Note 0: Mathematical Foundations

CS 70, Summer 2024

1 Sets

Definition

The foundations of mathematics lie in the theory of *sets*. Much work can be done in rewriting mathematical theories in terms of their set-theoretic foundations, or in developing the rules that govern sets—and as a result govern all of mathematics. As beautiful as this theory may be, it is not something we will concern ourselves *too* much with—we will take sets somewhat as granted, and will work through our mathematics without dwelling too much on its set-theoretic foundations. We will not, for example, write down the rules of numbers in terms of the underlying set theory rules. However, sets, ineluctable objects as they are, show up all throughout mathematics, and as such it would behoove us to understand them well.

A set is well-defined collection of objects, where the qualifier "well-defined" means "defined in a way that doesn't create issues for us." More on that later. The objects in a set are called its **elements** or its **members** and they can be anything—numbers, letters, people, cities, and even other sets. Conventionally, we denote sets with capital letters (e.g., S, T, X, Y, etc.).

Sets can be described in words or defined by listing their elements and surrounding the list with curly braces. For example, we can describe the set A to be the set whose members are the first five prime numbers, or we can explicitly define $P = \{2, 3, 5, 7, 11\}$. We indicate set membership using the $\in$ and $\notin$ symbols: $x \in A$ for any x which is an element of A and $x \notin A$ for any x which is not an element of A. For example, $2 \in P$ and $1 \notin P$ for the earlier described set P of the first five prime numbers. Two sets A and B are said to be **equal**, written $A = B$ if they have the same elements. The order and repetition of the elements do not matter, so

$$\{\text{red}, \text{white}, \text{blue}\} = \{\text{blue}, \text{white}, \text{red}\} = \{\text{red}, \text{white}, \text{white}, \text{blue}\}.$$

Often, we will need to define more complicated sets than those which can be defined by just listing the elements. To do so, we will use *set-builder notation.* Set-builder notation defines sets by demonstrating the properties that its elements must satisfy. In set-builder notation, we write a pair of curly brackets; on the left-hand side, we describe the relevant domain of objects, and on the right-hand side, we explain which properties they must satisfy. The left- and right-hand sides are joined together by a colon or bar, which is typically read as "such that." For example, $\mathbb{N}^+ = \{n \in \mathbb{N} : n > 0\}$ would be read as "the set of all natural numbers such that the number is positive," or, more simply, "the set of positive natural numbers."

This notation is flexible. For example, the set of rational numbers, denoted $\mathbb{Q}$, would usually be written as

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \text{ are integers and } b \neq 0 \right\}.$$

In English, this is read as "the set of all fractions such that the numerator is an integer and the denominator is a nonzero integer." The following is an equivalent notation of the rational numbers in set-builder notation:

$$\mathbb{Q} = \left\{ q : q = \frac{a}{b} \text{ where } a, b \text{ are integers and } b \neq 0 \right\}.$$

We must be careful about using set-builder notation, since it can lead us to problems; specifically the kinds of problems we are trying to avoid by saying that a set is a "well-defined" collection of objects. For example, consider the set

$$R = \{A : A \text{ is a set and } A \notin A\}.$$

Is R well-defined? Think about it. In particular, consider whether $R \in R$ or $R \notin R$. This set of all sets which are not members of themselves is quite famous for tearing down an early attempt to formalize the theory of mathematics. It is because of this set that sets can contain anything except one thing—themselves.

Cardinality

We can also talk about the size of a set, or its **cardinality**. The cardinality of a set is naturally thought of as the number of distinct elements in the set. For $P = \{2, 3, 5, 7, 11\}$ from before, the cardinality of P, denoted $|P|$, is 5. We require that equal sets have equal cardinality, so cardinality counts distinct elements. For example, $|\{0, 1, 1\}| = 2$, since we know that the set $\{0, 1, 1\}$ only has two distinct elements.

It is possible for the cardinality of a set to be 0. The set with cardinality zero is known as the empty set, typically denoted by $\varnothing$ or $\{\}$. It is possible to show that the empty set is unique; that is, there is only one set with a cardinality of 0. Sets can also be infinite. For example, the set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots, \}$ is infinite. So are the sets of integers, prime numbers, and odd numbers.

