Math 141: Lecture 1

Sets, natural numbers, induction, sums

Bob Hough

August 29, 2016

(Zermelo-Frenkel) Set Theory Basics

A *set* is a collection of objects, called *elements*. Objects include:

- Numbers
- Functions
- Mathematical symbols
- Other *sets*

Examples of sets

- The set containing 1, 2, and 3 as elements, $\{1, 2, 3\}$
- The emptyset containing no elements, written $\emptyset$ or $\{\}$
- The set containing the empty set $\{\emptyset\}$
- The set of positive natural numbers $\{1, 2, 3, 4, ...\}$
- The set $\mathbb{R}$ of real numbers
- The set of non-negative real numbers, $\{x \in \mathbb{R} : x \geq 0\}$

Another way of expressing the non-negative reals is as

$$\{y^2 : y \in \mathbb{R}\}.$$

Set Notation

- $x \in A$ means 'x is an element of set A'
- $A \subset B$ or $A \subseteq B$, read 'A is a subset of B', means every element of A is an element of B
- $A = B$ means $A \subset B$ and $B \subset A$

These statements have negations, indicated by $\notin, \not\subset, \neq$.

- A is a *proper subset* of B, written $A \subsetneq B$, if $A \subset B$ but $A \neq B$.

Logical short-hand

- P and Q: $P \wedge Q$
- P or Q: $P \vee Q$
- There exists: $\exists$
- For all: $\forall$
- Such that: s.t.
- If P then Q: $P \Rightarrow Q$
- Negation of P: $\overline{P}$ or P^c
- P only if Q: $Q^c \Rightarrow P^c$
- If and only if: $\Leftrightarrow$

Example usage

$f : \mathbb{R} \to \mathbb{R}$ and $x \in \mathbb{R}$ are such that...

$$\forall \epsilon > 0, \; \exists \delta > 0, \text{ s.t. } |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon.$$

- This means: For each $\epsilon > 0$ there exists a $\delta > 0$ such that, if the distance between x and y is less than δ, then the distance between $f(x)$ and $f(y)$ is less than ϵ.
- Or: function f is *continuous* at x.
- Note: using too much short-hand is frowned upon. We'll use only a little to save time.

Operations on sets

Given sets A and B the following operations are defined.

- Union: $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- Intersection: $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- Set difference: $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$, read '$A$ minus B'
- Symmetric difference: $A \Delta B = (A \setminus B) \cup (B \setminus A)$
- Complement: A^c or $\overline{A}$ are used to indicate $B \setminus A$ in the case when $A \subset B$ and B is understood from the context.
  For example, in $\mathbb{R}$, $A = \{x \in \mathbb{R} : x < 0\}$ has $A^c = \{x \in \mathbb{R} : x \geq 0\}$.

Properties of $\cap$ and $\cup$

Theorem

Union and intersection satisfy the following properties:

1. *Commutative:* $A \cup B = B \cup A$, $A \cap B = B \cap A$
2. *Associative:*

$$A \cup (B \cup C) = (A \cup B) \cup C,$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

3. *Distribute over each other:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Properties of $\cap$ and $\cup$

Proof.

We'll check a part of item 3:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Let $x \in A \cap (B \cup C)$. Then $x \in A$ and either $x \in B$ or $x \in C$ (or both). If $x \in B$ then $x \in (A \cap B)$. Otherwise $x \in (A \cap C)$, whence in either case, $x \in (A \cap B) \cup (A \cap C)$. This proves

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C).$$

To prove the reverse inclusion, let $x \in (A \cap B) \cup (A \cap C)$. Then either x belongs to both A and B or else x belongs to both A and C. In either case, x belongs to both A and $B \cup C$.

□

De Morgan's Law

Theorem

Let A, B be subsets of a set X. Then

$$(A \cap B)^c = A^c \cup B^c, \qquad (A \cup B)^c = A^c \cap B^c.$$

For a proof, see HW1.

