Countability Of Sets

Task: **Understand what it means for a set to be countable, countably infinite, uncountably infinite. Show that the set of all languages over a finite alphabet is uncountably infinite, whereas the set of all regular languages over a finite alphabet is countably infinite.**

We want to understand sizes of sets. In the unit on functions last term, when we looked at functions defined on finite sets, we wrote down a set A with n elements as $A = \{a_1, ..., a_n\}$**.**
This notation mimics the process of counting : a_1 **is the first element of** A, a_2 **is the second element of** A**, and so on up to** a_n **is the** n^{th} **element of A. In other words, another way of saying A is a set of** n **elements is that there exists a bijective function** $f : A \longrightarrow \{1, 2, ..., n\}$**, let** $J_n = \{1, 2, ..., n\}$.

Def: **A set** A **has** n **elements** $\iff \exists f : A \longrightarrow J_n$ **a bijection**
NB: **This definition works** $\forall n \leq 1, n \in \mathbb{N}^*$

Notation: $\exists f : A \longrightarrow J_n$ **a bijection is denoted as** $A \sim J_n$
More generally, $A \sim B$ **means** $\exists f : A \longrightarrow B$ **a bijection, and it is a relation on sets. In fact, it is an equivalence relation (check!).** $[J_n]$ **is the equivalence class of all sets A of size** n**, i.e.** $\#(A) = n$

A set A is finite if $A \sim J_n$ for some $n \in \mathbb{N}^*$ or $A = \emptyset$.

A set A is infinite if A is not finite.

Examples: $\mathbb{N}, \mathbb{Q}, \mathbb{R}$**, etc.**

To understand sizes of infinite sets, generalise the construction above.

Let $J = \mathbb{N}^* = \{1, 2, ...\}$

Def: A set A is countably infinite if $A \sim J$.

Def: A set A is uncountably infinite if A is neither finite nor countably infinite.

In fact, we often treat together the cases A is infinite or A is countably infinite since in both of these cases the counting mechanism that is so familiar to us works. Therefore, we have the following definition:

Def: A set A is countable if A is finite ($A \sim B$ or $A = \emptyset$) or A is countably infinite ($A \sim B$).

There is a difference in terminology regarding countability between CS sources (textbooks, articles, etc.) and maths sources. Here is the dictionary:

CS	Maths
countable	at most countable
countably infinite	countable
uncountably infinite	uncountable

It's best to double check which terminology a source is using.

Goal: Characterise $[\mathbb{N}]$, the equivalence class of countably infinite sets, and $[\mathbb{R}]$, the equivalence class of uncountably infinite sets the same size as $\mathbb{R}$.

Bad News Both $[\mathbb{N}]$ and $[\mathbb{R}]$ consist of infinite sets.

Good News We only care about these two equivalence classes

Nb These are uncountably infinite sets of size bigger than $\mathbb{R}$ that can be obtained from the power set construction, but it is unlikely you will see them in your CS coursework.

To characterise $\mathbb{N}$ we need to recall the notion of a sequence:

Def: A sequence is a set of elements $\{x_1, x_2, ...\}$ indexed by J, i.e. $\exists f : J \longrightarrow \{x_1, x_2, ...\}$ such that $f(n) = x_n \ \forall n \in J$.

Recall that sequences and their limits were used to define various notions in calculus (differentiation, interpretation, etc.) Also calculators use sequences in order to compute with various rational and irrational numbers.

Examples

1. $\pi \simeq$ 3.1415... i.e. instead of π we can work with the following sequence of rational numbers :

$x_1 = 3$, $x_2 = 3.1$, $x_3 = 3.14$, $x_4 = 3.141$, $x_5 = 3.1415, ...$ $\lim_{n\to\infty} x_n = \pi$

π **is irrational** $\pi \in \mathbb{R}\backslash\mathbb{Q}$

2. $\frac{1}{3} \simeq$ 0.333... means we can set up the sequence of rational numbers $x_1 = 0$, $x_2 = 0.3$, $x_3 = 0.33$, $x_4 = 0.333$, $x_5 = 0.3333$ **etc. such that** $\lim_{n\to\infty} x_n = \frac{1}{3}$**.**

Note that $\frac{1}{3} \in \mathbb{Q}$.

Restatement of the definition of countably infinite: A set A is countably infinite if its elements can be arranged in a sequence $\{x_1, x_2, ...\}$. This is another of saying A is in bijective correspondence with J, i.e $\exists f : A \longrightarrow J$ **a bijection, namely $A \sim J$.**

Application of the restatement: $\mathbb{Z} \sim \mathbb{N}$

Indeed we can write $\mathbb{Z}$ as a sequence since $\mathbb{Z} = \{0, 1, -1, 2, -2, ...\}$ so $\mathbb{Z} \in [\mathbb{N}]$, **$\mathbb{Z}$ is countably infinite like $\mathbb{N}$.**

Big difference between finite and infinite sets:

Let A,B be finite sets such that $A \subsetneq B$, i.e. $A \subset B$ but $A \neq B$. Then $A \nsim B$ **since $\#(A) < \#(B)$ and $J_n \nsim J_m$ if $n \neq m$.**

Let A, B be infinite sets such that $A \subsetneq B$, $A \subset B$, but $A \neq B$.