Subsets

Another way we might think about the "size" of sets would be by looking at which elements they share in common. In particular, if every element of a set A is also an element of set B, we say that A is a **subset** of B, written $A \subseteq B$. We can equivalently say that B is a **superset** of A, written $B \supseteq A$.

A **proper subset** is a set that is strictly contained in the original set. That is, if every element of A is also an element of B and A has fewer elements than B, then A is a proper subset of B, written $A \subset B$. Proper supersets are defined analogously. For example, for $B = \{1, 2, 3, 4, 5\}$, we have that $\{1, 2, 3\}$ is both a subset and a proper subset. However, $\{1, 2, 3, 4, 5\}$ is a subset but not a proper subset.

Below are some basic properties regarding subsets.

- The empty set is a proper subset of any nonempty set. That is, for a set $A \neq \varnothing$, we have that $\varnothing \subset A$.
- The empty set is a subset of any set. That is, for any set A, we have that $\varnothing \subseteq A$.
- Every set is a subset (and not a proper subset) of itself. That is, for any set A, we have that $A \subseteq A$.

Noteworthy Sets

In mathematics, some sets are referred to so commonly that they are denoted by special symbols. Below we list a few.

- The **natural numbers** $\mathbb{N}$. We will not concern ourselves with defining the natural numbers, and take for granted that they are $\mathbb{N} = \{0, 1, 2, 3, \ldots, \}$.
- The **integer numbers** $\mathbb{Z}$. We write the integers as $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, where it is typically assumed that we understand what they are (i.e., we know what -1 is).

  However, for the sake of proof and disproof, the integers are defined as the set of differences between natural numbers:
  $$\mathbb{Z} = \{n - m : n, m \in \mathbb{N}\}.$$
  This definition is useful for proving or disproving that something is an integer.
- The **rational numbers** $\mathbb{Q}$. Like the integers, it is assumed we understand what they are. Unlike the integers, we can't quite enumerate them as a set.

  Thus the rational numbers are almost always written in terms of their definition: the set of well-defined ratios of the integer numbers.
  $$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}.$$
- The **real numbers** $\mathbb{R}$. Again, it is assumed we understand what they are, and we will not dwell too much on defining what they are.

  For those who are interested: the real numbers are defined by the rational numbers around them. In particular, a number x is real if we can find two sets L and R which partition the rationals such that $x > \ell$ for all $\ell \in L$ and $x \leq r$ for all $r \in R$. Such partitions are known as "Dedekind cuts."

Operations

We can perform operations on and between sets to get new sets. The **intersection** of a set A with a set B, written as $A \cap B$ is the set containing all elements that are in both A and B:

$$A \cap B \coloneqq \{x : x \in A \text{ and } x \in B\}.$$

We say that two sets are **disjoint** if they share no elements in common; that is, if $A \cap B = \varnothing$.

The **union** of a set A with a set B, written as $A \cup B$, is the set of all elements which are in either A or B (or both):

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

For example, if $A = \{0, 2, 4, 6, \ldots\}$ is the set of even natural numbers and $B = \{1, 3, 5, 7, \ldots, \}$ is the set of odd natural numbers, then $A \cap B = \varnothing$ and $A \cup B = \mathbb{N}$.

Below are a few properties of intersections and unions. For any sets A and B,

- $A \cup B = B \cup A$;
- $A \cap B = B \cap A$;
- $A \cup \varnothing = A$;
- $A \cap \varnothing = \varnothing$.

Another operation is the **relative complement** of A in B, also known as the **set difference** between B and A, written as $B \setminus A$ or $B - A$. It consists of the set of elements of B not in A:

$$B \setminus A \coloneqq \{x \in B : x \notin A\}.$$

For example, if $B = \{1, 2, 3\}$ and $A = \{3, 4, 5\}$, then $B \setminus A = \{1, 2\}$. This provides a way to get at the irrational numbers, which can be found as $\mathbb{R} \setminus \mathbb{Q}$.

Below are a few important properties of complements. For any set A,

- $A \setminus A = \varnothing$;
- $A \setminus \varnothing = A$;
- $\varnothing \setminus A = \varnothing$.

