1. Sets and Ordered Collections

Sets

A set is an unordered collection of distinct objects. *Unordered* is to say that order is irrelevant—two sets are considered to be equal when they contain the same elements. E.g., $\{1, 2, 3\}$ is the same set as $\{3, 2, 1\}$. *Distinct* means that a set cannot contain duplicates. For this reason, $\{1, 1, 2, 3\}$ is either not a set at all, or otherwise denotes the set $\{1, 2, 3\}$, depending on how you feel about it. (A set-like collection which is allowed to contain duplicates is called a *multiset*, or *bag*.)

Terminology and notation

We refer to the objects in a set as its *elements* (or sometimes *members*). If a is an element of S, we use the notation $a \in S$. Conversely, $b \notin S$ means that b is not in S. Using, so called, *set-builder* style, we write $\{s \in A \mid P(s)\}$ for the set of all elements $s \in A$ such that $P(s)$ holds, where P is some *predicate* on the set A, i.e., a boolean function $A \rightarrow \{true, false\}$. For example, $\{p \in \mathbb{N} \mid p \text{ is prime}\}$ is the set of all prime numbers. Set builder notation is similar to the list comprehension syntax available in some programming languages. Here is an example in Haskell code, where the predicate is `odd`—a function we can think of here as having type `Int -> Bool`.

```
[ x | x <- [1..100], odd x ]    -- Odd integers in the range 1 .. 100
```

Popular sets

$\mathbb{Z}$ is the set of integers. $\mathbb{N}$ is the set of all natural numbers $\{1, 2, 3, ...\}$. Sometimes, particularly in computer science, $\mathbb{N}$ is taken to also include zero. Because of this ambiguity, some authors prefer to use $\mathbb{Z}_+$ for the *positive integers*, and $\mathbb{Z}_{\geq 0}$ for the set of all *non-negative integers*. $\mathbb{Q}$ is the set of rational numbers, i.e., all numbers of the form $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. $\mathbb{R}$ is the set of real numbers, i.e., all rational and irrational numbers. To give a rigorous construction for $\mathbb{R}$ requires some more work. One way is to "complete" the set $\mathbb{Q}$ by adding in all possible limits of *Cauchy sequences* of rational numbers.

Both $\mathbb{R}$ and $\mathbb{Q}$ form, what is known as, *totally ordered fields*, but what makes the real numbers stand apart is that they satisfy an important property, known as *Dedekind completeness*. This property guarantees that any non-empty set of real numbers, for which there exists an *upper bound*, also has a *least upper bound* in $\mathbb{R}$. To see why this doesn't work for the set $\mathbb{Q}$, consider the set $\{x \in \mathbb{Q} \mid x^2 \leq 2\}$. The least upper bound of this set is $\sqrt{2}$, which is not a rational number. Finally, we say that the set $\mathbb{Q}$ is *dense* in the reals, which means that for any number $r \in \mathbb{R}$, either r is in $\mathbb{Q}$, or for every $\epsilon > 0$, there exists a number $q \in \mathbb{Q}$, such that $|q - r| < \epsilon$. That is, if r is not itself a rational number, then it is "arbitrarily close" to one.

Sizes of sets

Sets can be either *finite* or *infinite*. The sets $\{1, 2, 3\}$, $\{n \in \mathbb{N} \mid n < 5\}$, and $\{a, b, ..., z\}$ are all finite sets. The set of all natural numbers, $\mathbb{N} = \{1, 2, 3, ...\}$ is infinite and so is $\{x \in \mathbb{R} \mid 0 < x < 1\}$.

Since sets are identified by their members, there is exactly one *empty set*, usually denoted by the symbol $\varnothing$. The *cardinality* of a set is a measure of its size. For a finite set, it is just the number of its elements. If S is a set, then the cardinality of S is denoted $|S|$. For example, $|\{3,9\}| = 2$. Sets with only one element are called *singleton* sets. To show that two infinite sets have the same cardinality, one needs to produce a *bijection* (one-to-one correspondence) between the two sets. For instance, $|\{1,2,3,...\}| = |\{2,3,4,...\}|$. The bijection here is the map $x \mapsto x+1$.

For a fun thought experiment related to infinite sets, see Hilbert's Hotel:
https://en.wikipedia.org/wiki/Hilbert%27s_paradox_of_the_Grand_Hotel.

Subsets, Supersets and the Power Set

A set A is a *subset* of B, denoted $A \subseteq B$, if all elements of A are also elements of B. The empty set is a subset of every set, including itself. If A is a subset of B, then B is a *superset* of A. A *proper subset* of a set B is a subset which, at the same time, is not equal to B. We write $A \subset B$ to denote the fact that A is a proper subset of B. For finite sets, a proper subset is always strictly smaller than its parent. With infinite sets, things are more complicated. For example, the integers $\mathbb{Z}$ is a proper subset of the rational numbers $\mathbb{Q}$, but one can easily come up with a bijection between the two sets, hence they have the same cardinality.

