Three lectures on (un)countability for Math 131 A

BENJAMIN ANTIEAU

1. Lecture 26

While the rational numbers $\mathbb{Q}$ are dense in the real numbers $\mathbb{R}$, it *seems* like there are many, many more real numbers than rational. For instance, $\mathbb{Q}$ feels discrete, while $\mathbb{R}$ feels continuous. More concretely, every decimal expansion of a rational number is eventually repeating and conversely. There is no such restriction for irrational numbers, and certainly "most" decimal expansions are not repeating. The goal of these lectures is to make this idea precise and to prove in a rigorous way that there *are* more elements of $\mathbb{R}$ than there are of $\mathbb{Q}$. References for this material can be found in [1, Chapter 1] and [3, Chapter 2].

Recall that if A and B are sets, a function $f : A \to B$ assigns to every element x of A a unique element $f(x)$ of B. A function f is

- **injective** if $f(x) = f(y)$ implies $x = y$;
- **surjective** if for every $z \in B$ there exists $x \in A$ such that $f(x) = z$;
- **bijective** if it is injective and surjective.

Note that an injective function is also called one-to-one, while a surjective function is also called onto.

A set with only finitely many elements is called **finite**. A non-finite set is called **infinite**. Another way to describe finite sets is that after finitely many applications of the operation "remove an element" one arrives at the empty set $\emptyset$.

When A is a finite set, a good measure of the size of A is simply the number of elements of A. This doesn't extend well to infinite sets. But, two finite sets A and B have the same size if there is a bijection $f : A \xrightarrow{\simeq} B$. In general, we will write $A \cong B$ when A and B are bijective. This motivates the following definition.

Definition 1.1. Two sets A and B are called **equivalent** if there is a bijection $f : A \xrightarrow{\simeq} B$.

Now, we can ask whether or not $\mathbb{R}$ is equivalent to $\mathbb{Q}$. In fact, we will split the problem up into a couple of parts. Recall that $\mathbb{N}$ denotes the set $\{1, 2, 3, \ldots\}$ of natural numbers.

Definition 1.2. A set A is countable if $A \cong \mathbb{N}$.

A set A is countable if and only if it is possible to list the elements of A as a sequence $A = \{a_1, a_2, \ldots\}$.

Exercise 1.3. If $a < b$ and $c < d$, show that $[a, b]$ and $[c, d]$ are equivalent by constructing a linear function $y = mx + b$ from one to the other. This example shows that the idea of equivalence used here is different from the idea of length.

Example 1.4. The set of integers $\mathbb{Z}$ is countable. Indeed, one can list the integers as

$$0, -1, 1, -2, 2, -3, 3, \ldots$$

More specifically, simply define a bijection $f : \mathbb{N} \xrightarrow{\simeq} \mathbb{Z}$ by

$$f(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd,} \\ -\frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

The next example is even more important, but somewhat less concrete.

Example 1.5. The set of rational numbers $\mathbb{Q}$ is countable. To see this, suppose that $x = \frac{p}{q}$ is a rational number in lowest terms, where $q > 0$. Define the height of x as $h(x) = |p| + q$. Then, $h(x) > 0$ for all rational numbers x. The height 1 rational number is $\frac{0}{1}$. The rational numbers of height 2 are $\frac{-1}{1}$ and $\frac{1}{1}$. The rationals of height 3 are $\frac{-2}{1}$, $\frac{-1}{2}$, $\frac{1}{2}$, and $\frac{2}{1}$. Let H_n be the set of rational numbers of height n. Then, $H_n \cap H_m = \emptyset$ if $n \neq m$, and

$$\mathbb{Q} = \cup_{n=1}^{\infty} H_n.$$

Create a list of all rational numbers as follows. First, list all elements of height 1. Then, list all elements of height 2, and so on. The key point is that each H_n is finite.

This example is a special case of the following theorem.

Theorem 1.6. *Suppose that $A_1, \ldots, A_n, \ldots$ is a countable collection of sets each of which is finite or countable. Then,*

$$A = \cup_{n=1}^{\infty} A_n$$

is finite or countable.

