MATH 54 - LECTURE 2: COUNTABLE AND UNCOUNTABLE SETS

DAN CRYTSER

Definition A function $f : X \to Y$ is injective (or one-to-one) if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. We call an injective function an injection.

Example The functions $f, g, h : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x$, $g(x) = x^3$ and $h(x) = e^x$ are all injective. The functions $p, q, r : \mathbb{R} \to \mathbb{R}$ given by $p(x) = 1$, $q(x) = x^2$, and $r(x) = \sin(x)$ are *not* injective: $p(0) = p(1)$, $q(-1) = q(1)$, $r(0) = r(\pi)$.

Definition A function $f : X \to Y$ is surjective (or onto) if for each $y \in Y$ we can find $x \in X$ such that $f(x) = y$. A surjective function is called a surjection.

Example The functions $f, g, h : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x$,$g(x) = x^3$, and $h(x) = e^{x^2} \sin(x)$ are all surjective (the last one is weird-looking). The functions, $p, q, r : \mathbb{R} \to \mathbb{R}$ given by $p(x) = 1$, $q(x) = e^x$, $r(x) = \arctan(x)$ are not surjective.

Definition A function $f : X \to Y$ is bijective (or a one-to-one correspondence) if it is both injective and surjective. Call such a function a bijection.

Example If X is a set, then the function $i_X : X \to X$ given by $i_X(x) = x$ is a silly but extremely important example of a bijection. We call it the *identity function* on X.

Example The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ is a bijection. The function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \arctan(x)$ is not a bijection because it is not surjective, although it is injective. The function $h(x) = x^3 - x$ is not a bijection because it is not surjective (check $h(1) = h(-1) = h(0)$), but it is surjective. That h is surjective is not trivial to prove, but if you look at the graph of the function it is evident.

Note that if $f : X \to Y$ is a bijection, then for each y in Y there is a unique x in X such that $f(x) = y$. The existence follows from surjectivity of f and the uniqueness from the injectivity.

Definition Let $f : X \to Y$ be a bijection. We define $f^{-1} : Y \to X$ by the rule

$$f^{-1}(y) = x \leftrightarrow f(x) = y.$$

We call this the *inverse function* of f.

Note: $f^{-1} \circ f = i_X$ and $f \circ f^{-1} = i_Y$.

Now we are in a position to state our definition of a finite set.

Definition A set X is finite if it is empty or if there is a bijection $f : X \to \{1, \ldots, n\}$ for some positive integer $n > 0$.

We can think of a bijection as an assignment of numbers as labels.

Corollary 1. *(Munkres: Corollary 6.7) Let B be a nonempty set. Then the following are equivalent:*

1. *B is finite*
2. *There is a surjection $f : \{1, \ldots, n\} \to B$ for some positive integer n.*
3. *There is an injection $g : B \to \{1, \ldots, m\}$ for some positive integer m.*

Example Our class is a finite set.

Definition A set is infinite if it is not finite.

Corollary 2. *Let B be a nonempty set. Then the following are equivalent:*

(1) *B is infinite*
(2) *There is an injection $f : \{1, \dots, n\} \to B$ for every positive integer n.*
(3) *There is a surjection $g : B \to \{1, \dots, m\}$ for every positive integer m.*

Example The set $\mathbb{N}$ is infinite, as is the set of all odd numbers, the set of all square numbers, the set of all numbers that end in 47 copies of the number 47, etc.

Definition Let X be an infinite set. We say that X is countably infinite if there is a bijection $f : X \to \mathbb{N}$. If X is finite or countably infinite, we say that X is countable. A set is uncountable or uncountably infinite if it is not countable.

