Cardinalities of number systems

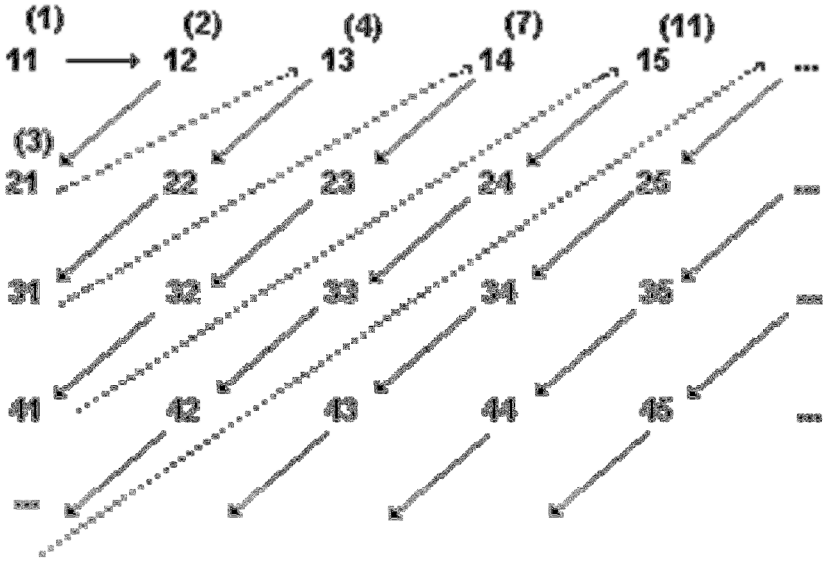
This lecture develops the additional tools needed to answer the following questions: ***What are the cardinalities of the standard number systems, including the rational numbers*** $\mathbb{Q}$, ***the real numbers*** $\mathbb{R}$, ***and the complex numbers*** $\mathbb{C}$? Several of the results that we prove are also significant in their own right, and the next lecture places many of these result s into a more general setting.

In the previous lecture we showed that the set $\mathbb{Z}$ of (signed) integers has the same cardinality as the set $\mathbb{N}$ of nonnegative integers using the identity $|\mathbb{N} \sqcup \mathbb{N}| = |\mathbb{N}|$. The main steps in finding the cardinalities for the other number systems involve further identities of this type.

Theorem. *There is a* $1-1$ *correspondence from* $\mathbb{N}\times\mathbb{N}$ *to* $\mathbb{N}$.

PROOF. We shall first define a $1-1$ mapping f from $\mathbb{N}_+ \times \mathbb{N}_+$ onto $\mathbb{N}_+$ by a diagonal construction due to Cantor. The picture below illustrates the idea behind the definition of the function; the explicit formula is

$$f(m,n) = \tfrac{1}{2}(m+n-1)(m+n-2) + m.$$



A verification that f is $1-1$ is straightforward; the ordered pairs (m, n) on the diagonal line $m + n = p$ are sent to the integers running from $\frac{1}{2}(p-1)(p-2)+1$ to $\frac{1}{2}(p-1)(p-2)$ as m runs from 1 to $p-1$.

We also have an easily defined $1-1$ mapping in the opposite direction sending n to $(n, 1)$. We can now use the Schröder – Bernstein Theorem to prove the equality $|\mathbb{N}_+| = |\mathbb{N}_+ \times \mathbb{N}_+|$. Since there is an obvious $1-1$ correspondence from $\mathbb{N}$ to $\mathbb{N}_+$ sending k to $k+1$, it also follows that $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.■

The discussion thus far naturally leads one to ask whether all infinite sets have the same cardinal number. However, the following fundamentally important result due to Cantor shows that there are many transfinite cardinal numbers.

Theorem (No largest cardinal number). *If A is a set then $|A| < |\mathcal{P}(A)|$.*

PROOF. Define a $1-1$ mapping from A to $\mathcal{P}(A)$ sending an element $a \in A$ to the one point subset $\{a\}$. This shows that $|A| \leq |\mathcal{P}(A)|$.

The proof that $|A| \neq |\mathcal{P}(A)|$ is carried out by using another ***Cantor diagonal process.*** Recall that there is a $1-1$ correspondence between $\mathcal{P}(A)$ and the set Y of all functions from A to $\{0, 1\}$ which is given by sending a subset B to its characteristic function χ_B, so it suffices to prove the inequality where $\mathcal{P}(A)$ is replaced by Y. Suppose that there is a $1-1$ correspondence $\mathbf{F} : A \to Y$. The idea is to construct a new function $g \in Y$ that is not in the image of $\mathbf{F}$.