The set of all subsets of a set A is called the *power set* of A and is usually denoted $\mathcal{P}(A)$ or 2^A. For example, let $S = \{1,2,3\}$. Then $\mathcal{P}(S) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. (Recall that the empty set is a subset of every set.) *Bonus question:* Can you see why the notation 2^A is sometimes used when referring to the power set of A?

Infinity and beyond

Infinite sets can be either *countable* or *uncountable*. All countable infinite sets have the same cardinality as the set of natural numbers.

> *A set is countably infinite if its elements can be put in one-to-one correspondence with the set of natural numbers. In other words, one can count off all elements in the set in such a way that, even though the counting will take forever, you will get to any particular element in a finite amount of time.* (from mathinsight.org)

That is, a countable set is either

- finite, or
- has the same size as $\mathbb{N}$.

However, all infinite sets are not countable. In particular, the real numbers form, what is known as, a *continuum* and cannot be put in one-to-one correspondene with $\mathbb{N}$. If we attempt to label the real numbers, one by one, using the natural numbers $\{1,2,3,...\}$, $\mathbb{R}$ will "outnumber" $\mathbb{N}$. To show why this is the case; assume it would be possible to create a list of all real numbers between 0 and 1, indexed by $\mathbb{N}$. Such a list could then look something like the following (arbitrarily ordered):
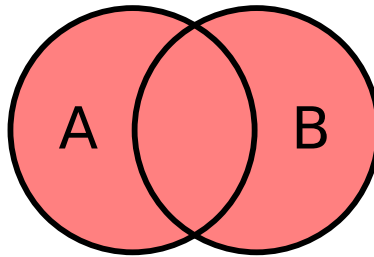
List position	Real number
10	0.000000000100000000000000000000000000000000000000...
128931	0.500000000000000000000000000000000000000000000...
583910	0.4142135623730950488016887242096980785696671875...
3291293	0.5151515151515151515151515151515151515151515151515...
78481839	0.7182818284590452353602874713526624977572470933...
948118319	0.1415926535897932384626433832795028841971693999...
⋮	⋮

Ordered by the naturals, we will instead denote these numbers as $0.d_{n1}d_{n2}d_{n3}...$, with n being the row number. We then get a list:

List position	Real number
1	$0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}d_{17}d_{18}d_{19}$ ...
2	$0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}d_{27}d_{28}d_{29}$ ...
3	$0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}d_{37}d_{38}d_{39}$ ...
⋮	⋮
n	$0.d_{n1}d_{n2}d_{n3}d_{n4}d_{n5}d_{n6}d_{n7}d_{n8}d_{n9}$ ...
⋮	⋮

Now imagine that we define a real number m as,

$$m = 0.(d_{11} + 1)(d_{22} + 1)(d_{33} + 1)(d_{44} + 1)(d_{55} + 1)(d_{66} + 1)...(d_{nn} + 1)...$$

We think of addition here as being modulo 10, so $9 + 1 = 0$. If our list, in fact, contains all real numbers, certainly m would appear in some position, say p. But what is this number p? It cannot be 1, since m differs from this number in the first decimal after the radix point ($d_{11} \neq d_{11} + 1$). It cannot be the second number either, since $d_{22} \neq d_{22} + 1$. Actually, it can't be any number in the list. Each row n fails to match m in the nth decimal of its fractional part. This tells us that a list like this cannot be constructed. The real numbers are simply too many.

The above proof is known as *Cantor's diagonalization argument.* In computer science, a similar technique can be used to show that the *Halting problem* is unsolvable. That is, to show that there is no effective procedure which will determine, for an arbitrary program, whether that program will terminate (halt) or continue to run forever.

The cardinality of the natural numbers is the smallest infinite cardinality. In the *transfinite cardinal* number system, it is written $\aleph_0$ (aleph-null). The cardinality of the real numbers is usually denoted $\mathfrak{c}$ (for continuum). According to Cantor's *continuum hypothesis*, there are no cardinalities of infinity strictly in between $\aleph_0$ and $\mathfrak{c}$. This would, in other words, mean that $\aleph_1 = \mathfrak{c}$.

Ordered structures

An n-tuple is an orderd collection, or *sequence* of n objects, i.e., a collection in which order matters. Tuples are represented using the notation $(a_1, a_2, ..., a_n)$ or sometimes with angle brackets: $\langle a_1, a_2, ..., a_n \rangle$. A 2-tuple is more commonly known as a pair.

Equality of ordered n-tuples

Two n-tuples $\langle a_1, a_2, ..., a_n \rangle$ and $\langle b_1, b_2, ..., b_n \rangle$ are equal if (and only if) $a_i = b_i$, for all $i : 1 \leq i \leq n$.

Operations on sets

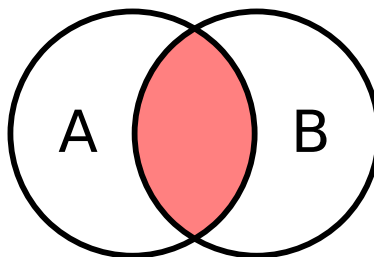Sets can be combined in different ways to produce other sets. Here are some of the most common operations on sets.