Proof. It suffices to prove that if A is infinite, then it is countable. Write $A_i = \{a_{i1}, a_{i2}, a_{i3}, \ldots\}$. Let G_n be the set $\{a_{1,n-1}, a_{2,n-2}, \ldots, a_{n-1,1}\}$. Then, G_n is finite. So, as in the example, we can list the elements of A by listing those in G_1, then those in G_2, and so on. There is a subtlety in this argument. Unlike what happened for $\mathbb{Q}$, the sets G_n need note be disjoint. So, this process might lead to a function $f : \mathbb{N} \to A$ that is surjective but not injective. Nevertheless, there is an infinite subset B of $\mathbb{N}$ such that the restriction of f to B is a bijection. Since B is an infinite subset of $\mathbb{N}$, it is countable (this is justified in the following exercise), which means that A is countable. ■

Exercise 1.7. Show that every subset of a countable set is finite or countable.

Exercise 1.8. Show that every infinite set has a countable subset.

2. Lecture 27

When two sets A and B are equivalent, we say that they have the same **cardinality**. Let $m(A)$ denote the cardinality of a set A. At the moment, this is not particularly well-defined. We should think of the cardinality as being a measure of the size of the set A, so that A and B are the same size if and only if they have the same cardinality. Thus, $m(A)$ might be the name of the set of all sets equivalent to A. Let's not worry about the details too much, especially as to write the details correctly requires some care to avoid set-theoretic paradoxes. The cardinality of $\mathbb{N}$ is denoted $\aleph_0$, while that of $\mathbb{R}$ is written c, $\aleph$, or $2^{\aleph_0}$.

If $A \subseteq B$, we decree that $m(A) \leq m(B)$. We will see that this creates a well-defined partial ordering on the cardinals. For the moment, it is enough to think intuitively that if A is contained in B, then the size of B is at least as big as the size of A. In fact, although we won't get to it in these lectures, this definition provides a total ordering for the cardinals. More about this in the next lecture.

Lemma 2.1. *The cardinal $\aleph_0$ is the smallest infinite cardinal.*

As a special case, since $\mathbb{N} \subseteq \mathbb{R}$, we have $\aleph_0 \leq c$. The point of this lecture is to show that the inequality is strict: the real numbers are *not* countable. We will prove this using decimals.

A decimal is a sequence $k.d_1d_2d_3\ldots$, where k is an integer and $d_i \in \{0, 1, 2, \ldots, 9\}$. This is a string in a certain alphabet. It is not a number! However, to every decimal we can associate a real number

$$x = k + \sum_{k=1}^{\infty} \frac{d_k}{10^k}.$$

To see that this number exists, it suffices to check that the infinite sequence converges. Note that the partial sums form a non-decreasing sequence, so it is enough to check that it is bounded above. But, each d_k is at most 9. So,

$$\sum_{k=1}^{\infty} \frac{d_k}{10^k} \leq \sum_{k=1}^{\infty} \frac{9}{10^k} = \frac{9}{10} \sum_{k=0}^{\infty} \frac{1}{10^k} = \frac{9}{10} \frac{1}{1 - 10^{-1}} = 1,$$

Thus, not only does x exist, but $x \in [k, k+1]$. The decimal $k.d_1\ldots$ is called a **decimal expansion** of x.

Conversely, if x is a real number we can construct a decimal from x as follows. Let k be the largest integer such that $k \leq x$. Then, $x - k \in [0, 1)$. So, $10x - 10k \in [0, 10)$. Let d_1 be the largest integer such that $d_1 \leq 10x - 10k$. Then, $d_1 \in \{0, \ldots, 9\}$, and $10x - 10k - d_1 \in [0, 1)$. Thus, $100x - 100k - 10d_1 \in [0, 10)$. Let d_2 be the largest integer such that $d_2 \leq 100x - 100k - 10d_1$. And so on. Let $s_n = k.d_1\ldots d_n$. Then, by construction, $10^n(x - s_n) \in [0, 1)$. It follows that $x - s_n < 10^{-n}$. Therefore, $\lim s_n = x$, so that the constructed decimal is a decimal expansion for x.