It is possible that $A \sim B$. We saw this behaviour in Hilbert's hotel problem (Hilbert's Paradox of the Grand Hotel): $\mathbb{N}^* \longrightarrow \subsetneq \mathbb{N}$

but $\mathbb{N} \sim \mathbb{N}^*$ via the bijection $f : \mathbb{N} \longrightarrow \mathbb{N}^*$ given by $f(n) = n + 1$ so

$\{0, 1, 2, ...\} \sim \{1, 2, 3, ...\}$

In the same vein, we get the following result:

<u>Theorem:</u> Every infinite subset of a countably infinite set is itself countably infinite.

<u>Proof:</u> Let $E \subseteq A$ be the subset in question, where E is infinite and A is countably infinite. A is countably infinite $\iff$ $A \sim J$ $\iff$ $A =$

$\{x_1, x_2, ...\}$

To show E is countably infinite, we want to show we can represent $E = \{x_{n1}, x_{n2}, ...\}$. We construct this sequence of n_j's from the indices of the elements of A in the enumeration $\{x_1, x_2, ...\}$

Let n_1 be the smallest integer in J such that $x_{n_1} \in E \subseteq A$.

We construct the rest of the sequence of $n_j' s$ by induction. Say we have constructed $n_1, n_2, ..., n_{k-1} \in \mathbb{N}^*$ Let n_k be the smallest integer greater than n_{k-1} such that $x_{n_k} \in E$. By construction $n_1 < n_2 < ...$ and

$E = \{x_{n_1} < x_{n_2} < ...\}$ $(Q.E.D)$

Remark: $\{x_{n_1}, x_{n_2}, ...\}$ **is called a subsequence of** $\{x_1, x_2, ...\}$

Algorithmic restatement of previous proof:

Let $A = \{x_1, x_2, ...\}$ **be an enumeration of** A **(i.e. writing the countably infinite set** A **as a sequence). We process** $\{x_1, x_2, ...\}$ **as a queue. First look at** x_1**. If** $x_1 \in E$**, keep** x_1 **and let** $n_1 = 1$**; otherwise, discard** x_1**. Process each** x_i **in turn, keeping only those that are in** E**. Their indices form the subsequence** $\{n_j\}_{j=1,2,...}$ **where** $E = \{x_{n_1}, x_{n_2}, x_{n_3}, ...\}$**.**

Next, we want to show $\mathbb{Q} \sim \mathbb{N}$**, the set of rational numbers is countably infinite.**

Notation: **A sequence** $\{x_{n_1}, x_{n_2}\}$ **can also be denoted by** $\{x_i\}_{i=1,2,...}$

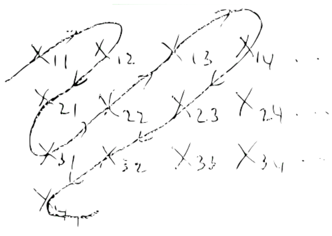
Theorem: **Let** $\{A_n\}_{n=1,2,...}$ **be a sequence of countably infinite sets.**

Let $S = \bigcup\limits_{n=1}^{\infty} A_n$. **Then** S **is countably infinite.**

Proof: **Each** A_n **is countably infinite** $\iff$

$A_n \sim J \ \forall n \geq 1 \iff A_n = \{x_{n_k}\}_{k=1,2,...} = \{x_{n_1}, x_{n_2}, x_{n_3}, ...\}$

We use two indices like for the entries of a matrix. The first index tells us which A_n **set the element belongs to, while the second index tells us where the element is in the enumeration (the counting) of** A_n**.**



$\{x_{11}, x_{12}, x_{21}, x_{31}, x_{22}, x_{13}, x_{14}, x_{23}, x_{32}, x_{41}, ...\} = \bigcup_{n=1}^{\infty} A_n = S$ **is countably infinite because even if some x_{ij}'s are the same.**

$A_n \subseteq S \ \forall n \geq 1$ **and** $A_n \sim J$

Corollary 1: Suppose an indexing set I is countable, and $\forall i \in I$, A_i is countable, then $T = \bigcup_{i \in I}$ is countable.

Proof: The biggest set we can obtain is when I is countably infinite and each A_i is countably infinite. By the previous theorem, T is countably infinite in that case. Therefore T is at most countably infinite (may be finite if I is finite and each A_i is finite), so T is countable.$(Q.E.D)$

Corollary 2: Let A be a countably infinite set, and let $A^n = A \times ... \times A = \{(a_1, a_2, ..., a_n) | a_1, a_2, ..., a_n \in A\}$.

Then A^n is countably infinite.

