Discrete Mathematics 14/01/2019

Lecture 2: Natural Numbers & Countability

Instructor: Goutam Paul *Scribe: Wribhu Banik*

1 Introduction

When we try to define a number n, we may assume there is a particular set A with n elements, and define *"n"* to be that set A only.

Now, the selection of the standard set A should be motivated by intuition and simplicity. Suppose a number $\boldsymbol{n}$ has already been defined as a set with n elements; now how does one define *"$n+1$"*?

We shall try to find a set B consisting of exactly $n+1$ elements. We already have a set $\boldsymbol{n}$ with exactly n elements in it. What should we use as an extra element to adjoin to them? An answer to this question is the number(set) $\boldsymbol{n}$ itself. The idea is to define $n+1$ to be the set consisting of the n elements of $\boldsymbol{n}$, together with $\boldsymbol{n}$, *i.e.*

$$n + 1 = n \cup \{n\}$$

Definition 1.1. For every set x we define the *Successor* x^+ of x to be the set obtained by adjoining x to the elements of x ; in other words,

$$x^+ = x \cup \{x\}$$

Construction of $\mathbb{N}$

With the idea of successor of a set x, we can now construct natural numbers. While defining 0 to be a set with zero elements *i.e.* ϕ, we write;

$$\mathbf{0} = \phi.$$

Now, according to our motivation behind defining natural numbers, every number $n+1$ is the successor of n. So 1 is defined to be the successor of 0. And similarly we go on defining 2, 3, ... by

$$\begin{aligned}
\mathbf{1} &= 0^+ = \phi \cup \{\phi\} = \{\phi\}(= \{0\}),\\
\mathbf{2} &= 1^+ = \{\phi\} \cup \{\{\phi\}\} = \{\phi, \{\phi\}\}(= \{0, 1\}),\\
\mathbf{3} &= 2^+ = \{\phi, \{\phi\}\} \cup \{\{\phi, \{\phi\}\}\} = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}(= \{0, 1, 2\})\\
&\vdots
\end{aligned}$$

Definition 1.2. We define $\mathbb{N}$, the set of Natural numbers by

- $0 \in \mathbb{N}$,
- $n \in \mathbb{N} \implies n^+ \in \mathbb{N}$, and nothing else belongs to $\mathbb{N}$.

2 Set Dominance

Definition 2.1. For sets X, Y if $\exists$ a 1-to-1 correspondence from X to Y, we say $X \sim Y$ *i.e.* X and Y are *equivalent* or *equipotent as sets.*

For sets X and Y, we say Y *dominates* X ($X \precsim Y$) if $\exists$ a 1-to-1 correspondence from X to a subset of Y *i.e.* X *is equivalent to a subset of* Y.

Clearly, $X \precsim Y$ implies there is an injection $f : X \to Y$.

If X and Y are sets such that $X \precsim Y$, but $Y \not\precsim X$, we shall say $X \prec Y$ *i.e.* Y *strictly dominates* X.

Question 2.1 For sets X and Y, do $X \precsim Y$ and $Y \precsim X$ together always imply $Y = X$?

Consider $Y = \mathbb{N}$ and $X = \mathbb{N}^* = \mathbb{N} \cup \{0\}$; and define $f : \mathbb{N}^* \to \mathbb{N}$ by $f(x) = x + 1$, $\forall x \in \mathbb{N}^*$.

Clearly f is linear in x, hence one-one. Again $f(x) = n \implies x = n - 1$, $\forall n$. As $n \in \mathbb{N}$, we have $x \geq 0$ *i.e.* $x \in \mathbb{N}^*$. So f is onto. Hence f is a bijection; *i.e.* $X \sim Y$.

If we take this f, we easily show that $X \precsim Y$ and $Y \precsim X$; but $Y \neq X$.

Question 2.2 For sets X, Y, Z; do $X \precsim Y$ and $Y \precsim Z$ together imply $X \precsim Z$?

If $X \precsim Y$, then there is a function $f : X \to Y$ such that f is a one-to-one correspondence between X and $A \subseteq Y$, i.e. $X \sim A$.

Again, if $Y \precsim Z$ then there is an injection $g : Y \to Z$. We may restrict g to the range of f(the set A) and define $g^* : A \to Z$ by $g^*(x) = g(x)\ \forall\ x \in A$, which is again one-one.

We compound g^* with f to get $g^* \circ f : X \to Z$, an injective map; and conclude is that X is equivalent to a subset of Z. In other words, if $X \precsim Y$ and $Y \precsim Z$, then $X \precsim Z$.