Indexing sets

Sometimes collections of sets are identified by elements of an indexing set $\mathcal{I}$, so $\forall i \in \mathcal{I}$ there is set S_i. Notation:

$$\bigcup_{i\in\mathcal{I}} S_i = \{x : \exists i \in \mathcal{I} \text{ s.t. } x \in S_i\}$$

$$\bigcap_{i\in\mathcal{I}} S_i = \{x : \forall i \in \mathcal{I}, x \in S_i\}$$

Common indexing sets have notational variants:

- $\mathcal{I} =$ the numbers $\{1, 2, ..., n\}$: $\bigcup_{i=1}^{n}, \bigcap_{i=1}^{n}$
- $\mathcal{I} =$ the positive integers $\{1, 2, 3, ...\}$: $\bigcup_{i=1}^{\infty}, \bigcap_{i=1}^{\infty}$

Other variants should be self-explanatory, but ask if you are unsure.

Products

- An *ordered pair* (a, b) is defined set-theoretically by

$$(a, b) = \{a, \{a, b\}\}$$

  The elements of an ordered pair can consist of numbers, sets, functions, etc, and need not all be of the same type (although at the most basic level, all of these will be sets).

- Given sets A, B, the *product set* is

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

- Exponent notation: $A^1 = A$, for $n \geq 2$, $A^n = A \times A^{n-1}$

Functions

Definition

Given sets A, B a function $f : A \to B$ is a subset $F \subset A \times B$ satisfying

1. For all $x \in A$ there exists $y \in B$ s.t. $(x, y) \in F$
2. For all $x \in A$, if $(x, y_1) \in F$ and $(x, y_2) \in F$ then $y_1 = y_2$.

- The unique y s.t. $(x, y) \in F$ is written $y = f(x)$. Also $f : x \mapsto y$.
- A is called the *domain*
- The set $f(A) = \{y \in B : \exists x \in A,\ f(x) = y\}$ is called the *range*.
- The *pre-image* of $y \in B$ is the set $f^{-1}(y) = \{x \in A : f(x) = y\}$.

Function properties

Let A and B be sets. A function $f : A \to B$ is

- *surjective* if the range is B
- *injective*, or $1-1$, if $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$ implies $x_1 = x_2$
- *bijective* if both surjective and injective.

If there exists a bijective function $f : A \to B$ then A and B are said to have the same *cardinality*. The cardinality of $\{1, 2, ..., n\}$ is n.
If there exists an injective function $f : A \to \{1, 2, 3, ...\}$ then A is *countable*.

Examples

- The function $f(x) = 2x$ is a bijection between $\{1, 2, 3\}$ and $\{2, 4, 6\}$. Both have cardinality 3.
- The function $f(x) = x$ is an injection from $\{1, 2\}$ to $\{1, 2, 3, 4, 5\}$.
- A bijection $f : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ is also called a *permutation on n letters* or a *shuffle on n cards*.

Examples

Theorem

The integers are countable.

Proof.

We will be able to make this more formal by the end of the lecture. Define $f : \mathbb{Z} \to \{1, 2, ...\}$ by

$$f(x) = \begin{cases} 2x & x > 0 \\ -2x + 1 & x \leq 0 \end{cases}.$$

That $f(\mathbb{Z}) \subset \{1, 2, ...\}$ follows from the fact that multiplication by 2 preserves the sign. Thus it suffices to check that f is injective. Suppose $f(x_1) = f(x_2)$. If both $x_1, x_2 > 0$, or both $x_1, x_2 \leq 0$ then solving a linear equation we see $x_1 = x_2$. Meanwhile, if $x_1 > 0$ but $x_2 \leq 0$ then $f(x_1)$ is even while $f(x_2)$ is odd, so they are not equal. Thus $f(x_1) = f(x_2)$ implies $x_1 = x_2$. □

Equivalence relations

Definition

An *equivalence relation* $\sim$ on a set S is a subset $E \subset S \times S$ satisfying E is

1. Reflexive: $\forall x \in S$, $(x, x) \in E$
2. Symmetric: $(x, y) \in E \Leftrightarrow (y, x) \in E$
3. Transitive: If $(x, y) \in E$ and $(y, z) \in E$, then $(x, z) \in E$.