Union

The *union* $\cup$ of two sets A and B is the set of all elements either in A or B (or both).
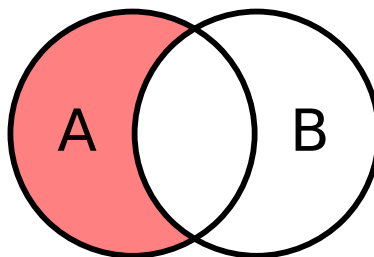
$$A \cup B = \{s \mid s \in A \text{ or } s \in B\}$$

Intersection

The *intersection* $\cap$ of two sets A and B is the set of all elements which appear in both A and B.

$$A \cap B = \{s \mid s \in A \text{ and } s \in B\}$$

Complement and set difference

The difference of two sets A and B, also called the *relative complement* of B in A, and written $A\backslash B$ (or sometimes $A - B$) is the set of all elements in A, except those that are also in B.

$$A\backslash B = \{s \mid s \in A \text{ and } s \notin B\}$$

So, for example, we can write the set of all irrational numbers as $\mathbb{R}\backslash\mathbb{Q}$. Note that, in general, $A\backslash B \neq B\backslash A$. In other words, the set difference operation is not *commutative*.

Sometimes one considers all sets to be defined in a specific *universe*, such as the integers. If a set A belongs to a universe U, the *absolute complement* of A, written A' or A^c, is the relative complement of A with respect to that universe, i.e., $U\backslash A$.
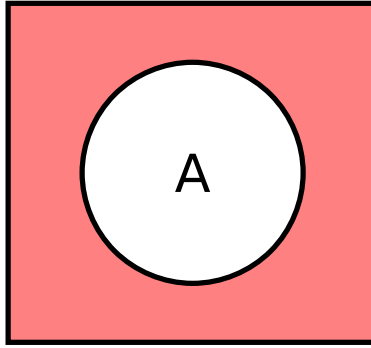
Cartesian product

The *cartesian product* of two sets A and B, written $A \times B$, is the set of all pairs $\langle a, b \rangle$, where a and b are elements of the sets A and B respectively. That is,

$$A \times B = \{\langle a, b \rangle \mid a \in A, b \in B\}.$$

For any set A : $A \times \varnothing = \varnothing = \varnothing \times A$. Just like the set-theoretic difference, the cartesian product is not commutative. Specifically, $A \times B$ is not equal to $B \times A$, unless

- $A = B$, or
- either A or B is the empty set $\varnothing$.

The cartesian product generalizes to more than two sets, so that

$$S_1 \times S_2 \times \cdots \times S_n = \{\langle s_1, s_2, \ldots, s_n \rangle \mid s_i \in S_i, 1 \leq i \leq n\}.$$

Russell's paradox

George Cantor's early set theory ran into trouble back in 1901, when Bertrand Russel showed it to be inconsistent. In what we now refer to as *naive* set theory, pretty much anything that can be written as a set comprehension is considered a set. Now, let, $R = \{x \mid x \notin x\}$. That is, R is defined to be the set of all sets who are not members of themselves. From this, it follows that R is a member of itself precisely when $R \notin R$. A contradiction! As a result of this, axiomatic set theories were developed, such as the Zermelo-Fraenkel set theory. Today, ZFC (where the C refers to the *Axiom of Choice*) serves as a standard foundation of mathematics.

To put in more practical terms, we have to be careful when talking about sets of other sets. In particular, there is no "set of all sets." In axiomatic set theory, this would instead be referred to as a *proper class*.

A popular version of Russel's paradox, which doesn't involve set-theoretic terminology, is the *Barber paradox* (although it isn't really a paradox):

> *There is a town and in this town there is a barber. The barber shaves all those men in this town who do not shave themselves, and only those men. Then, who shaves the barber?*

The following is a program written in Haskell, which is trying to determine whether the barber shaves himself. It includes a recursion guard to terminate the program after a certain number of steps.

```haskell
module Main where

import Control.Monad.State.Strict

data Townsman = Customer | SelfShaver | Barber

-- The barber shaves precisely those men in town who do not shave themselves.
barberShaves :: Townsman -> State Int Bool
barberShaves man = do
    (stopAfterSteps 300 "not (not (not (not (not ... Too much recursion, guy!")
    liftM not (shavesHimself man)

-- Given a type of man, does this man shave himself?
shavesHimself :: Townsman -> State Int Bool
shavesHimself SelfShaver = return True
shavesHimself Customer   = return False
shavesHimself Barber     = barberShaves Barber

-- Recursion guard to prevent infinite loops.
stopAfterSteps :: Int -> String -> State Int ()
stopAfterSteps n msg = do
    a <- get
    if a > n
        then error msg
        else put (succ a)

askWhether :: Num s => t -> (t -> State s a) -> a
askWhether a b = evalState (b a) 0

main :: IO ()
main = print
    ( askWhether Customer shavesHimself
    , askWhether SelfShaver shavesHimself
    , askWhether Barber shavesHimself )
```