Theorem 2.2 (Schröder-Bernstein Theorem)**.** *If $X \precsim Y$ and $Y \precsim X$, then $Y \sim X$.*

The theorem states that, if X and Y are sets, and there are injections $f : X \to Y$ and $g : Y \to X$, then there is a bijection $h : X \to Y$.

3 Countability

Definition 3.1. For sets, countability and finiteness are defined as below;

- **Finiteness**: We say a set X is *finite* iff $X \prec \mathbb{N}$; *i.e.* X is finite if it is *equivalent* to some natural number n.

  X is called *infinite* iff $\mathbb{N} \precsim X$.

- **Countability**: We say a set X is *countable* if $X \precsim \mathbb{N}$. Now for a countable set X, we have the following cases:

  1. If $\mathbb{N} \not\precsim X$ *i.e.* $X \prec \mathbb{N}$, X is called *finite.*
  2. If $\mathbb{N} \precsim X$ *i.e.* $X \sim \mathbb{N}$, X is called *countably infinite.*

  And, if X is NOT countable, X is called *uncountable.*

Lemma 3.2. Any subset of a countable set is countable.

Proof. Suppose Y is countable *i.e.* $Y \precsim \mathbb{N}$, and let $X \subseteq Y$. X has the trivial bijection with X, which is a subset of Y, hence $X \precsim Y$.

Since $X \precsim Y$ and $Y \precsim \mathbb{N}$, we have $X \precsim \mathbb{N}$. So X is countable. □

Corollary 3.3. Superset of any uncountable set is uncountable.

Result 3.4. $\mathbb{Z}$ is countable.

Proof. Define, $f : \mathbb{N} \to \mathbb{N}$ by,

$$f(n) = (-1)^n \left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

To prove that f is a bijection, we first show that f is injective. Let us assume for $x, y \in \mathbb{N}$, we have $f(x) = f(y)$. Since the signs of both $f(x)$ and $f(y)$ are same, both x and y have to be of the same parity. We check the following cases:

- Both x and y are even. Then

$$f(x) = f(y) \implies \frac{x}{2} = \frac{y}{2} \implies x = y$$

- Both x and y are odd. Then

$$f(x) = f(y) \implies -\frac{x-1}{2} = -\frac{y-1}{2} \implies x = y$$

So f is injective. To prove f is surjective, we need to show for all $z \in \mathbb{Z}$ there is an $n \in \mathbb{N}$ where $f(n) = z$. We again check the cases:

- If $z > 0$ then $2z > 0$, so $2z \in \mathbb{N}$ and $2z$ is even, so

$$f(2z) = \frac{2z}{2} = z$$

- If $z \leq 0$ then $-2z + 1 > 0$, so $-2z + 1 \in \mathbb{N}$ and $-2z + 1$ is odd, so

$$f(-2z+1) = -\frac{-2z+1-1}{2} = z$$

Hence, f is surjective. Therefore f is a one-to-one correspondence between $\mathbb{N}$ and $\mathbb{Z}$; hence $\mathbb{N} \sim \mathbb{Z}$. So $\mathbb{Z}$ is countable. □

Lemma 3.5. *Let A, B, C, D be sets. If $A \sim C$ and $B \sim D$, then $A \times B \sim C \times D$.*

Proof. By definition of equivalence of sets, we know there exist bijections $f : A \to C$ and $g : B \to D$. It is natural to define a function $h : A \times B \to C \times D$ by $h(a, b) = (f(a), g(b))$.

It can be easily shown that h is a bijection from $A \times B$ to $C \times D$. □

Result 3.6. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. Define, $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by,

$$g(m, n) = 2^{m-1}(2n - 1)$$

Clearly g is well defined. Now suppose for two different points (m_1, n_1), (m_2, n_2) in $\mathbb{N} \times \mathbb{N}$ we have, $g(m_1, n_1) = g(m_2, n_2)$.

WLOG assume that $m_2 > m_1$; then

$$\begin{aligned} & g(m_1, n_1) = g(m_2, n_2) \\ \Longrightarrow\ & 2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1) \\ \Longrightarrow\ & (2n_1 - 1) = 2^{m_2-m_1}(2n_2 - 1) \end{aligned}$$

but then above equality implies an even number equals an odd number, which is a contradiction. So $m_2 \not> m_1$; similarly we can show that $m_1 \not> m_2$.