Specifically, choose g such that, for each $a \in A$, the value $g(a)$ will be the unique element of $\{0, 1\}$ which is **NOT** equal to $[\mathbf{F}(a)](a)$; recall that $\mathbf{F}(a)$ is also a function from A to $\{0, 1\}$ and as such it can be evaluated at a. Since the values of g and $\mathbf{F}(a)$ at $a \in A$ are different, these two functions are distinct, and since $a \in A$ is arbitrary it follows that g cannot lie in the image of $\mathbf{F}$. However, we were assuming that $\mathbf{F}$ was onto, so this yields a contradiction. Therefore there cannot be a $1-1$ correspondence between A and $\mathcal{P}(A)$.■

Comments on the method of proof. The reason for the name ***diagonal process*** is illustrated below when A is the set $\mathbb{N}_+$ of positive integers. One assumes the existence of a $1-1$ correspondence between $\mathbb{N}_+$ and $\mathcal{P}(\mathbb{N}_+)$ and identifies the latter with the set of functions from $\mathbb{N}_+$ to $\{0, 1\}$ in the standard fashion. Then for each positive integer one has an associated sequence of 0's and 1's that are indexed by the positive integers, and one can represent them in a table or matrix form as illustrated

below, in which each of the terms x_j (where x is a letter and j is a positive integer) is equal to either $\mathbf{0}$ or $\mathbf{1}$.

$$
\begin{aligned}
&1 \cdots \mathbf{a_1}.\, a_2.\, a_3.\, a_4.\, a_5 \cdots \ldots \\
&2 \cdots b_1.\, \mathbf{b_2}.\, b_3.\, b_4.\, b_5 \cdots \ldots \\
&3 \cdots c_1.\, c_2.\, \mathbf{c_3}.\, c_4.\, c_5 \cdots \ldots \\
&4 \cdots d_1.\, d_2.\, d_3.\, \mathbf{d_4}.\, d_5 \cdots \ldots \\
&5 \cdots e_1.\, e_2.\, e_3.\, e_4.\, \mathbf{e_5} \cdots \ldots \\
&\ldots
\end{aligned}
$$

The existence of a $\mathbf{1-1}$ correspondence implies that all sequences appear on the list. However, if we change each of the bold entries (*i.e.*, the entry in the n^{th} row and n^{th} column for each n) by taking $\mathbf{0}$ if the original entry is $\mathbf{1}$ and vice versa, we obtain a new sequence that is not already on the list, showing that $\mathcal{P}(\mathbb{N}_+)$ cannot be put into correspondence with $\mathbb{N}_+$ and thus represents a higher order of infinity.■

The preceding result implies that "***there is no set of all cardinal numbers.***" Stated differently, there is no set S such that every set A is in $\mathbf{1-1}$ correspondence with a subset of S. If such a set existed, then $\mathcal{P}(S)$ would be in $\mathbf{1-1}$ correspondence with some subset $T \subset S$, and hence we would obtain the contradiction

$$|\mathcal{P}(S)| \;=\; |T| \;\leq\; |S| \;<\; |\mathcal{P}(S)|.\blacksquare$$

Theorem (Cardinality of the rational numbers). *If $\mathbb{Q}$ denotes the rational numbers, then its cardinality satisfies $|\mathbb{N}| = |\mathbb{Q}|$.*

PROOF. The idea is to construct $\mathbf{1-1}$ maps from $\mathbb{Q}$ to $\mathbb{N}$ and vice versa, and then to apply the Schröder – Bernstein Theorem.

We can construct a mapping from $\mathbb{N}\times\mathbb{N}$ onto the positive rationals $\mathbb{Q}_+$ by sending the ordered pair (p, q) to the fraction

$$\frac{p+1}{q+1}$$

and then applying the result which states that the existence of such an onto map implies $|\mathbb{Q}_+| \leq |\mathbb{N}\times\mathbb{N}|$. Since $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$, it follows that $|\mathbb{Q}_+| \leq |\mathbb{N}|$. Likewise, we can map $\mathbb{N}$ onto the nonpositive rational numbers in $\mathbb{Q}$; namely, use the composite map $\mathbb{N} \to \mathbb{N}\times\mathbb{N} \to \mathbb{Q}_+$ to define an onto mapping from $\mathbb{Q}_-$ (the ***negative*** rationals)

to $\mathbb{N}_+$ and send $\mathbf{0}$ to itself. Combining these, we obtain an onto map from the disjoint union $\mathbb{N} \sqcup \mathbb{N}$ to $\mathbb{Q}$, and therefore we have $|\mathbb{Q}| \leq |\mathbb{N} \sqcup \mathbb{N}| = |\mathbb{N}|$.

