SET THEORY - LECTURE 2

YOAV LEN

1. Functions

A function is an assignment from one set to another. The input set, the one where elements are coming from is called the *domain*. The output set, the one where elements are assigned to is called the *range* or *codomain*. We denote a function f by

$$f : A \to B,$$

where A is the domain, and B is the range. Note that not every element in B needs to be achieved by f. If $f(a) = b$, we say that b is the *image* of a.

Example 1.

$$f : \mathbb{Z} \to \mathbb{Z}, f(a) = 5k.$$

$$g : \{4, 3, 2\} \to \{5, 6, 7\}, g(4) = 5, g(3) = 7, g(2) = 6.$$

$$h : \mathbb{Q} \to \mathbb{R}, h(x) = 4x + 7.$$

Note that the image by h of every rational number is rational, so we could have defined the range of h to be $\mathbb{Q}$.

Useful terminology.

- We say that a function is *surjective* or *onto* if every element in the range is being hit. For instance, f above is not surjective, g is, and h is not. However, if we change the range of h to $\mathbb{Q}$ then it becomes surjective.
- We say that a function is *injective* or *one-to-one* if every element in the range is only being hit once. Namely, if no element in the range is the image of two different elements. All the functions f, g, h are injective. On the other hand, the functions

  $$k : \{4, 5, 6\} \to \{1, 2\}, k(4) = 1, k(5) = 2, k(6) = 2,$$

  $$s : \mathbb{R} \to \mathbb{R}, s(x) = x^2$$

  are not.
- A function is called a *bijection* or an *isomorphism* if it is both surjective and injective.

2. Size of sets revisited

If a finite set B has more items than a set A, then we can find an injective function from A to B. Similarly, we can find a surjective function from B to A. We therefore redefine what it means for one set to be "bigger" or "smaller" than another: A is smaller or equal than B, if there is an injection from A to B or a surjection from B to A. The sets A and B are of equal size if each of them is smaller or equal than the other. Equivalently, they are of the same size if there is a bijection between them.

We defined what it means for one set to be bigger than another, but what is the size of the set? A set A has *cardinality* k, if there is a bijection between A and the set $\{1, 2, \ldots, k\}$. In this case, we denote $|A| = k$. For instance, if $A = \{5, 7, 2, 3\}$, then $f(5) = 1, f(7) = 2, f(2) = 3, f(3) = 4$ is a bijection, so $|A| = 4$.

Why did we make our lives harder with this convoluted definition? Because this definition works for infinite sets as well!

Example 2. $|\{1, 2, 3\}| \leq |\mathbb{N}|$ because the function $f(1) = 1, f(2) = 2, f(3) = 3$ is an injection. Similarly, $|\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{R}|$, and $|\mathbb{N}| \leq |\{-1, 0, 1, 2, 3, \ldots\}|$.

A set is *infinite* if it is bigger or equal than every finite set. For instance, $\mathbb{N}$ is infinite. As we will see, Infinite sets tend to exhibit strange behaviour.

A slightly surprising fact. $\{-1, 0, 1, 2, 3, \ldots\} \leq \mathbb{N}$: define the function $f : \{-1, 0, 1, 2, 3, \ldots\} \to \mathbb{N}, f(n) = n + 1$.

A more surprising fact. $\mathbb{Z} \leq \mathbb{N}$. Why? Define $f(0) = 0, f(1) = 1, f(2) = -1, f(3) = 2, f(4) = -2$, and so on. Since also $|\mathbb{N}| \leq |\mathbb{Z}|$, we have $|\mathbb{N}| = |\mathbb{Z}|$. In fact, any set is smaller or equal $|\mathbb{N}|$ if we can 'enumerate' or 'count' its objects.

An even more surprising fact. $|\mathbb{Q}_{\geq 0}| \leq |\mathbb{N}|$! How can that be? Form a table as follows,

	1	2	3	...
1	2	3	4	...
2	1	2/3	2/4	...
3	3/2	1	3/4	...
4	4/2	4/3	1	...
⋮	⋮	⋮	⋮	⋮

Table 1. Table to test captions and labels

The entry in the i-th row and j-th column is i/j. All the positive rational numbers show up in the table. If we go along the diagonals, we eventually count all the rationals (some will be over counted, but that doesn't matter). By minor changes we can also count all the rationals. Conclusion: the set of rational numbers is as big as the set of natural numbers!

Maybe every infinite set has the same size? No!