So, we must have $m_2 = m_1$, but that along with $g(m_1, n_1) = g(m_2, n_2)$ implies

$$(2n_1 - 1) = (2n_2 - 1) \implies n_1 = n_2$$

Hence $g(m_1, n_1) = g(m_2, n_2)$ implies $(m_1, n_1) = (m_2, n_2)$, $\forall\ (m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$. So g is injective. Again we observe that, given any $n \in \mathbb{N}$, we can decompose it in product of primes. That decomposition gives us a unique representation for any $n \in \mathbb{N}$. So any n can be written uniquely in the form,

$$n = 2^p q$$

where $p \in \mathbb{N}^*$, $q \in \mathbb{N}$ and $\gcd(2^p, q) = 1$.

Above representation gives us $p+1 \in \mathbb{N}$ and q is odd, *i.e.* $\frac{q+1}{2} \in \mathbb{N}$. Take $n^* = (p+1, \frac{q+1}{2})$ and look at $g(n^*)$, that is

$$g(p + 1, \frac{q + 1}{2}) = 2^{p+1-1}(2 \cdot \frac{q + 1}{2} - 1) = 2^p q = n$$

So for any $n \in \mathbb{N}$, there exists $n^* \in \mathbb{N} \times \mathbb{N}$ such that $g(n^*) = n$. So g is surjective. Hence g is a bijection and therefore, $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$; *i.e.* $\mathbb{N} \times \mathbb{N}$ is countable. □

Corollary 3.7. $\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \sim \mathbb{N}$ for any(finite) number of factors in the Cartesian product on the left, and therefore $\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$ is countable.

Corollary 3.8. $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, and therefore $\mathbb{Z} \times \mathbb{N}$ is countable.

Result 3.9. $\mathbb{Q}$ is countable.

Proof. We define the map $\phi : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ as follows:

$$\phi\Big(\frac{p}{q}\Big) = (p, q), \quad \text{where } p \in \mathbb{Z}, q \in \mathbb{N} \text{ and } \gcd(2^p, q) = 1$$

ϕ is clearly an injective map from $\mathbb{Q}$ to $\mathbb{Z} \times \mathbb{N}$, *i.e.* $\mathbb{Q} \precsim \mathbb{Z} \times \mathbb{N}$. Since, $X \precsim Y$, $Y \precsim Z \implies X \precsim Z$; we have $\mathbb{Q} \precsim \mathbb{Z} \times \mathbb{N} \precsim \mathbb{N}$.

Again, define $\varphi : \mathbb{N} \to \mathbb{N}$ by $\varphi(n) = n$, Clearly, φ is an injective map and therefore $\mathbb{N} \precsim \mathbb{Q}$.

Therefore from **Theorem 2.2** we have $\mathbb{Q} \sim \mathbb{N}$. So $\mathbb{Q}$ is countable. □

Theorem 3.10 (Cantor)**.** *For any set* X , $X \prec \mathcal{P}(X)$.

Corollary 3.11. $\mathcal{P}(\mathbb{N})$ is uncountable.

Lemma 3.12. $(0, 1)$ is uncountable.

Proof. Let us assume that the interval $(0, 1)$ is countable. Define, $f : \mathbb{N} \to (0, 1)$ by $f(n) = 10^{-n}$. Clearly f is injective and hence $\mathbb{N} \precsim (0, 1)$.

Again, $(0, 1)$ is countable implies $(0, 1) \precsim \mathbb{N}$. Since $X \precsim Y$ and $Y \precsim X$ imply $Y \sim X$, we have $(0, 1) \sim \mathbb{N}$. So there is a bijection $\varphi : \mathbb{N} \to (0, 1)$.

We can then write down all the decimal expansions of the reals in $(0, 1)$ in a list as follows:

$\varphi(1) = 0.$	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	$\dots$
$\varphi(2) = 0.$	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}	$\dots$
$\varphi(3) = 0.$	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	$\dots$
$\varphi(4) = 0.$	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}	$\dots$
$\varphi(5) = 0.$	a_{51}	a_{52}	a_{53}	a_{54}	a_{55}	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

where $\forall i, j$, $0 \le a_{ij} \le 9$, and there is no infinite string of 9's. That means the decimal representations are unique.

Define

$$b_i = \begin{cases} a_{ii} + 1 & \text{if } a_{ii} < 9 \\ 0 & \text{if } a_{ii} = 9 \end{cases}$$

and say, $s = 0.b_1b_2b_3b_4b_5\dots$, since $s \in (0, 1)$ and φ is a bijection, $\exists\ m \in \mathbb{N}$ such that $\varphi(m) = s$. But s differs from the m^{th} element of the list $\big(\varphi(m)\big)$ in the m^{th} decimal place.