We write $x \sim y$ if $(x, y) \in E$ and say 'x and y are equivalent'. The *equivalence class* of $x \in S$ is

$$\overline{x} = \{y \in S : x \sim y\}.$$

The *quotient set* or *set of equivalence classes* is

$$S/\sim = \{\overline{x} : x \in S\}.$$

Examples

- An equivalence relation $\sim$ on $\mathbb{Z}$ is given by $m \sim n$ if and only if $m - n$ is even. The quotient $\mathbb{Z}/\sim = \{\bar{0}, \bar{1}\}$ is also denoted $\mathbb{Z}/2\mathbb{Z}$.
- An equivalence relation on $\{1, 2, 3, 4, 5, 6\}$ has classes $\{1, 2\}, \{3, 4\}, \{5, 6\}$.

Equivalence relations

Theorem

Let $\sim$ be an equivalence relation on a set S. Let $x, y \in S$. If $x \sim y$ then $\overline{x} = \overline{y}$. If $x \not\sim y$ then $\overline{x} \cap \overline{y} = \emptyset$.

Proof.

Suppose $x \sim y$. Let $z \in \overline{y}$. Thus $y \sim z$. It follows that $x \sim z$ and hence $z \in \overline{x}$ by transitivity, so $\overline{y} \subset \overline{x}$. By symmetry, $y \sim x$ so $\overline{x} \subset \overline{y}$. Hence $\overline{x} = \overline{y}$.

Now suppose that $x \not\sim y$ and suppose that there exists $z \in \overline{x} \cap \overline{y}$. Then $x \sim z$ and $y \sim z \Rightarrow z \sim y$ from which it follows that $x \sim y$. Since this is false, it follows that $\overline{x} \cap \overline{y} = \emptyset$. □

The Zermelo-Frenkel Construction of $\mathbb{N}$

Historically $\mathbb{N}$ begins with 1, but for us, $0 \in \mathbb{N}$.

- Define $0 = \emptyset = \{\}$.
- The *Successor function* S is defined at set n by $S(n) = \{n\} \cup n$.
- Hence

$$\begin{aligned} 1 = &\quad S(0) &&= \{\{\}\} \\ 2 = &\quad S(S(0)) &&= \{\{\{\}\}, \{\}\} \\ 3 = &\quad S(S(S(0))) &&= \{\{\{\{\}\}, \{\}\}, \{\{\}\}, \{\}\}. \end{aligned}$$

- $\mathbb{N}$ is defined 'recursively' to be the smallest set s.t. $0 \in \mathbb{N}$ and $\forall n \in \mathbb{N}, S(n) \in \mathbb{N}$.

The principle of mathematical induction

The recursive definition of $\mathbb{N}$ gives a way to prove statements about all elements of $\mathbb{N}$ by 'mathematical induction': A statement P is true of all $n \in \mathbb{N}$ if both

1. $P(0)$ is true
2. For all $n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$.

Operations on natural numbers

(Polish notation)
Functions $+, \times, \mathrm{EXP} : \mathbb{N}^2 \to \mathbb{N}$ are defined recursively as follows.

$$+ : \begin{cases} & +(0,0) = 0 \\ \forall m, n \in \mathbb{N} & +(S(m), n) = S(+(m,n)) \\ \forall m, n \in \mathbb{N} & +(m, S(n)) = S(+(m,n)) \end{cases}$$

$$\times : \begin{cases} & \times(0,0) = 0 \\ \forall m, n \in \mathbb{N} & \times(S(m), n) = +(\times(m,n), n) \\ \forall m, n \in \mathbb{N} & \times(m, S(n)) = +(\times(m,n), m) \end{cases}$$

$$\mathrm{EXP} : \begin{cases} \forall n \in \mathbb{N} & \mathrm{EXP}(0, n) = 0 \\ \forall n \in \mathbb{N} & \mathrm{EXP}(n, 0) = 1 \\ \forall m, n \in \mathbb{N} & \mathrm{EXP}(m, S(n)) = \times(\mathrm{EXP}(m,n), m). \end{cases}$$

