18.100A: Complete Lecture Notes

Lecture 3:
Cantor's Remarkable Theorem
and the Rationals' Lack of the Least Upper Bound Property

Question 1. *Is anything bigger than* $\mathbb{N}$*?*

If A is a set then $\mathcal{P}(A) = \{B \mid B \subset A\}$. Here are a few examples:

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

In general, if $|A| = n$ then $|\mathcal{P}(A)| = 2^n$. This is why we call $\mathcal{P}(A)$ the power set of A.

Theorem 2 (Cantor)
If A is a set, then $|A| < |\mathcal{P}(A)|$.

Remark 3. *Therefore,*

$$\mathbb{N} < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots.$$

Hence, there are an infinite number of infinite sets.

Proof: Define the function $f : A \to \mathcal{P}(A)$ by $f(x) = \{x\}$. Then, f is 1-1– as if $\{x\} = \{y\} \implies x = y$. Thus, $|A| \leq |\mathcal{P}(A)|$. To finish the proof now all we need to show is that $|A| \neq |\mathcal{P}(A)|$. We will do so through contradiction. Suppose that $|A| = |\mathcal{P}(A)|$. Then, there exists a surjection $g : A \to \mathcal{P}(A)$. Let

$$B := \{x \in A \mid x \notin g(x)\} \in \mathcal{P}(A).$$

Since g is surjective, there exists a $b \in A$ such that $g(b) = B$. There are two cases:

1. $b \in B$. If this is the case, then $b \notin g(b) = B \implies b \notin B$.
2. $b \notin B$. If this is the case, then $b \notin g(b) = B \implies b \in B$.

In either case we obtain a contradiction. Thus, g is not surjective $\implies |A| \neq |\mathcal{P}(A)|$. □

Remark 4. *This is another proof method: casework. If the conclusion for every case is true, then the conclusion must be true.*

Corollary 5
For all $n \in \mathbb{N} \cup \{0\}$, $n < 2^n$.

Remark 6. *This can also be shown by induction, see Assignment 1.*

Real Numbers

Remark 7. *In a sense, to be made precise, the set of real numbers is the unique set with all of the* <u>*algebraic*</u> *and* <u>*ordering*</u> *properties of the rational numbers, but none of the holes.*

Problem 8

Now let's try to precisely describe $\mathbb{R}$.

We will start by stating what our end result will be, and then we will derive it:

Theorem 9 (Real Numbers ($\mathbb{R}$))

There exists a unique **ordered field** containing $\mathbb{Q}$ with the **least upper bound property**. We denote this field by $\mathbb{R}$.

<u>**Ordered Sets & Fields**</u>

Definition 10 (Ordered set)

An ordered set is a set S with a relation $<$ called an "ordering" such that

1. $\forall x, y \in S$ either $x < y$, $y < x$, or $x = y$.
2. If $x < y$ and $y < z$ then $x < z$.

Here are a few examples and one non-example:

- $\mathbb{Z}$ is an ordered set, with the relation that $m > n \iff m - n \in \mathbb{N}$.
- $\mathbb{Q}$ is an ordered set, with the relation that $p > q \iff \exists m, n \in \mathbb{N}$ such that $p - q = \frac{m}{n}$.
- $\mathbb{Q} \times \mathbb{Q}$ is an ordered set with the relation $(q, r) > (s, t) \iff q > s$ or $q = s$ and $r > t$.
- Consider the set $\mathcal{P}(\mathbb{N})$. Let $A, B \in \mathcal{P}(\mathbb{N})$ and let $A \prec B$ if $A \subset B$. This is **NOT** an ordered set– it doesn't satisfy the first property of an ordered set.

Definition 11 (Bounded Above/Below)

Let S be an ordered set and let $E \subset S$. Then,

1. If there exists a $b \in S$ such that $x \leq b$ for all $x \in E$, then E is bounded above and b is an <u>vocab</u> of E.
2. If $\exists c \in S$ such that $x \geq c$ for all $x \in E$, then E is bounded below and c is a lower bound of E.

From here, there are some very important definitions in real analysis. We say that b_0 is the **least upper bound**, or the supremum of E if

A) b_0 is an upper bound for E and

B) if b is an upper bound for E then $b_0 \leq b$.

We denote this as $b_0 = \sup E$. Similarly, we say that c_0 is the **greatest lower bound**, or the infimum of E if

A) c_0 is a lower bound for E and

B) if c is a lower bound for E then $c < c_0$.

We denote this as $c_0 = \inf E$.

Example 12
Here are a few examples of infimums and supremums:

- $S = \mathbb{Z}$ and $E = \{-2, -1, 0, 1, 2\}$. Then, $\inf E = -2$ and $\sup E = 2$.
- But, note that the supremum nor the infimum need to be in E. Consider the sets $S = \mathbb{Q}$ and

  $$E = \{q \in \mathbb{Q} \mid 0 \leq q < 1\}.$$

  Then, $\inf E = 0 \in E$, but $\sup E = 1 \notin E$.
- Furthermore, neither the supremum nor the infimum need exist. Consider the sets $S = \mathbb{Z}$ and $E = \mathbb{N}$. Then, $\inf E = 1$, but $\sup E$ does not exist as there is not an integer greater than all natural numbers.

