CARDINALITY, COUNTABLE AND UNCOUNTABLE SETS
PART ONE

With the notion of bijection at hand, it is easy to formalize the idea that two *finite* sets have the same number of elements: we just need to verify their elements can be placed in pairwise correspondence; that is, that there is a bijection between them. It is then natural to generalize this to infinite sets, and indeed to arbitrary sets.

Definition 1. Let A, B be sets. We say A and B are *equipotent* (or have the same *cardinality*) if there exists a bijection $f : A \to B$. We'll use the *notation* $A \sim B$ in this case.

Clearly $A \sim A$, $A \sim B \to B \sim A$ and $A \sim B \wedge B \sim C \to A \sim C$. So this looks very much like "an equivalence relation in the class of all sets", and indeed this can be formalized in axiomatic set theory, but we'll leave that for the advanced course.

The notion of "cardinality" of a set was develop in the late 19th/early 20th centuries by the German mathematician Georg Cantor, motivated by questions arising from Analysis (specifically, Fourier series). One is led to consider some unusual subsets of the real line, and it is then natural to wonder if one can give a precise meaning to the intuitive feeling that some infinite sets have "more elements" than other infinite sets (for example, the real line seems to have "more elements" than, say, the rational numbers in it.)

In this handout we'll use the notation:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}, \quad \mathbb{I}_n = \{1, 2, 3 \ldots, n\}.$$

Definition 2. Let A be a non-empty set. A is *finite*, with cardinality N, if $A \sim \mathbb{I}_N$. A is *countably infinite* if $A \sim \mathbb{N}$. In either case, A is said to be *countable.* If A is not countable, we say A is *uncountable.*

Ex. 1. $\mathbb{Z} \sim \mathbb{N}$.
We "count" the elements of $\mathbb{Z}$ as follows:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots\}.$$

This corresponds to the following bijection $f : \mathbb{N} \to \mathbb{Z}$:

$$f(n) = n/2, n \text{ even} \;; \quad f(n) = -(n-1)/2, n \text{ odd} \;.$$

Ex. 2. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

This may look counterintutive at first: there are "just as many" ordered pairs of natural numbers as there are natural numbers themselves! This can be proven through Cantor's "diagonal count":

$$\mathbb{N} \times \mathbb{N} = \{(1,1),(1,2),(2,1),(1,3),(2,2),(3,1),(1,4),(2,3),(3,2),(4,1),\ldots\}.$$

That is, we order the pairs according to the sum of the two coordinates, and within each sum list them in the order of the first coordinate. This corresponds to the bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by:

$$f(j,k) = \frac{1}{2}(j+k-1)(j+k-2)+j.$$

This example generalizes to:

$$\mathbb{N} \times \mathbb{N} \ldots \times \mathbb{N} \sim \mathbb{N},$$

for any (finite) number of factors in the cartesian product on the left. This follows from the next example.

Ex. 3. 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 equipotent, 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 $h(a,b) = (f(b), g(c))$. We leave it as an exercise to show that h is a bijection from $A \times B$ to $C \times D$.

The following results are often used to establish that given sets are countably infinite.

Proposition 1. Let $A \subset \mathbb{N}$. Assume A is neither empty nor finite. Then A is countably infinite (that is, $A \sim \mathbb{N}$).

Proof. Define a function $f : \mathbb{N} \to A$ as follows. Let $f(1)$ be the smallest element of A (in the usual ordering of $\mathbb{N}$). This exists by the Well-Ordering Principle, since $A \neq \emptyset$. Then let $f(2)$ be the smallest element in $A \setminus \{f(1)\}$. Note that this set is also non-empty (since A, being infinite, cannot equal $\{f(1)\}$), so the Well-Ordering Principle applies again.

In general, given $\{f(1), \ldots, f(n)\}$, we let $f(n+1)$ be the smallest element in $A \setminus \{f(1), \ldots, f(n)\}$ (which is a non-empty subset of $\mathbb{N}$). This defines the function f inductively; f is *injective*, since from the construction we have:

$$f(1) < f(2) < f(3) < \ldots < f(n) < f(n+1) < \ldots$$

That f is *onto* can be proved by contradiction: assume $A \setminus f(\mathbb{N}) \neq \emptyset$ and let a be the smallest element in this set. Thus $a - 1 = f(N)$ for some $N \in \mathbb{N}$. Then $f(N+1)$ is the smallest element in $A \setminus \{f(1), \ldots, f(N)\}$, so $f(N+1) > a - 1$ (since $a - 1 = f(N)$ is in this set). Thus $f(N+1) \geq a$; but since $a \in A \setminus \{f(1), \ldots, f(N)\}$ we can't have $f(N+1) > a$. Thus $f(N+1) = a$, contradicting $a \notin f(\mathbb{N})$.