Example The set $\mathbb{N}$ is countably infinite. The set $\mathbb{Q}$ of all rational numbers $\mathbb{Q} = \{m/n : \gcd(m, n) = 1\}$ is countable by the following argument:

arrange all the fractions (including unreduced fractions) in an infinite by infinite grid, so that the (m, n) entry is the fraction $\frac{m}{n}$. Go through and strike out all the unreduced fractions. Note that this means all the remaining fractions are distinct from one another, and that all the rational numbers appear as fractions on this list. Now zig-zag from $\frac{1}{1}$ down to $\frac{2}{1}$, then up and to the right to $\frac{1}{2}$, then to the right to $\frac{1}{3}$, then down and to the left through $\frac{2}{2}$, $\frac{3}{1}$, then down to $\frac{4}{1}$, then up and to the right through $\frac{3}{2}$, $\frac{2}{3}$, and $\frac{1}{4}$. And so on and so on. Every rational number appears on this infinite sequence precisely once, yielding a bijection between $\mathbb{N} = \{1, \dots\}$ and $\mathbb{Q}$.

Now, I would look more idiotic than I am comfortable with if I introduced such a fancy notion and term as "countably infinite" and you later discovered that every set in the universe was countable. Fortunately, such is not the case. The following theorem and argument/proof rate among the most famous and influential in the history of mathematics.

Definition The set $\prod_{i=1}^{\infty}\{0, 1\}$ is the set of all infinite sequences 101010001010.... all of whose entries lie in $\{0, 1\}$. Think of infinite binary strings.

Theorem 1. *(Cantor, 1891) The set $\prod_{i=1}^{\infty}\{0, 1\}$ of infinite binary strings is uncountable.*

Proof. The proof is remarkably simple and clever. We will denote elements of the collection of strings with overlines, like $\overline{x}_1$, $\overline{x}_2$, etc. For individual binary letters like $\{0, 1\}$, we use x_1, x_2, etc. For the first entry of the binary string $\overline{x}_1$, we will write $\overline{x}_{1,1}$, for the second entry of the binary string $\overline{x}_3$, we will write $\overline{x}_{3,2}$. Suppose that $\overline{x}_1, \overline{x}_2, \overline{x}_3, \dots$ is a sequence of infinite binary strings. Claim: there exists $\overline{x}_0$ which is not in the sequence. Proof of claim. Define $\overline{x}_{0,n} = 1 - \overline{x}_{n,n}$. As $\overline{x}_{n,n}$ is always in the set $\{0, 1\}$, clearly $\overline{x}_{0,n} \in \{0, 1\}$ as well. Now $\overline{x}_n$ and $\overline{x}_0$ differ in the nth spot.

So we have shown that every sequence of elements from the set $\prod_{i=1}^{\infty}\{0, 1\}$ misses some elements. A bijection $f : \mathbb{N} \to \prod_{i=1}^{\infty}\{0, 1\}$ would give an infinite sequence which did *not* miss any elements. So there cannot be any bijection between $\mathbb{N}$ and $\prod_{i=1}^{\infty}\{0, 1\}$. □

There is another theorem which shows why there must exist uncountable sets.

Theorem 2. *Let A be a set. There is no surjective function $g : A \to \mathcal{P}(A)$, where $\mathcal{P}(A)$ is the collection of all subsets of A.*

Proof. Suppose that $g : A \to \mathcal{P}(A)$ is a function. We show that there must exist some $B \subset A$ such that B is not in the image of g, that is, $B \neq g(a)$ for all $a \in A$. This in particular shows that there is no surjective map $g : A \to \mathcal{P}(A)$.

Let $B = \{a \in A : a \notin g(a)\}$. As $g(a) \subset A$ for each a, this makes sense as a definition.

Claim: $B \notin g(A)$. We prove this via a contradiction. Suppose that $B = g(a_0)$. Then we can certainly ask the question: is $a_0 \in B$? Suppose that $a_0 \in B$. Then $a_0 \notin g(a_0)$, because $B = g(a_0)$. But $a_0 \notin g(a_0)$ is precisely the condition which gives $a_0 \notin B$. So $a_0 \in B$ implies $a_0 \notin B$, which is an outrageous contradiction. Thus we must assume that B lies outside of the image of g. $\square$