI", what is $|S|$?

It might be tempting to just count the number of letters in the string and stop there, but that isn't quite correct. Attempting to construct S gives us {M, I, S, S, I, S, S, I, P, P, I}, but when we remove duplicates, we are left with only {M, I, S, P}. Thus, the cardinality of S is 4. Now, try this exercise:

Exercise 1.8. Let A and B be sets. When is $|A \cup B| = |A| + |B|$ a true statement?

There are two other important properties of cardinality that we will discuss.

Example. Let A and B be finite sets. Then, $|A \times B| = |A| \cdot |B|$.

For each a in A, there are $|B|$ elements in B we can pair it up with, so there are $|B|$ sequences that have a as the first element. Repeating this for each of the $|A|$ elements of A gives us a total of $|A| \cdot |B|$ sequences. You might be wondering if perhaps we need to eliminate duplicates. However, through this process, it is impossible to get duplicates. To get two copies of some sequence, say (a, b), would require two copies of a in A or two copies of b in B, which can't be the case because sets don't have duplicate elements. Try working through the following to confirm that this identity holds.

Exercise 1.9. Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Evaluate $A \times B$ and verify that $|A \times B| = |A| \cdot |B|$.

We can also say something about the cardinality of the powerset:

Example. Let A be a finite set. Then $|\mathcal{P}(A)| = 2^{|A|}$.

The idea here is that for any subset of A, every element of A can either be in that subset or not in that subset. For a set of size 2, you get $4 = 2^2$ elements in the powerset since there are 4 ways to choose a subset–there are two options for the first element (whether it is in the subset or not) and you multiply that by the two options for the second element. For a set with n elements, you similarly multiply 2 by itself n times, representing the n choices you can make. Verify the identity holds in the following exercise:

Exercise 1.10. Let $A = \{4, 6, 8\}$. Evaluate $\mathcal{P}(A)$ and verify that $|\mathcal{P}(A)| = 2^{|A|}$.

1.6 Sets Review

Make sure you understand each of the following concepts, symbols, and terms:

- set
- $\in$ (membership)
- $\notin$
- set equality
- set-builder notation
- $\emptyset$ (empty set)
- $\mathbb{N}$ (natural numbers)
- $\mathbb{Z}$ (integers)
- $\mathbb{Z}^+$ (positive integers)
- $\mathbb{Q}$ (rational numbers)
- $\mathbb{R}$ (real numbers)
- Venn diagram
- $\subseteq$ (subset)
- $\subset$ (proper subset)
- $\supseteq$ (superset)
- $\supset$ (proper superset)
- $\cup$ (union)
- $\cap$ (intersection)
- disjoint
- A^c (complement)
- $\setminus$ (set difference)
- sequence
- $\times$ (Cartesian product)
- $\mathcal{P}(A)$ (powerset)
- $|A|$ (cardinality)
- $|A \times B| = |A| \cdot |B|$
- $|\mathcal{P}(A)| = 2^{|A|}$

1.7 Extension - Sets and Comprehensions in Python

The Python programming language has a set data structure built in. This data structure is an unordered collection of unique values and supports several set operations.

In the following snippet, you can see it in action. First, a set called A is initialized with the curly brace syntax. The duplicate zero will be automatically removed. Then, in line 3, we attempt to add the element 3 to A, and it will be added since it was not previously in the set. After that, we create a new set called B by applying the set function to the list $[2, 3, 4]$. Finally, we print the union of A and B and the intersection of A and B.

```
1  A = {0, 0, 1, 2}
2  # A = {0, 1, 2}
3  A.add(3)
4  # A = {0, 1, 2, 3}
5  B = set([2, 3, 4])
6  print(A | B) # A union B
7  # {0, 1, 2, 3, 4}
8  print(A & B) # A intersect B
9  # {2, 3}
```

Python also supports **comprehensions**, which are very similar to set-builder notation. You can use them to generate lists or sets, and it is not uncommon to see list comprehensions show up in codebases.

In the following snippet, we start with a list, A, and then construct a list B to contain the square of each of the elements of A using a list comprehension. After that, we construct a set C to contain the square of the elements of A using a set comprehension. Notice the similarity to set-builder notation–the `x*x` to the left of the `for` is what actually ends up in the data structure, and the `x in A` afterward is the rule used to select elements.

Starting in line 9, we define two new sets, S and T, and then use a set comprehension to create the Cartesian product of the two sets.

```
1  A = [1, 2, 3, 3]
2
3  B = [x*x for x in A] # list comprehension
4  # B = [1, 4, 9, 9]
5
6  C = {x*x for x in A} # set comprehension
7  # C = {1, 4, 9}
8
9  S = {1, 2, 3}
10 T = {4, 5}
11 StimesT = {(x, y) for x in S for y in T}
12 # StimesT = {(2, 4), (3, 4), (1, 5), (1, 4), (2, 5), (3, 5)}
```

1.8 Extension - Axiomatic Set Theory

Among other things, Bertrand Russell was a famous mathematician and logician who made contributions to set theory. One such contribution is known as **Russell's Paradox**:

Definition. Let A be defined as the set that contains all sets that are not members of themselves. That is,

$$A = \{x : x \notin x\}.$$

Then, consider whether A is an element of itself. This leads to a contradiction, because $A \in A$ implies $A \notin A$ and $A \notin A$ implies $A \in A$.