Corollary 1. If B is countable and $A \subset B$, $(A \neq \emptyset)$, then A is countable.

Proof. If B is finite, A is clearly finite. If B is countably infinite, there is a bijection $f : B \to \mathbb{N}$. Then $f(A) \subset \mathbb{N}$, so by the proposition $f(A)$ is either finite or countably infinite. Since $A \sim f(A)$ (given that f is injective), it follows that A is countable.

As the following result shows, to establish that a set A is countable it is enough to find a function from $\mathbb{N}$ *onto* A, or a one-to-one function from A into $\mathbb{N}$; this is easier than exhibiting a bijection $\mathbb{N} \to A$.

Proposition 2. Let A be a nonempty set. The following are equivalent:
(1) A is countable (that is, there is a bijection $h : A \to \mathbb{I}_N$, or $h : A \to \mathbb{N}$.)
(2) There exists $f : \mathbb{N} \to A$ surjective.
(3) There exists $g : A \to \mathbb{N}$ injective.

Proof. (1) $\Rightarrow$ (2): If A is countably infinite, we may take $f = h$. If A is finite with cardinality N, consider the surjective function:

$$f_N : \mathbb{N} \to \mathbb{I}_N, \quad f(n) = n \text{ for } 1 \leq n \leq N, \quad f(n) = N \text{ for } n \geq N.$$

Then $f = h^{-1} \circ f_N : \mathbb{N} \to A$ is surjective.

(2) $\Rightarrow$ (3). Let f be as in (2), and define $g : A \to \mathbb{N}$ as follows. Given $a \in A$, the preimage $f^{-1}(\{a\})$ is a non-empty subset of $\mathbb{N}$ (since f is surjective). By the Well-Ordering Principle, this set has a smallest element; we let $g(a)$ be this smallest element. g is injective, since for two elements $a_1 \neq a_2$ in A the preimages $f^{-1}(\{a_1\})$ and $f^{-1}(\{a_2\})$ are *disjoint*, and hence their smallest elements are distinct.

(3) $\Rightarrow$ (1). Let g be as in (3). $g(A)$ is a non-empty subset of $\mathbb{N}$, hence (by Proposition 1) $g(A)$ is countable. Since $A \sim g(A)$ (given that A is injective), it follows that A is countable.

Remark 1. Note that the statement of Propositon 2 remains true if we replace $\mathbb{N}$ by an arbitrary countably infinite set (using composition of functions.)

Corollary 2. $\mathbb{Q} \sim \mathbb{N}$: the set of rational numbers is countably infinite.

Proof. Define $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ by $f(p,q) = p/q$. Since each rational number is of the form p/q for some $p \in \mathbb{Z}$ and some $q \in \mathbb{N}$ (not necessarily unique ones), it follows that f is surjective. Since $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$ (using examples 1,2, and 3), it follows from part (2) of Proposition 2 and Remark 1 that $\mathbb{Q}$ is countable (hence countaly infinite.)

Corollary 3. Let $A_1, A_2, A_3, \ldots$ be non-empty countably infinite sets (not necessarily disjoint), Then their union is countably infinite:

$$\bigcup_{i \geq 1} A_i \sim \mathbb{N}.$$

Proof. We're given that, for each $i \in \mathbb{N}$, there exists a bijection $f_i : \mathbb{N} \to A_i$. Define

$$f : \mathbb{N} \times \mathbb{N} \to \bigcup_{i \geq 1} A_i, \quad f(i,j) = f_i(j).$$

To see that f is surjective, let $x \in \bigcup_{i \geq 1} A_i$ be arbitrary. Then $x \in A_i$ for some $i \in \mathbb{N}$, so $x = f_i(j)$ for some $j \in \mathbb{N}$; thus $x = f(i,j)$.

Before describing the proof of the fact that $\mathbb{R}$ is uncountable, we need to review some basic facts about decimal expansions of real numbers. This expansion is not unique. For example:

$$0.9999999... = 1.$$

This equality is not approximate, it is **EXACT**, a fact that some students find surprising; both sides are different decimal representations (in base 10) of *the same* rational number. One way to see this is:

$$0.99999... = 9 \sum_{j=1}^{\infty} 10^{-j} = \frac{9/10}{1 - 1/10} = 1,$$

using the well-known formula for the sum of a convergent geometric series, $\sum_{j=0}^{\infty} aq^{-j} = \frac{a}{1-q}$ if $|q| < 1$. The same would happen for any rational number with a terminating decimal expansion, for example:

$$0.1234567 = 0.12345669999999...$$

Thus if we want to assign to each real number a unique decimal expansion, we need to make a choice; for the purpose of the argument that follows, we'll choose the "non-terminating expansion", that is, the one that is eventually an infinite sequence of 9's.