Now, we state with partial proof two theorems about decimals. Full proofs can be found in [2]. A repeating decimal is written as $k.d_1\ldots d_n\overline{d_{n+1}\ldots d_{n+r}}$. This means that the decimal is $k.d_1\ldots d_nd_{n+1}\ldots d_{n+r}d_{n+1}\ldots d_{n+r}\ldots$, the part with the overline being repeated forever.

Theorem 2.2. *A real number x is rational if and only if it has a repeating decimal expansion.*

Proof. We prove that if x has a repeating decimal expansion $x = k.d_1\ldots d_n\overline{d_{n+1}\ldots d_{n+r}}$, then x is rational. Let $e_i = d_{n+i}$ for $1 \leq i \leq r$, and set $y = 0.\overline{e_1\ldots e_r}$. It is enough to check that y is rational because $x - 10^{-n}y = k.d_1\ldots d_n\overline{0}$, which is rational. But, because of the repeating decimals, which repeat with period r,

$$y = \sum_{j=1}^{r} \frac{e_j}{10^j} \sum_{k=0}^{\infty} \frac{1}{10^{rk}} = \sum_{j=1}^{\infty} \frac{e_j}{10^j} \frac{1}{1 - 10^{-r}},$$

which is rational. ∎

Theorem 2.3. *If a real number x has more than one decimal expansion, then it has exactly two, one ending in $\overline{9}$, the other ending in $\overline{0}$. In particular, such a number is rational by the previous theorem.*

Now, we arrive at our main theorem, which is that the real numbers are uncountable.

Theorem 2.4. *The set $\mathbb{R}$ of real numbers is uncountable.*

Proof. Suppose to the contrary that $\mathbb{R}$ was countable, and let $f : \mathbb{N} \xrightarrow{\simeq} \mathbb{R}$ be a bijection. Set $x_n = f(n)$. So, $\{x_1, x_2, \ldots\}$ is a list of all real numbers. Let $x_k = a_k.d_{k1}d_{k2}d_{k3}\ldots$ be a decimal expansion of x_k. Construct a new number $y = 0.e_1e_2e_3\ldots$ as follows. Let $e_i \in \{1, \ldots, 8\}$ be any number different than d_{ii}. The decimal $0.e_1\ldots$ is distinct by construction from any of the decimal expansion $a_k.d_{k1}d_{k2}d_{k3}\ldots$. It follows that either $y \neq x_k$ for any k or that $y = x_k$, but they are given by different decimal expansions. By the previous theorem, the decimal expansion $0.e_1\ldots$ of y must terminate in all 0s or all 9s. But, this is absurd, since e_i is never 0 or 9. Thus, $y \neq x_k$ for any k. It follows that y is not a real number (since it is not on our complete guest list of all real numbers). This is a contradiction. ∎

Corollary 2.5. *The set of irrational numbers $\mathbb{R} - \mathbb{Q}$ is uncountable.*

Proof. Since $\mathbb{R}$ is the union of $\mathbb{Q}$ and $\mathbb{R} - \mathbb{Q}$, if $\mathbb{R} - \mathbb{Q}$ were countable, $\mathbb{R}$ would be countable too by Theorem 1.6, which contradicts the theorem. ∎

A similar proof shows that if $a < b$, then the intervals (a, b), $[a, b)$, $(a, b]$, and $[a, b]$ are all uncountable. In fact they are all equivalent, and so each has cardinality c.

The following hypothesis has a long history. It was first studied by Georg Cantor in the 19th century.

Hypothesis 2.6 (The continuum hypothesis)**.** *There is no set whose cardinality is strictly between $\aleph_0$ and c.*

Cantor, who gave the first rigorous definition of $\mathbb{R}$, failed to establish whether or not this is false, and there is a good reason for this. This was the 1st of David Hilbert's 23 problems, presented in 1900 to the International Congress of Mathematicians as a road-map for work in the 20th century. He had tried to establish the hypothesis himself for many years. Kurt Gödel proved in 1940 that the continuum hypothesis (CH) cannot be proved in Zermelo-Fraenkel set theory with the axiom of choice (ZFC), the standard axiomatic framework for modern mathematics. Then, in 1963, Paul Cohen showed that CH cannot be disproven in ZFC either!