Defining the mapping in the other direction is much easier; we need only take the standard inclusion of $\mathbb{N}$ in $\mathbb{Q}$. Since we have now constructed $\mathbf{1-1}$ mappings in both directions, we can apply the Schröder – Bernstein Theorem to complete the proof.■

Theorem (Cardinality of the real numbers). *If $\mathbb{R}$ denotes the real numbers, then its cardinality satisfies $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$ and therefore we have $|\mathbb{R}| > |\mathbb{N}| = |\mathbb{Q}|$.*

PROOF. Usually this is derived using decimal expansions of real numbers, but we shall give a proof that does not involve decimals (although the idea is similar). The idea is to construct $\mathbf{1-1}$ maps from $\mathbb{R}$ to $\mathcal{P}(\mathbb{N})$ and vice versa and then to apply the Schröder – Bernstein Theorem.

Let $D: \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ be the Dedekind cut map sending a real number x to the set of all ***rational*** numbers less than x. Since there is always a rational number between any two distinct real numbers, it follows that this map is $\mathbf{1-1}$. Furthermore, since $|\mathbb{Q}| = |\mathbb{N}|$ it follows that there is a $\mathbf{1-1}$ correspondence from $\mathcal{P}(\mathbb{Q})$ to $\mathcal{P}(\mathbb{N})$, and the composite of D with this map gives the desired $\mathbf{1-1}$ map from $\mathbb{R}$ to $\mathcal{P}(\mathbb{N})$.

Let $\mathcal{P}_\infty(\mathbb{N})$ denote the set of all ***infinite*** subsets of $\mathbb{N}$, and define a function σ from $\mathcal{P}_\infty(\mathbb{N})$ to $\mathbb{R}$ as follows: Given an infinite subset B, let X_B be its characteristic function and consider the infinite series

$$\sigma(B) = \sum_k X_B(k) \cdot 2^{-k-1} .$$

This series always converges by the Comparison Test because its terms are nonnegative and less than or equal to those of the geometric series

$$1 = \sum_k 2^{-k-1} .$$

Note that all these sums lie in the interval $[0, 1]$. Furthermore, we claim that *different **infinite** subsets will yield different values*. Verifying this is not difficult, but we shall give the details for the sake of completeness: Given subsets X and Y of $\mathbb{N}$, write the function values as base 2 floating point expressions

$$\sigma(X) = 0.x_1x_2x_3\ldots \quad \text{and} \quad \sigma(Y) = 0.y_1y_2y_3\ldots$$

where the x's and y's are 0 or 1 and there are infinitely many 1's in both cases. If X and Y are distinct subsets, then there is some first k such that k belongs to one set but not the other, and this translates to the inequality $x_k \neq y_k$. Since k is the first integer which is in one set but not the other, we also have $x_j = y_j$ for $j < k$. We might as well assume that $x_k = 0$ and $y_k = 1$ (if not, simply reverse the roles of x and y in the argument that follows). The goal is then to show that $\sigma(X) < \sigma(Y)$, which will imply that σ is $1-1$.

Let c be the (finite) binary fraction obtained by taking $c_j = y_j$ for $j \leq k$ and $c_j = 0$ if $j > k$. . An upper estimate d for $\sigma(X)$ is given by taking $d_j = x_j$ for $j \leq k$ and $d_j = 1$ if $j > k$. Clearly we then have $\sigma(X) \leq d$. However, one can also check directly that $c = d$ by a geometric series arbument. Now there are infinitely many 1's in the series for $\sigma(Y)$, and in particular we have $y_m = 1$ for some $m > k$. Therefore it follows that $\sigma(X) \leq d = c \leq \sigma(Y)$, which is what we wanted to prove. This completes the proof that σ is $1-1$.