With this choice, it is then a *theorem* about the real numbers (which won't be proved here) that every real number in the interval $(0,1]$ has a unique non-terminating expansion: an infinite sequence taking values in $\{0,1,\dots,9\}$, arbitrary except tfor the fact that it can't be eventually all 0's. Thus, there is a bijection between the interval $(0,1]$ and the set:

$$\{f:\mathbb{N}\to\{0,1,\dots,9\}|(\forall n\in\mathbb{N})(\exists m>n)(f(m)\neq 0)\}.$$

Under this correspondence between nonterminating decimal expansions and sequences we have, for example:

$$0.314515199999... \longleftrightarrow (3,1,4,5,1,5,1,9,9,9,9...)$$

Remark 2. This representation can be done in an arbitrary base r, corresponding to sequences taking values in $\{0,1,2,...,r-1\}$; for example, using base 2 we get a bijective correspondence between real numbers in $(0,1]$ and those infinite sequences of 0s and 1s which are not eventually 0.

We are now ready to state and prove Cantor's theorem.

Theorem. (G.Cantor, 1874). The set $\{x\in\mathbb{R}|0<x\leq 1\}$ is uncountable.

Proof. Arguing by contradiction, suppose a bijection $f:\mathbb{N}\to(0,1]$ exists. Listing the $f(n)$ by their nonterminating decimal expansions, we build a bi-infinite array:

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

Given the array we can explicitly exhibit a real number $x\in(0,1]$ that it can't possibly include. Namely, let x be the number with nonterminating decimal expansion:

$$x=0.d_1d_2d_3d_4d_5...$$

where the d_n are defined using the diagonal entries of the array, modified as follows:

$$d_n=a_{nn}+1 \text{ if } a_{nn}\in\{0,1,\dots,8\};\quad d_n=8 \text{ if } a_{nn}=9.$$

Note that $d_n \neq 0$ for all n, so this nonterminating decimal expansion os of the allowed kind, and defines a real number in $(0, 1]$.

We *claim* that for all $n \in \mathbb{N}$ $f(n) \neq x$, contradicting the fact that f is onto. To see this, observe that the n-th. digits in the decimal expansion of x is d_n, and in the expansion of $f(n)$ is d_{nn}; these are different (from the construction above). This concludes the proof.

Numerical example. We have no control over the "listing" f that is assumed to exist at the start of the argument, but suppose (for example) the first five entries were (highlighting the diagonal entries of the array):

$$\begin{aligned}
f(1) &= 0.\mathbf{1}2034506...\\
f(2) &= 0.1\mathbf{3}579017...\\
f(3) &= 0.24\mathbf{6}08046...\\
f(4) &= 0.314\mathbf{1}5926...\\
f(5) &= 0.2178\mathbf{4}143...\\
...
\end{aligned}$$

Then the first five digits of x would be: $x = 0.24725...$, and it is clear that x can't be any of the first five elements on the list (and indeed can't be any element on the list).

Remark 3. It follows from the theorem and Corollary 1 that $\mathbb{R}$ is uncountable.

Remark 3. A similar proof gives the following result: *the set of infinite sequences of 0s and 1s is uncountable.* By contradiction, suppose we had such a listing (as above), and modify the diagonal entries (in the only way possible) to find a sequence which can't possibly be included on the list.

This result about infinite sequences of 0s and 1s can be stated as a result about the power set of $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$. An infinite sequence is a function $f : \mathbb{N} \to \{0, 1\}$; the set of such sequences is usually denoted $\{0, 1\}^{\mathbb{N}}$. A subset $A \subset \mathbb{N}$ defines a function $f : \mathbb{N} \to \{0, 1\}$ via:

$$f(n) = 1 \text{ if } n \in A; \quad f(n) = 0 \text{ if } n \notin A.$$

And conversely, any function $f : \mathbb{N} \to \{0, 1\}$ determines the subset $A = f^{-1}(\{1\}) \subset \mathbb{N}$. Thus we have a bijective correspondence:

$$\mathcal{P}(\mathbb{N}) \longleftrightarrow \{0, 1\}^{\mathbb{N}}.$$

Combining these observations, we obtain the following result:

Theorem. (Cantor 1891) $\mathcal{P}(\mathbb{N})$ is uncountable.

Indeed it turns out that $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$. Cantor also proved that, for any set A (including uncountable sets) the cardinality of A is strictly smaller than that of $\mathcal{P}(A)$ (in the sense that there exists an injective function from A to $\mathcal{P}(A)$, but not a bijection).