3. Lecture 28

Recall that a **partial ordering** $\leq$ on a set S is a binary relation such that

(1) $x \leq x$ for every $x \in S$ (**reflexivity**);
(2) if $x \leq y$ and $y \leq z$, then $x \leq z$ (**transitivity**);
(3) if $x \leq y$ and $y \leq x$, then $x = y$ (**antisymmetry**).

We can write $x < y$ if $x \leq y$ and $x \neq y$. The usual intuitions about comparisons apply, except that for a partial ordering, not every pair of elements needs to be comparable: we might have neither $x \neq y$ nor $y \leq x$. When one can compare any two elements, the partial ordering is a **total ordering**.

Last lecture, we introduced a binary relation for cardinals by saying that if $A \subseteq B$, then $m(A) \leq m(B)$, we claimed that it is a partial ordering. Reflexivity and transitivity are clear, but antisymmetry is less clear. This is provided by the next theorem.

Theorem 3.1 (Cantor-Bernstein)**.** *Let A and B be sets and suppose that $A \cong B_1 \subseteq B$ and $B \cong A_1 \subseteq A$ (that is, $m(A) \leq m(B)$ and $m(B) \leq m(A)$). Then, $A \cong B$.*

Proof. Let $f : A \to B$ be an injective map with image B_1; let $g : B \to A$ be an injective map with image A_1. The composition $A \xrightarrow{f} B \xrightarrow{g} A$ is injective. Let A_2 be the image $g(f(A)) \subseteq A_1$. In general, let A_{k+2} be the image $g(f(A_k))$. Then, there is a sequence of inclusions

$$\cdots \subseteq A_3 \subseteq A_2 \subseteq A_1 \subseteq A.$$

Set

$$D = \cap_{k=1}^{\infty} A_k.$$

Note that $gf(A - A_1) = A_2 - A_3$, $gf(A_2 - A_3) = A_4 - A_5$, and so forth. We can write A and A_1 as disjoint unions

$$A = D \cup (A - A_1) \cup (A_1 - A_2) \cup (A_2 - A_3) \cup \cdots$$
$$A_1 = D \cup (A_1 - A_2) \cup (A_2 - A_3) \cup (A_3 - A_4) \cup \cdots .$$

Define sets M, N, and N_1 by

$$M = (A_1 - A_2) \cup (A_3 - A_4) \cup \cdots$$
$$N = (A - A_1) \cup (A_2 - A_3) \cup \cdots$$
$$N_1 = (A_2 - A_3) \cup (A_4 - A_5) \cup \cdots ,$$

so that $A = D \cup M \cup N$ and $A_1 = D \cup M \cup N$. But, $N \cong N_1$, so that $A \cong A_1 \cong B$. ■

Therefore, the relation $\leq$ is a partial ordering on cardinals. It turns out to be a partial ordering, so that for any two sets A and B either $m(A) \leq m(B)$ or $m(B) \leq m(A)$. The proof of this fact requires the use of ordinal numbers and is outside the scope of these notes.

In order to show that there are infinitely many infinite cardinals, we introduce the notion of the power set. If A is a set, the power set of A is

$$P(A) = \{X | X \subseteq A\},$$

the set of all subsets of A. For example, $P(\emptyset) = \{\emptyset\}$ (note that $\emptyset \neq \{\emptyset\}$). Similarly, $P(\{1\}) = \{\emptyset, \{1\}\}$, and $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. More generally, if A has $n \geq 0$ elements, then $P(A)$ has 2^n elements.