On the other hand, if A is a ***finite*** subset, consider the finite sum

$$\sigma(A) = 2 + \sum_k X_B(k) \cdot 2^{-k-1}.$$

Once again it follows that different finite subsets determine different real (in fact, ***rational***) numbers. Furthermore, since the value associated to a finite set lies in the interval $[2, 3]$ it is clear that a finite set and an infinite set cannot go to the same real number. Therefore we have constructed a $1-1$ function from $\mathcal{P}(\mathbb{N})$ to $\mathbb{R}$.

Since we have constructed $1-1$ mappings in both directions, we can apply the Schröder – Bernstein Theorem to complete the proof.■

Finally, we need to determine the cardinality of the complex numbers $\mathbb{C}$. By construction, the complex numbers are in $1-1$ correspondence with the points on the coordinate plane $\mathbb{R}^2$, so the cardinality of $\mathbb{C}$ is given by the following result:

Theorem (Cardinality of the complex numbers). *If $\mathbb{C}$ denotes the real numbers, then its cardinality satisfies $|\mathbb{C}| = |\mathbb{R}^2| = |\mathbb{R}|$.*

One slightly nonintuitive consequence of this theorem is the existence of a $1-1$ correspondence between the points of the number line and the points on the coordinate plane. Of course, these objects with all their standard mathematical structures are quite different, but the theorem says that the two number systems cannot be shown to be distinct simply by means of transfinite cardinal numbers.

PROOF. The proof uses a few general facts about the sets of functions from one set to another.

Lemma 1. *If X, Y and C are nonempty sets and there is a $1-1$ correspondence f from X to Y, then there is a $1-1$ correspondence of function sets from $\mathbf{F}(Y, C)$ to $\mathbf{F}(Y, C)$.*

PROOF. Let $\varphi(f)\colon \mathbf{F}(Y, C) \to \mathbf{F}(X, C)$ send $g\colon Y \to C$ to $g \circ f$. Direct calculation shows that $\varphi(f^{-1})\colon \mathbf{F}(X, C) \to \mathbf{F}(Y, C)$ is an inverse function to $\varphi(f)$.■

Lemma 2. *If A, B and C are nonempty sets, then there is a $1-1$ correspondence from $\mathbf{F}(A \sqcup B, C)$ to $\mathbf{F}(A, C) \times \mathbf{F}(B, C)$.*

PROOF. A function $f\colon A \sqcup B \to C$ is completely determined by its restrictions to the summands $A \times \{1\}$ and $B \times \{2\}$, and conversely every ordered pair of mappings $f\colon A \times \{1\} \to C$ and $g\colon B \times \{2\} \to C$ can be pieced together into a well – defined function from $A \sqcup B$ to C because $A \times \{1\}$ and $B \times \{2\}$ have no elements in common. This proves the lemma if A and B are replaced by $A \times \{1\}$ and $B \times \{2\}$. Since there are standard $1-1$ correspondences $A \leftrightarrow A \times \{1\}$ and $B \leftrightarrow B \times \{2\}$ given by $a \leftrightarrow (a, 1)$ and $b \leftrightarrow (b, 2)$ respectively, Lemma 2 follows from the preceding argument and Lemma 1.■

Application to proving the theorem. We know that there is a $1-1$ correspondence h from $\mathbb{R}$ to $\mathbf{F}(\mathbb{N}, \{0, 1\})$, and if we define

$$h \times h\colon \mathbb{R} \times \mathbb{R} \to \mathbf{F}(\mathbb{N}, \{0, 1\}) \times \mathbf{F}(\mathbb{N}, \{0, 1\}) \quad \text{by} \quad h \times h(u, v) = \big(h(u), h(v)\big)$$

then $h \times h$ defines a $1-1$ correspondence of the associated Cartesian squares whose inverse is $h^{-1} \times h^{-1}$. By Lemma 2 the codomain of $h \times h$ is in $1-1$ correspondence with $\mathbf{F}(\mathbb{N} \sqcup \mathbb{N}, \{0, 1\})$, and by Lemma 1 and the previously shown identity $\mathbb{N} \sqcup \mathbb{N} \leftrightarrow \mathbb{N}$ we know that there is a $1-1$ correspondence from the last function set to $\mathbf{F}(\mathbb{N}, \{0, 1\})$. Combining these observations, we obtain a $1-1$ correpondence from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Since $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ by construction, it follows that $|\mathbb{C}| = |\mathbb{R}^2| = |\mathbb{R}|$.■