So our assumption leads to a contradiction, and hence we conclude that $(0, 1)$ is uncountable. □

Lemma 3.13. Let $I_1 = [a, b]$, $I_2 = (c, d) \subseteq \mathbb{R}$ be any two intervals. Then, $I_1 \sim I_2 \sim \mathbb{R}$

Proof. We shall show that any closed interval $[a, b]$ in $\mathbb{R}$ is equivalent to $[0, 1]$. Define $f : [a, b] \to [0, 1]$ by

$$f(x) = \frac{x - a}{b - a}$$

f is a bijection and hence $[a, b] \sim [0, 1]$.

Similarly for an open interval (c, d) in $\mathbb{R}$, we define $g : (c, d) \to (0, 1)$ by $g(x) = \dfrac{x - c}{d - c}$ and it is again a bijection. Hence, $(c, d) \sim (0, 1)$.

Claim 3.14. $[0, 1] \sim (0, 1)$

Proof. Define, $\psi : [0,1] \to (0,1)$ by

$$\psi(x) = \begin{cases} \dfrac{1}{2} & \text{if } x = 0 \\ \dfrac{1}{2^{n+2}} & \text{if } x = \dfrac{1}{2^n} \text{ for } n \geq 0 \\ x & \text{otherwise} \end{cases}$$

We show that ψ defined as above is bijective.

Let $y \in (0,1)$ be any real. We check the following cases:

1. When $y = \dfrac{1}{2}$, we see that $\psi(0) = y$.
2. If y is of the form $\dfrac{1}{2^n}$ for $n > 1$, then $\dfrac{1}{2^{n-2}}$ is an obvious pre-image of y under ψ.
3. If y is not of the form $\dfrac{1}{2^n}$ for $n \geq 1$, the definition of ψ clearly implies $\psi(y) = y$.

Hence ψ is surjective.

To show that ψ is one-one, we observe that if $x \notin \{0,1\} \cup \{\dfrac{1}{2^n} : n \geq 1\}$, $\psi(x)$ is not of the form $\dfrac{1}{2^n}$. Suppose for $x_1, x_2 \in [0,1]$, we have $\psi(x_1) = \psi(x_2)$; we again consider the cases:

1. $\psi(x_i)$ is NOT of the form $\dfrac{1}{2^n}$. Then clearly

$$\psi(x_1) = \psi(x_2) \implies x_1 = x_2$$

2. $\psi(x_i)$ is of the form $\dfrac{1}{2^n}$. We see for $n = 1$, $\psi(x_i)$ cannot have a pre-image other than 0. And if $n > 1$ we have

$$\psi(x_1) = \psi(x_2) \implies \frac{1}{2^{n_1}} = \frac{1}{2^{n_2}} \implies x_1 = x_2$$

So ψ is an injection and therefore a bijective map. We get, $[0,1] \sim (0,1)$. □

Now we have proved that for any intervals I_1,$I_2 \in \mathbb{R}$(where I_1 is open and I_2 is closed respectively), $I_1 \sim (0,1) \sim [0,1] \sim I_2$.

We take the interval $I = (-\frac{\pi}{2}, \frac{\pi}{2})$ and define $h : I \to \mathbb{R}$ by $h(x) = \tan(x)$ which is a bijection, hence $I \sim \mathbb{R}$. But since $I \sim (0,1)$ we have $\mathbb{R} \sim (0,1) \sim [0,1]$.

Therefore, $\mathbb{R} \sim I_1 \sim I_2$. □

Corollary 3.15. Any interval in $\mathbb{R}$ is uncountable.

Theorem 3.16. $\mathbb{R}$ *is uncountable.*

Proof. We have already shown that $\mathbb{R} \sim (0,1)$ and $(0,1)$ is uncountable.

Together they will imply that $\mathbb{R}$ is uncountable. □

Theorem 3.17. $\mathcal{P}(\mathbb{N}) \sim (0, 1)$.

Proof. For each subset $X \in \mathcal{P}(\mathbb{N})$, we associate it with a decimal number, namely

$$X \to 0.x_1x_2x_3x_4\ldots$$

where $\forall i \in \mathbb{N}$, $x_i = 1$ iff $i \in X$. Otherwise, $x_i = 0$, and there is no infinite string of 1's. For example, the set $\{1, 2, 3, 5, 6, 8, 9\}$ has the decimal representation, $0.11101101100\ldots$; again take any decimal y of the above form, then looking at the i^{th} decimal place, we can check whether the number i is in a set or not. The we can construct a set Y as

$$Y = \{i \in \mathbb{N} : y_i = 1\}$$

For example the number $0.101011011100\ldots$ denotes the set $\{1, 3, 5, 6, 8, 9, 10\}$.