We can also combine sets in more interesting ways. The **Cartesian product** or **cross product** of two sets A and B, written $A \times B$, is the set of all ordered pairs whose first component is an element of A and second component is an element of B:

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

For example, if $A = \{1, 2, 3\}$ and $B = \{u, v\}$, then

$$A \times B = \{(1, u), (1, v), (2, u), (2, v), (3, u), (3, v)\}.$$

As another example,

$$\mathbb{N} \times \mathbb{N} = \{(0, 0), (1, 0), (0, 1), (1, 1), (2, 0), \ldots\}$$

is the set of all pairs of natural numbers. A useful one is $\mathbb{R} \times \mathbb{R}$, which is the set of all real pairs. We often denote cross products of a set with itself $A \times A$ as A^2. So the two previous examples can be written as $\mathbb{N}^2$ and $\mathbb{R}^2$.

Repeated cross products yield longer ordered lists. $A \times B \times C$ is the set of all ordered triples with first, second, and third components from A, B, and C, respectively. This can be extended to arbitrary many cross products.

Our final set operation is unary: it's acts on one set. Given a set A, the **power set** of A, written 2^A or $\wp(A)$ is the set of all subsets of A:

$$2^A = \{S : S \subseteq A\}.$$

For example, if $A = \{1, 2, 3\}$, then the power set of A is

$$2^A = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Below are a few important properties of power sets. For any set A,

- $\varnothing \in 2^A$;
- $A \in 2^A$;
- If $|A| = k$, then $|2^A| = 2^k$.

If the last one seems very obvious, that is likely the fault of the very suggestive notation for the power set.

2 Sums and Products

We will frequently write sums or products of large or even infinite numbers of items. We can often communicate such sums or products through the use of an ellipsis: e.g., $1+2+\ldots+n-1+n$ for the sum of the first n positive natural numbers. However, this can be vague, and it requires the pattern between terms to be sufficiently clear. Instead, we can make this completely formal and rigorous through the use of **summation notation**:

$$1 + \ldots + n = \sum_{i=1}^{n} i.$$

More generally, we write the sum

$$f(m) + f(m + 1) + \ldots + f(n)$$

as

$$\sum_{i=m}^{n} f(i).$$

This makes the pattern explicit, and avoids depending on other' abilities to determine what it might be. We can think of the sum like a `for` loop, and the function f like the instructions on what to add to the running total in each iteration of the loop. As an example,

$$\sum_{i=5}^{n} i^2 = 5^2 + 6^2 + \ldots + n^2.$$

Analogously, to write the product $f(m) \cdot f(m + 1) \cdot \ldots \cdot f(n)$, we use the notation

$$\prod_{i=m}^{n} f(i).$$

For example,

$$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot \ldots \cdot n$$

is the product of the first n positive natural numbers.

The variable over which the sum iterates (i in all the above examples) is a dummy variable, and the specific symbol used is irrelevant. Additionally, the index of the sum can be done over a set. For example, for a set A, the sum

$$\sum_{a \in A} a$$

is understood to be the sum of the elements of A.

The term inside a sum or a product can also be another sum or product. This yields expressions such as nested sums. We can think of these like nested `for` loops. For example,

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{i} ij &= \sum_{i=1}^{n} i \cdot \big(1 + \ldots + i\big) \\ &= 1 \cdot 1 + \\ &\quad 2 \cdot 1 + 2 \cdot 2 + \\ &\quad 3 \cdot 1 + 3 \cdot 2 + 3 \cdot 3 + \\ &\qquad \vdots \\ &\quad n \cdot 1 + n \cdot 2 + n \cdot 3 + \ldots + n \cdot n.\end{aligned}$$

A famous sum which we will find occasional use for is the finite geometric series: for any $r \neq 1$,

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1 - r}.$$

To prove this, multiply the sum by $1 - r$. Some algebra yields the result.

Infinite Series

Some sums (and some products) can have infinitely many terms. There are many such “infinite series,” but we will primarily concern ourselves with the following.

The first is the infinite geometric series. For any $|r| < 1$,

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1 - r}.$$

Showing that this is the case requires first showing that the limit indeed exists. But once that is done, the same technique used for showing the finite geometric series result works as well.

The second is possibly the most famous and important infinite series of all time: the Taylor series expansion of the exponential. For any $x \in \mathbb{R}$,

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

This result takes a bit more theory to prove than just some algebra, and thus we will not concern ourselves with why it is true, and simply accept that it is.