Definition 13 (Least Upper Bound Property)
An ordered set S has the least upper bound property if every $E \subset S$ which is nonempty and bounded above has a supremum in S.

One example of such a set is

$$-\mathbb{N} = \{-1, -2. -3. \dots\}.$$

Then, $E \subset S$ is bounded above if and only if $-E \subset \mathbb{N}$ is bounded below. By the well-ordering principle, $-E$ has a least element $x \in -E$, and thus $-x = \sup E$.

We will now show that $\mathbb{Q}$ does not have the least upper bound property.

Theorem 14
If $x \in \mathbb{Q}$ and

$$x = \sup\{q \in \mathbb{Q} \mid q > 0, q^2 < 2\}$$

then $x > 0$ and $x^2 = 2$.

Proof: Let E equal the set on the right hand side, and suppose $x \in \mathbb{Q}$ such that $x = \sup E$. Then, since $1 \in E$ and x is an upper bound for E, $1 \leq x \implies x > 0$.

We now prove that $x^2 \geq 2$. Suppose that $x^2 < 2$. Define $h = \min\left\{\frac{1}{2}, \frac{2-x^2}{2(2x+1)}\right\} < 1$. Then, if $x^2 < 2$ then $h > 0$. We now prove that $x + h \in E$. Indeed,

$$\begin{aligned}(x+h)^2 &= x^2 + 2xh + h^2 \\ &< x^2 + h(2x+1)\end{aligned}$$

as $h < 1$. Hence

$$\begin{aligned}(x+h)^2 &\leq x^2 + (2 - x^2) \cdot \frac{2x+1}{2(2x+1)} \\ &= x^2 + \frac{2 - x^2}{2} \\ &< 2 + \frac{2-2}{2} \\ &= 2.\end{aligned}$$

Therefore, $x + h \in E$ and $x + h > x \implies x$ is not an upper bound for E. Therefore, $x \neq \sup E$ which is a contradiction. Hence, $x^2 \geq 2$.

We now prove that $x^2 \leq 2$. Suppose $x^2 > 2$. Let $h = \frac{x^2-2}{2x}$. Hence, if $x^2 > 2$ then $h > 0$ and $x - h > 0$. We will show that $x - h$ is an upper bound for E. We have

$$\begin{aligned}(x-h)^2 &= x^2 - 2xh + h^2 \\ &= x^2 - (x^2 - 2) + h^2 \\ &= 2 + h^2 \\ &> 2.\end{aligned}$$

Let $q \in E$. Then, $q^2 < 2 < (x-h)^2 \implies (x-h)^2 - q^2 > 0$. Hence,

$$((x-h)+q)((x-h)+q) > 0 \implies (x-h) - q > 0.$$

Thus, for all $q \in E$, $q < x - h < x \implies x \neq \sup E$. This is a contradiction. Therefore, $x^2 = 2$. □

Theorem 15

The set $E = \{q \in \mathbb{Q} \mid q > 0 \text{ and } q^2 < 2\}$ does not have a supremum in $\mathbb{Q}$.

Proof: Suppose there exists an $x \in \mathbb{Q}$ such that $x = \sup E$. Then, by our previous theorem, $x^2 = 2$. In particular, note that $x > 1$ as otherwise $x \leq 1 \implies 2 = x^2 < 1^2$. Thus, $\exists m, n \in \mathbb{N}$ such that $m > n$ and $x = \frac{m}{n}$. Therefore, $\exists n \in \mathbb{N}$ such that $nx \in \mathbb{N}$. Let

$$S = \{k \in \mathbb{N} \mid kx \in \mathbb{N}\}.$$

Then, $S \neq \emptyset$ since $n \in S$. By the well-ordering property of $\mathbb{N}$, S has a least element $k_0 \in S$. Let $k_1 = k_0 x - k_0 \in \mathbb{Z}$. Then, $k_1 = k_0(x-1) > 0$ since $k_0 \in \mathbb{N}$ and $x > 1$. Therefore, $k_1 \in \mathbb{N}$. Now $x^2 = 2 \implies x < 2$, as otherwise $x^2 > 4 > 2$. Thus, $k_1 = k_0(x-1) < k_0(2-1) = k_0$. So, $k_1 \in \mathbb{N}$ and $k_1 < k_0 \implies k_1 \notin S$ as k_0 is the least element of S. But,

$$xk_1 = k_0 x^2 - xk_0 = 2k_0 - xk_0 = k_0 - k_1 \in \mathbb{N} \implies k_1 \in S.$$

This is a contradiction. Thus, $\nexists x \in \mathbb{Q}$ such that $x = \sup E$. □

$\mathbb{Q}$ is an example of a field, which we will start to discuss in the next lecture.