Say B contains all decimal numbers of the above form, then B corresponds to the set of all the subsets of $\mathbb{N}$ and this correspondence is one-to-one, *i.e.* $B \sim \mathcal{P}(\mathbb{N})$.

Claim 3.18. $B \sim (0, 1)$.

Proof. As per definition, B contains all the decimal numbers whose digits are either 0 or 1. Clearly, B is the set of all decimal numbers written in their binary representations.

Since there is NO decimal number in B with an infinite sequence of 1's, $1 \notin B$. We have the set of all decimal reals written in decimal representation, which does not contain 1 namely, $[0, 1)$. We have the two results,

- $B \sim [0, 1)$, since set of all decimal reals in their binary representation is equivalent to that in decimal representations.
- $[0, 1) \sim (0, 1)$, which is true as we define $f : [0, 1) \to (0, 1)$ by,

$$f(x) = \begin{cases} \frac{1}{2} & \text{if } x = 0 \\ \frac{1}{2^{n+1}} & \text{if } x = \frac{1}{2^n} \\ x & \text{otherwise} \end{cases}$$

  and show f is bijection (Check).

These results give that, $B \sim [0, 1) \sim (0, 1)$. □

Since $\mathcal{P}(\mathbb{N}) \sim B$ and $B \sim (0, 1)$, we get $\mathcal{P}(\mathbb{N}) \sim (0, 1)$,and therefore $\mathcal{P}(\mathbb{N})$ is uncountable. □

Lemma 3.19. $(0, 1) \times (0, 1) \sim (0, 1)$.

Proof. It is sufficient to show that $(0, 1) \precsim (0, 1) \times (0, 1)$ and $(0, 1) \times (0, 1) \precsim (0, 1)$, since by **Theorem 2.2**, that will imply $(0, 1) \times (0, 1) \sim (0, 1)$.

We first assume that for the decimal representation of a real number in $(0, 1)$ is, $x = 0.x_1x_2x_3\ldots$ where an infinite string of 9's does not occur. Therefore $\forall x \in (0, 1)$ we have one unique decimal representation.

We define $g : (0,1) \times (0,1) \to (0,1)$ by

$$g(0.x_1x_2x_3\dots, 0.y_1y_2y_3\dots) = 0.x_1y_1x_2y_2x_3y_3\dots$$

To see that g is injective we take $(x,y),(z,w) \in (0,1)$ and assume that $g(x,y) = g(z,w)$. hence we get

$$0.x_1y_1x_2y_2x_3y_3\dots = 0.z_1w_1z_2w_2z_3w_3\dots$$

Since these two representations are unique, we get $\forall i$, $x_i = z_i$ and $y_i = w_i$, *i.e.* $x = z, y = w$. So g is an injection, and hence $(0,1) \times (0,1) \precsim (0,1)$.

We define $h : (0,1) \to (0,1) \times (0,1)$ by $h(x) = \left(x, \frac{1}{2}\right)$ and quite clearly, h is injective. So $(0,1) \precsim (0,1) \times (0,1)$. Since $X \precsim Y$, $Y \precsim X \implies X \sim Y$, we get $(0,1) \times (0,1) \sim (0,1)$. And $(0,1) \times (0,1)$ is uncountable. □

Corollary 3.20. $(0,1) \times (0,1) \times \cdots \times (0,1) \sim (0,1)$ for finite number of factors in the Cartesian product on the left.

Corollary 3.21. $\mathbb{R}^n \sim \mathbb{R}$.

Proof. We have previously shown that $\mathbb{R} \sim (0,1)$, that implies $\mathbb{R} \times \mathbb{R} \sim (0,1) \times (0,1)$.

Previous lemma implies, $(0,1) \times (0,1) \sim (0,1)$, and thence gives,

$$\mathbb{R} \sim (0,1) \sim (0,1) \times (0,1) \sim \mathbb{R} \times \mathbb{R}$$

Therefore $\mathbb{R}^2 \sim \mathbb{R}$, which also implies $\mathbb{R}^2$ is uncountable.

Similarly we can show that $\mathbb{R}^n \sim \mathbb{R}$ for any n, and we conclude $\mathbb{R}^n$ is uncountable. □