If A is an element of itself, then it should not be an element of itself since A is supposed to contain the sets which do not have themselves as elements. If A is not an element of itself, then it should be an element of itself for the same reason. In mathematics, the reason we adopt axioms and prove theorems rigorously is specifically to avoid strange paradoxes like this, which is why we need an **axiomatic set theory**.

Mathematicians had been operating under the **axiom of unrestricted comprehension**, which allowed them to define a set using any arbitrary rule. This is what allowed them to create the set that results in Russell's Paradox. However, this axiom is clearly problematic. Instead, we choose to adopt the **axiom of restricted comprehension**:

Definition. The **axiom of restricted comprehension** states that if A is a set, then B is a set if

$$B = \{x : x \in A \text{ and } P(x)\}$$

where $P(x)$ is a **predicate**, which can be likened to a function that takes in a variable and returns true or false.

The restriction is that you can choose a *subset* of a set using any arbitrary rule. If you recall when we defined set complements, we spoke of a universal set–the reason we need such a set is because the axiom of restricted comprehension requires it.

There are several different axiomatic set theories, but by far the most widely used is **ZFC Set Theory**, which stands for Zermelo-Fraenkel Set Theory with the addition of the Axiom of Choice. Some of the axioms include the axiom of extensionality, which defines set equality, the axiom of union, which says that the union of a set of sets is a set, and the axiom of the powerset, which defines the powerset. We won't go through all of them, but it is important to understand that all of the tools and theorems of set theory ultimately derive from some basic axioms.

1.9 Extension - Quantifiers in Code

Here, we'll try to provide another perspective on evaluating the truth of quantified expressions. Here, we define the predicate $P(x)$ in lines 1 and 2 to be true if x is even and false otherwise. We then define the set A. We are interested in the quantified expression,

$$\forall x \in A.P(x),$$

which we evaluate the truth of in lines 6 through 8. We start with `result` being `True` and check each element of A one at a time. If any of them were to be odd, then in line 8, we `and` the current value of `result` with `False` and so `result` would be set to `False`.

Line 11 does the same thing in one line–it uses `map`, which applies P to each element in A and then `all` returns `True` if all values are even.

```
1  def P(x):
2      return x%2 == 0
3
4  A = {2, 4, 6, 8}
5
6  result = True
7  for element in A:
8      result = result and P(element)
9  # result is True
10
11 result = all(map(P, A))
12 # result is True
```

Here is another example with the same predicate but a different set. We're interested in the following quantified expression:

$$\exists x \in A.P(x).$$

In line 6 we start with `result` being `False` since we're using an existential quantifier. Then, we look at each element in A and if any of them are even, we `or` the value of `result` and `True` in line 8.

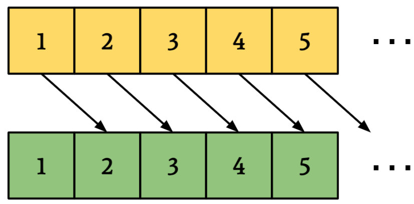
In line 11, we can accomplish the same thing. We use `any`, which will return `True` if, when we `map` the predicate P to the set A, any of the values are even.

```
1  def P(x):
2      return x%2 == 0
3
4  A = {1, 2, 3, 5}
5
6  result = False
7  for element in A:
8      result = result or P(element)
9  # result is True
10
11 result = any(map(P, A))
12 # result is True
```

1.10 Extension - Cardinality of Infinite Sets

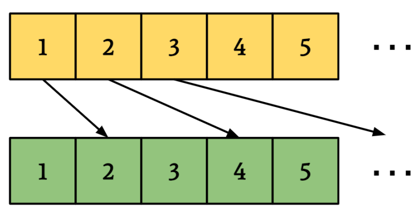
The mathematician David Hilbert came up with a thought experiment centered around an imaginary hotel called the Grand Hotel. The Grand Hotel has an infinite number of rooms, and currently, every room is occupied. A customer walks into the hotel and asks for a room–is there any way to accommodate this customer?

As a matter of fact, there is. Have the person who was staying in room 1 move to room 2, then have the person who was staying in room 2 move to room 3, and so on. The person who was in room n will now be in room $n + 1$.



This process creates a vacancy in room 1 that our new customer can occupy. In general, if we have k new arrivals, where k is some natural number, we could move the person in room n to room $n + k$ and have enough spaces to occupy the new customers.

Ok, we can handle any finite number of new arrivals–but what if we have an *infinite* number of new customers? As a matter of fact, we can deal with that scenario as well! Have the person in room 1 go to room 2, have the person in room 2 go to room 4, and in general, have the person in room n go to room $2n$.



Now, even odd-numbered room is unoccupied, and there are an infinite number of odd numbers, so our new guests have a place to stay.