Some properties of $\mathbb{N}$

$$\begin{aligned}
+,\ \times \text{ commutative:}\quad & +(m,n) = +(n,m), \times(m,n) = \times(n,m)\\
+,\ \times \text{ associative:}\quad & +(m,+(n,p)) = +(+(m,n),p),\\
& \times(m,\times(n,p)) = \times(\times(m,n),p)\\
+,\ \times \text{ identities:}\quad & +(n,0) = \times(n,1) = n\\
\times \text{ distributes over } +\text{:}\quad & \times(m,+(n,p)) = +(\times(m,n),\times(m,p))\\
\text{cancellation:}\quad & +(m,n) = +(m,n') \Rightarrow n = n'\\
& \text{for } m \neq 0,\ \times(m,n) = \times(m,n') \Rightarrow n = n'\\
\text{succession:}\quad & \forall x, S(x) \neq 0,\\
& \forall x \neq 0, \exists y, S(y) = x.
\end{aligned}$$

- If $\times(m,n) = p$ and $m \neq 0$ we write $m|p$ and say 'm divides p'; define $\div(p,m) = n$.

Some properties of $\mathbb{N}$

Proof.

We'll check $+(m,n) = +(n,m)$ which is representative of the proofs.
We first check that $\forall m,\ +(m,0) = +(0,m) = m$:

- Base case: $m = 0$. $+(0,0) = 0$ holds by definition.
- Inductive step: Assuming $+(m,0) = +(0,m) = m$, we find $+(S(m),0) = S(+(m,0)) = S(m) = +(0,S(m))$ which completes the inductive sub-proof.

Now we check that $\forall n,\ +(m,n) = +(n,m)$.

- Base case: $n = 0$. $+(m,0) = +(0,m)$ holds by the above argument.
- Inductive step: Assume that $+(m,n) = +(n,m)$. Then $+(m,S(n)) = S(+(m,n)) = S(+(n,m)) = +(S(n),m)$.

This completes the inductive proof. □

Ordering $\mathbb{N}$

Definition

Given $m, n \in \mathbb{N}$, define $m < n$ if there exists $x \in \mathbb{N}$, such that $+(m, S(x)) = n$. Set $m \leq n$ if $m < n$ or $m = n$. Write $m > n$ if $n < m$ (similarly $\geq$).

Theorem (Trichotomy law for $\mathbb{N}$)

For each $m, n \in \mathbb{N}$ exactly one of $m < n$, $m = n$ or $m > n$ is true. If $m < n$ then $S(m) \leq n$.

See HW1 for a proof.

Well-ordering principle

Theorem (Well-ordering principle of $\mathbb{N}$)

Let $A \subset \mathbb{N}$ be non-empty. Then A contains a least member x, which satisfies $\forall y \in A$, $x \leq y$.

Proof.

Suppose for contradiction that A contains no least member. Let $B = \{x \in \mathbb{N} : \forall a \in A, x \leq a\}$. We show by induction that $\forall n \in \mathbb{N}$, $n \in B$, whence $A = \emptyset$, a contradiction.

- Base case: $0 \in B$ since $0 \leq n$ for every $n \in A$.
- Inductive case: Suppose $n \in B$ so that, for all $a \in A$, $n \leq a$. It follows that $n \notin A$, and thus, for all $a \in A$, $n < a$. By the trichotomy law, for all $a \in A$, $S(n) \leq a$. Thus $S(n) \in B$.

□

Summation and product notation

Given some numbers $a_1, a_2, a_3, \ldots$ (technically, a function $a : \mathbb{N} \to S$ for some set S on which $+$ and $\times$ are defined) define the notations

$$\sum_{i=1}^{n} a_i, \qquad \prod_{i=1}^{n} a_i$$

recursively as follows.