Remark 4. It is an easy exercise that the set of irrational numbers is uncountable (see below), but it is harder to prove that, in fact, $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R}$. Indeed the following natural question arises: if $A \subset \mathbb{R}$ is infinite, is it true that either $A \sim \mathbb{N}$ or $A \sim \mathbb{R}$? (*continuum hypothesis*). The attempt to answer this question led to fundamental developments in logic and set theory throughout the 20th. century, which continue to this day.

PROBLEMS.

1. Prove that if $f : A \to C$ and $g : B \to D$ are bijections, the function:

$$h : A \times B \to C \times D, \quad h(a, b) = (f(a), g(b))$$

is also a bijection. Thus, $A \sim C$ and $B \sim D \to A \times B \sim C \times D$.

2. Prove that if A and B are sets: $A \sim B \to \mathcal{P}(A) \sim \mathcal{P}(B)$.

3. (i) Prove that if A and B are countably infinite, then so is $A \cup B$. *Hint:* First show that, for any sets A, B, we have: $A \cup B = A \cup (B \setminus A)$, where $A \cap (B \setminus A) = \emptyset$.

(ii) Prove that if A is uncountable and $B \subset A$ is a countably infinite subset of A, then $A \setminus B$ is uncountable. This shows that the set $\mathbb{R} \setminus \mathbb{Q}$ of irrational numbers is uncountable.

4. Show that the following sets are countably infinite: (i) the set of even integers; (ii) $\mathbb{Q} \times \mathbb{Q}$.

5. (a) Show that $[0, 1] \sim [-4, 12]$.

(b) Show that $(-1, 1) \sim \mathbb{R}$.

(c) Show that $(0, 1) \sim (0, 1]$. *Hint*: let $f(\frac{1}{n}) = \frac{1}{n+1}$, and let f be the identity elsewhere. Show that $f : (0, 1] \to (0, 1]$ is a bijection.

(d) Show that $(0, 1) \cup (1, 2) \sim (0, 2)$.

6. If A and B are nonempty sets, denote by B^A the set of all functions $f : A \to B$.

(a) Prove that if $A \sim B$ and $C \sim D$, then $C^A \sim D^B$.

(b) Prove that if A, B, C are sets and $A \cap B = \emptyset$, then $C^{A \cup B} \sim C^A \times C^B$.

(c) Prove that if A and B are finite sets, $\#B^A = \#B^{\#A}$. (*Hint:* Use induction on $\#A$.)

PART TWO (Outline)

1. Cantor-Bernstein-Schroeder theorem: Let A, B be sets. If there exist injective functions $f : A \to B$ and $g : B \to A$, then $A \sim B$.

Ex.1. $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.

Ex.2. $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R}$.

Ex.3. $(0, 1] \sim \mathbb{R}$.

2. Cardinality trumps dimensionality. The unit square $(0, 1) \times (0, 1) \subset \mathbb{R}^2$ is equipotent with the unit interval $(0, 1) \subset \mathbb{R}$.

Idea of proof. Construct an injection $(0, 1) \times (0, 1) \to (0, 1)$ in terms of decimal expansions:

$$(0.a_1a_2a_3..., 0.b_2b_2b_3...) \mapsto 0.a_1b_1a_2b_2a_3b_3...$$

Ex.4. $\mathbb{R}^2 \sim \mathbb{R}$; in fact $\mathbb{R}^n \sim \mathbb{R}$ for each n.

Ex.5. (i) The set $\mathbb{R}^{\mathbb{R}}$ of all functions $f : \mathbb{R} \to \mathbb{R}$ is equipotent with $\mathcal{P}(\mathbb{R})$. *Hint*: note that $\mathbb{R}^{\mathbb{R}}$ is a subset of $\mathcal{P}(\mathbb{R} \times \mathbb{R})$, and $\mathcal{P}(\mathbb{R} \times \mathbb{R}) \sim \mathcal{P}(\mathbb{R})$ (since $\mathbb{R}^2 \sim \mathbb{R}$). For the other injection, consider characteristic functions.

(ii) The set of all functions $f : \mathbb{Q} \to \mathbb{R}$ is equipotent with $\mathbb{R}$.

(iii) The set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ is equipotent with $\mathbb{R}$. (*Hint*: if f and g are continuous functions and take the same value at each rational number, then $f = g$.)

Ex.6. The set of all algebraic real numbers (roots of polynomials with integer coefficients) is countable. Hence transcendental numbers exist.

3. Theorem. (G. Cantor) Let A be any nonempty set. Then $\mathcal{P}(A)$ and A are not equipotent.

Note that there is an obvious injection from A to $\mathcal{P}(A)$: $x \mapsto \{x\}$.