Proof: We use induction:

Base case $n = 1$ $A^1 = A \sim J \implies A^1$ **is countably infinite**

Inductive step **Assume A^{n-1} is countably infinite.**

$A^n = A^{n-1} \times A = \{(b,a)|b \in A^{n-1}, a \in A\}$

$\forall b \in A^{n-1}$ $S_b = \{(b,a) \in A^n | a \in A\} \sim J \sim A \implies S_b$ **is countably infinite.**

$A^n = \bigcup_{b \in A^{n-1}} S \sim J$ **by Corollary 1, so A^n is indeed countably infinite as claimed.** $(Q.E.D)$

Corollary 3: $\mathbb{N}^n$ **is countably infinite** $\forall n \geq 1$.

Proof: $\mathbb{N} \sim J$ **so the result follows form Corollary 2.** $(Q.E.D)$

Corollary 4: $\mathbb{Z}^n$ **is countably infinite** $\forall n \geq 1$.

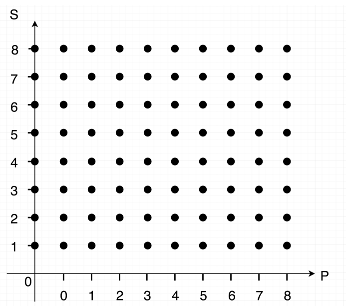
Proof: **We showed $\mathbb{Z} \sim J$, so the result follows from Corollary 2.** $(Q.E.D)$

Corollary 5: $\mathbb{Q}$ **is countably infinite**

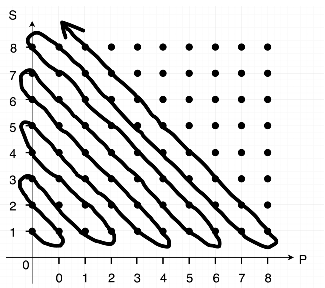
Proof: $\mathbb{Q} = \{\frac{p}{q} \; |q \neq 0, \; p,q \in \mathbb{Z}, (p,q) = 1$ **(no common factors)**$\}$ **, but we can represent $\mathbb{Q}$ as** $\frac{\{(p,q) \;|\; q \neq 0 \;\; p,q \in \mathbb{Z}\}}{\sim} \subseteq \mathbb{Z}^2$, **where** $(p_1, q_1) \sim (p_2, q_2) \iff \frac{p_1}{q_1} = \frac{p_2}{q_2} \iff p_1 \; q_2 = p_2 \; q_1$ **by cross multiplication. We also know $\mathbb{Z} \subseteq \mathbb{Q}$ (let $q = 1$). Therefore, $\mathbb{Q}$ is sandwiched between $\mathbb{Z} = \mathbb{Z}^1$ and $\mathbb{Z}^2$, both of which are countably infinite $\implies \mathbb{Q}$ is countably infinite.** $Q.E.D$

Remark:

We can give a visual representation of the previous argument as follows:



The dots are pairs (p,q) w/ $q \neq 0$ $p, q \in \mathbb{Z}$, which form a lattice. We can use the snake trick from the theorem to show that the positive rational numbers $Q^{+} = \{\frac{p}{q} \in \mathbb{Q} \mid \frac{p}{q} > 0\}$ are countably infinite.



Similarly we can show $\mathbb{Q}^{-} = \{\frac{p}{q} \in \mathbb{Q} \mid \frac{p}{q} > 0\}$ is countably infinite.

Then $\mathbb{Q} = \mathbb{Q}^{-} \cup \{0\} \cup \{\mathbb{Q}^{+}\}$ is countably infinite by Corollary 1.

Next, show that the set of sequences of 0's and 1's is uncountably infinite. We will use this result to show other sets are uncountably infinite.

Theorum: **Let** A **be the set of all sequences** $s = \{x_1, x_2, ...\} = \{x_n\}_{n=1,2,3...}$ **such that** $x_n \in \{0, 1\}\ \forall n \geq 1$. **Then** A **is uncountably infinite**

Remark: **This result is proven via a clever construction, which is due to Georg Cantor (1845 - 1918). A very famous German mathematician who invented set theory. Cantor also came up with the diagonal argument (snake trick) we used to prove a countably infinite union of countably infinite sets is countably infinite, the idea that sizes of sets should be understood via bijections** $(A \sim B for A, B sets)$. **As well as the notions of countably infinite and uncountably infinite.**

Proof: **Assume A is countable** $\iff A = \{s_1, s_2, ...\}$ **,where** $s_j = \{x_n^j\}_{n=1,2,...}$ **for** $x_n^j = 0$ **or** $x_n^j = 1$. **We will now construct a sequence** s_0 **of** $0's$ **and** $1's$ **that cannot be in the enumeration** $\{s_1, s_2, ...\}$. **Let** s_0 **be such that**

$$x_j^0 = \begin{cases} 1, & \text{if } x_j^j = 0. \\ 0, & \text{if } x_j^j = 1. \end{cases} \tag{1}$$

In other words s_0 **differs form each** s_j **in the** j^{th} **element**
$\implies s_0 \notin \{s_1, s_2, ...\}$, **but** s_0 **is a sequence of 0's and 1's** $\Rightarrow s_0 \in A \Rightarrow\Leftarrow$