- $$\sum_{i=1}^{0} a_i = 0, \qquad \prod_{i=1}^{0} a_i = 1$$
- For all $n \in \mathbb{N}$,

$$\sum_{i=1}^{S(n)} a_i = +\left(\sum_{i=1}^{n} a_i, a_{n+1}\right), \qquad \prod_{i=1}^{S(n)} a_i = \times\left(\prod_{i=1}^{n} a_i, a_{n+1}\right).$$

Summation example

Theorem (School-age Gauss)

For all $n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof.

The proof is by induction.

- Base case: When $n = 0$, $\sum_{i=1}^{0} i = 0 = \frac{0\times 1}{2}$.
- Inductive step: Assume $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Then

$$\sum_{i=1}^{n+1} i = (n+1) + \frac{n(n+1)}{2} = \frac{(n+2)(n+1)}{2}.$$

□

Area calculation by exhaustion

Archimedes calculated the area within the curvi-linear triangular region T defined by

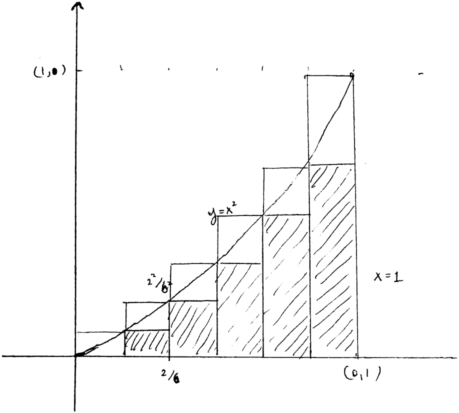
$$T = \{(x, y) : 0 \leq x \leq 1, 0 \leq y \leq x^2\}$$

to be $\mathrm{Area}(T) = \frac{1}{3}$. The method is as follows.

1. Let $n \geq 1$ be a natural number, and subdivide the interval $0 \leq x \leq 1$ into n equally sized segments.
2. In each segment $\frac{i}{n} \leq x \leq \frac{i+1}{n}$ draw a lower rectangle defined by $0 \leq y \leq \frac{i^2}{n^2}$, and an upper rectangle defined by $0 \leq y \leq \frac{(i+1)^2}{n^2}$
3. The sums of the areas of the lower rectangles is $L(n)$ and the upper rectangles $U(n)$. For each n, $L(n) \leq T \leq U(n)$.
4. Calculate

$$L(n) = \frac{1}{n^3} \sum_{i=1}^{n-1} i^2, \qquad U(n) = \frac{1}{n^3} \sum_{i=1}^{n} i^2.$$

Area calculation by exhaustion



Schematic of Archimedes' construction. The shaded region represents the region whose area is $L(6)$. Including the boxes above gives the region whose area is $U(6)$.

Area calculation by exhaustion

Recall that

$$L(n) = \frac{1}{n^3}\sum_{i=1}^{n-1} i^2, \qquad U(n) = \frac{1}{n^3}\sum_{i=1}^{n} i^2.$$

In HW2 you will partly complete Archimedes method by checking by induction that

$$\sum_{i=1}^{n-1} i^2 \le \frac{n^3}{3} \le \sum_{i=1}^{n} i^2.$$

Since $U(n) - L(n) = \frac{1}{n}$, we obtain

$$\frac{1}{3} - \frac{1}{n} \le L(n) \le \mathrm{Area}(T) \le U(n) \le \frac{1}{3} + \frac{1}{n}.$$

Archimedes concluded $\mathrm{Area}(T) = \frac{1}{3}$ by taking increasingly large values of n.

Food for thought/philosophy

In the physical world, is there a world's largest number? If so, is it possible to prove a statement about every physical natural number by mathematical induction?

We work in a *model* which abstracts away questions of physics and computation, but which has been applied to the physical world to great effect.