Theorem 3.2. *If A is any set, then $P(A)$ is not equivalent to A. Specifically, $m(A) < m(P(A))$.*

Proof. Note that $m(A) \leq m(P(A))$ because A is equivalent to the subset of $P(A)$ consisting of singleton sets. That is, there is an injective function $f : A \to P(A)$ given by $f(x) = \{x\}$. Now, suppose that $g : A \xrightarrow{\simeq} P(A)$ is a bijection between A and $P(A)$. Define a subset X of A by

$$X = \{x \in A | x \notin g(X)\}.$$

Since g is a bijection, there is some element y of A such that $g(y) = X$. If $y \in g(y)$, then $y \notin X = g(y)$, which is silly. On the other hand, if $y \notin g(y) = X$, then $y \in X$, by definition of X. This is also absurd. Thus, we have arrived at a contradiction, so there is no bijection between A and $P(A)$. ■

The computation for finite sets suggests that we define $2^{m(A)} = m(P(A))$. By the theorem, $m(A) < 2^{m(A)}$ for all sets A.

Lemma 3.3. *A countable union of sets of cardinality c has cardinality c.*

Proof. It suffices to prove that $m(\mathbb{N} \times \mathbb{R}) = c$. Let $f : \mathbb{R} \xrightarrow{\simeq} (0, 1)$ be a bijection. Then, define $g : \mathbb{N} \times \mathbb{R} \to \mathbb{R}$ by

$$g(n, x) = n + f(x).$$

This is an injection, so that $m(\mathbb{N} \times \mathbb{R}) \leq c$. On the other hand, the injection $\mathbb{R} \times \mathbb{N} \times \mathbb{R}$ given by $x \mapsto (1, x)$ show the opposite inequality. ■

This lets us consider the cardinality of functions.

Example 3.4. The set $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$ of all functions from $\mathbb{R}$ to $\mathbb{R}$ has cardinality bigger than c. Indeed, there is an injection $P(\mathbb{R}) \to \mathrm{Fun}(\mathbb{R}, \mathbb{R})$ given by sending a set A to the function

$$f(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $m(\mathrm{Fun}(\mathbb{R}, \mathbb{R})) \geq 2^c > c$.

Now, we are going to show that various sets have cardinality c. First, consider the set $\mathrm{Fun}(\mathbb{N}, \{0,1\})$ of function $\mathbb{N} \to \{0,1\}$. This set is bijective to the power set $P(\mathbb{N})$, by the same argument as in the example. Since every real number has an infinite binary sequence, there is an injection $\mathbb{R} \to \mathrm{Fun}(\mathbb{N}, \mathbb{R})$. So, $c \le 2^{\aleph_0}$. On the other hand, as in the cases of decimals, only binary expansions of rational numbers have any ambiguity. Since there are only countably many of these, in fact $c = 2^{\aleph_0}$!

Similarly, sequences of integers or of real numbers also have cardinality c. Since $\mathrm{Fun}(\mathbb{N}, \{0,1\}) \subseteq \mathrm{Fun}(\mathbb{N}, \mathbb{Z}) \subseteq \mathrm{Fun}(\mathbb{N}, \mathbb{R})$, it suffices to show that the cardinality of $\mathrm{Fun}(\mathbb{N}, \mathbb{R})$ is c. Briefly, it is enough to show that $\mathrm{Fun}(\mathbb{N}, (0,1))$ has cardinality $\le c$ (since it obviously has cardinality $\ge c$). Let $f : \mathbb{N} \to (0,1)$ be a sequence, and let $f(n) = 0.d_{n1}d_{n2}\ldots$ be a decimal representation. Create a new decimal $y = 0.d_{11}d_{21}d_{12}d_{31}d_{22}d_{13}\ldots$, by taking diagonals. This construction of a real number from a sequence of real numbers gives an injective (except at possibly a countable subset) map from $\mathrm{Fun}(\mathbb{N}, (0,1))$ to decimals. Hence the upper bound.

References

[1] A. N. Kolmogorov and S. V. Fomīn, *Introductory real analysis*, Dover Publications Inc., New York, 1975. Translated from the second Russian edition and edited by Richard A. Silverman; Corrected reprinting.

[2] K. A. Ross, *Elementary analysis: the theory of calculus*, Springer-Verlag, New York, 1980. Undergraduate Texts in Mathematics.

[3] W. Rudin, *Real and complex analysis*, 3rd ed., McGraw-Hill Book Co., New York, 1987.