3. Cantor's diagonal method

In fact, the set of real numbers is strictly bigger than the set of natural numbers. To prove this, we will show that every function from $\mathbb{N}$ to $\mathbb{R}$ is not surjective. Let f be such a function. Denote $a_1 = f(1), a_2 = f(a_2)$, and so on. We are going to construct a real number that is not in the image. Denote b_1 the first digit of a_1 after the decimal point plus 1. Let b_2 be the second digit of a_2 plus 1, and so on. Define a number r as $0.b_1b_2b_3, \ldots$... I claim that r is not in the image of f:

Is it $f(1)$? No, because its first digit is different from the first digit of a_1. Is it $f(2)$? No, because its second digit is different from the second digit of a_2. Is it $f(k)$ for some k? Again, no, because its k-th digit is different from the k-th digit of a_k. We have shown that f is not surjective. We haven't made any assumption on f, so every function from $\mathbb{N}$ to $\mathbb{R}$ is not surjective. Conclusion: $|\mathbb{N}| < |\mathbb{R}|$. Note, we have actually shown that $|\mathbb{N}| < |[0,1]|$. In fact, for every segment $[a,b]$, we have $|[a,b]| = |\mathbb{R}|$.

Let us give these cardinalities names. The cardinality of $\mathbb{R}$ is denoted using the Hebrew letter $\aleph$ (read *Aleph*). We use $\aleph_0$ for $\mathbb{N}$. What we have shown above is that $\aleph_0 < \aleph$. Also, for every finite number k, we have $k < \aleph_0 < \aleph$. A set of cardinality $\aleph_0$ is referred to as *countable*. The cardinalities are also called cardinal numbers. A set of cardinality higher than $\aleph_0$ is called *uncountable*.

Remark. Just like finite numbers, we can add, multiply and take powers of cardinal numbers. But that's a topic for another lecture series.

4. Other cardinalities

Is $\aleph$ the biggest cardinality? Are there any cardinalities between $\aleph_0$ and $\aleph$?

Theorem 3. *If A is any set, then $|\mathcal{P}(A)| > |A|$.*

Proof. First, we need to find an injection from A to $\mathcal{P}(A)$. Define $i : A \to \mathcal{P}(A)$ by $i(a) = \{a\}$. Then i is clearly an injection since for any $a \neq b$, we have $\{a\} \neq \{b\}$. Therefore, $|A| \leq |\mathcal{P}(A)|$.

To prove that the inequality is strict, we need to show that there is no surjection from A to $\mathcal{P}(A)$. Let $f : A \to \mathcal{P}(A)$ be any function. We need to find a set B that is not in the image. For every a, its image $f(a)$ is some subset of A. We can ask whether this subset contains a.

Define B to be the set of all the elements a of A, such that $f(a)$ does not contain a. I claim that B is not in the image of f, and in particular, f is not surjective. Let's assume for a second that B is in the image, so that $f(b) = B$ for some b. Is $b \in B$? If it is, then by the definition of B, $b \notin B$. But if it's not in B, then by the definition of B, $b \in B$. Contradiction! That means that the assumption that B is in the image of f is impossible. □

For any set A, we denote $\mathcal{P}(A) = 2^A$, and $|\mathcal{P}(A)| = 2^{|A|}$. Conclusion: for every set A, we have $|A| < 2^{|A|}$. Moreover, $\aleph_0 < 2^{\aleph_0}$, and $\aleph < 2^{\aleph} < 2^{2^{\aleph}} < 2^{2^{2^{\aleph}}} < \ldots$.

In the assignment, you will show that $2^{|\aleph_0|} = \aleph$. It can be shown that there is a cardinality which is greater than $\aleph_0$, such that there are no other cardinalities between them. This cardinality is called $\aleph_1$. Similarly, there are cardinal numbers $\aleph_2, \aleph_3, \aleph_4 \ldots$.

There is also a cardinality $\aleph_\omega$, which comes exactly after all of these. Then there is $\aleph_{\omega+1}$, and so on. So we have

$$0 < 1 < 2 < \ldots < \aleph_0 < \aleph_1 < \aleph_2 < \ldots < \aleph_\omega < \aleph_{\omega+1} < \ldots$$

Which one of these equals $\aleph$? In the 19-th century, Georg Cantor made the following conjecture.

Conjecture 1 (The Continuum hypothesis)**.** $\aleph = \aleph_1$.

This problem was one of the famous list of 23 presented by David Hilbert at the ICM in Paris in 1900. By the work of Gödel (1940) and Cohen (1963), it is shown that this hypothesis is independent of the other axioms of set theory. In other words, whether this statement is true or false, we can never prove it! It is common in set theory to take the hypothesis as an axiom.

Annoyingly, there are other facts that we can never prove or disprove. For instance, suppose that A and B are infinite sets. It is not always clear that either $|A| < |B|, |A| > B$, or $|A| = |B|$. A priori, all the functions between might be neither injective nor surjective. We need another axiom for that, known as the Axiom of Choice. In plain words, the axiom says that given a set, there is always an algorithm for choosing elements in it. This may seem obvious for the sets that we are familiar with, but it is not clear for sets that arise using a complicated definition. It is even less clear that we can continue choosing more and more elements ad infinitum.