So, what's going on here? These kinds of manipulations clearly wouldn't work for a hotel with a finite number of rooms. The set of guests who were present at the beginning is a proper subset of the set of guests we have at the end after shuffling everyone around, and yet, every room was full before and every room is full at the end. In some sense, the set of guests before and after are the same size, since they both completely occupied the rooms of the hotel, and the number of rooms did not change.

It seems that infinite sets don't work quite the same way as finite sets, and we need a different definition of cardinality that will work for them. In fact, this definition of cardinality will work for all sets.

Definition. Let A and B be sets. They have the same **cardinality**, that is,

$$|A| = |B|,$$

if and only if there exists a bijective function from A to B. We say that

$$|A| \leq |B|$$

if and only if there exists an injective function from A to B.

Essentially, we are trying to "match up" the elements of two sets, and if we can do this, they have the same cardinality. Two finite sets will only have the same cardinality when they have exactly the same number of elements so that you can match them up, one by one. If one set is bigger, then there will be some elements left over that are unmatched.

As we saw with the Grand Hotel, we could create a bijective function between the set of positive integers and the set of even positive integers (map each integer to twice its value), so they have the same cardinality. This is true even though the set of even positive integers is a proper subset of the set of positive integers. We can also create a bijection from the natural numbers to the positive integers (map n to $n+1$).

Definition. An infinite set A is **countably infinite** if $|\mathbb{N}| = |A|$.
An infinite set B is **uncountable** if $|\mathbb{N}| \neq |B|$.

Countable sets include the positive integers, the rational numbers, and $\mathbb{N} \times \mathbb{N}$. Uncountable sets include $\mathcal{P}(\mathbb{N})$ and the real numbers. A nice proof for why the real numbers are uncountable is called **Cantor's diagonalization argument**.

First, note that the open interval $(0, 1)$ has the same cardinality as $\mathbb{R}$ since an arctan-like function provides a bijection between them. So, it will suffice to show that there is no bijective function from $\mathbb{N}$ to $(0, 1)$. For contradiction, assume that we have some bijective function f from $\mathbb{N}$ to $(0, 1)$. Then, we can construct a table like the one below, where to the right of the equal sign, you have the decimal representation of some real number in $(0, 1)$.

$$\begin{array}{ccccccc}
f(0) & = & .a_{00} & a_{01} & a_{02} & a_{03} & \cdots \\
f(1) & = & .a_{10} & a_{11} & a_{12} & a_{13} & \cdots \\
f(2) & = & .a_{20} & a_{21} & a_{22} & a_{23} & \cdots \\
f(3) & = & .a_{30} & a_{31} & a_{32} & a_{33} & \cdots \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Let b be the number represented by the decimal $.b_1 b_2 b_3 \ldots$ where $b_i = 3$ if $a_{ii} = 2$ and $b_i = 2$ otherwise. So, for all i, we have $b_i \neq a_{ii}$. We have constructed a number b based on the diagonal of the table in such a way that b cannot possibly be in any row of the table. If you were to claim, for instance, that $f(489) = b$, I would point out that $b_{489} \neq a_{489,489}$ by construction, so b cannot be in that row. By the same argument, b cannot be in any row of the table. However, this means that b is a real number in $(0, 1)$ that f cannot reach, so we have a contradiction since f is supposed to be surjective. Thus, it is not possible to have a bijection between $\mathbb{N}$ and $(0, 1)$, so $|\mathbb{N}| \neq |\mathbb{R}|$.

1.11 Extension - Cantor's Theorem

In this section, we'll do what I think is a pretty clever proof.

Definition. (Cantor's Theorem) Let A be a set. Then,

$$|A| < |\mathcal{P}(A)|.$$

The cardinality of a set is always strictly less than the cardinality of its powerset.

Proof. There are two things we need to show here. First, to show that $|A| \leq |\mathcal{P}(A)|$, we need to find an injective function from A to its powerset. This is quite simple–just map any element x to $\{x\}$.

Second, we need to show that $|A| \neq |\mathcal{P}(A)|$. For this, we need to prove that there is no surjective function from A to $\mathcal{P}(A)$. We proceed by contradiction, and assume that there is some surjective function $f : A \mapsto \mathcal{P}(A)$. The function maps elements of A to subsets of A.

We define a set B as follows:

$$B = \{a : a \notin f(a)\}.$$

If f maps an element a to a subset of A that does not contain a, then we put a in B. Since f is surjective, and $B \in \mathcal{P}(A)$, then there must be some element $x \in A$ such that $f(x) = B$.

Now, consider whether x is in B. If $x \in B$, then this implies that $x \notin B$ since B contains elements that do not map to subsets that contain them. If $x \notin B$, then this implies that $x \in B$ since x maps to a subset that doesn't contain it. This is a contradiction, and it must be that f was not surjective in the first place since no element can map to B.

Since we have shown $|A| \leq |\mathcal{P}(A)|$ and $|A| \neq |\mathcal{P}(A)|$, we can conclude $|A| < |\mathcal{P}(A)|$. $\square$

1.12 Citation

This is a citation[1].

References

[1] H. Ren, "Template for math notes," 2021.