SETS, FUNCTIONS, AND THE CONTINUUM HYPOTHESIS

CATHAL O CLEIRIGH

1. Cardinality

We denote the **size** or **cardinality** of a set M by $|M|$. For finite sets we simply count the number of elements - if M has exactly n elements, then M has cardinality n. Hence, two finite sets M and N have equal cardinality, $|M| = |N|$ if and only if they contain the same number of elements. But how do we generalise this to infinite sets? Clearly, if M and N are finite sets with $|M| = |N|$, there exists a bijection ϕ between the two sets. Therefore, we make this our definition for the general case - not just finite sets.

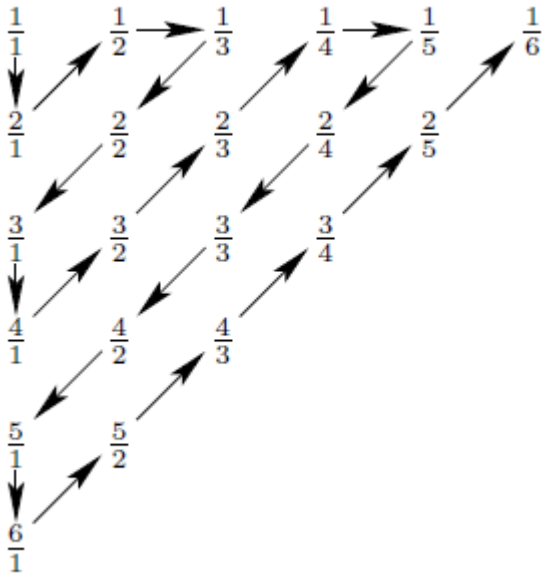
Definition 1.1. Two arbitrary sets M and N (finite or infinite) are said to be of **equal size** or **equal cardinality**, if and only if there exists a bijection ϕ from M onto N.

This notion of equal size is an equivalence relation, so to each equivalence class of equal-sized sets, we associate a so-called **cardinal number**. For a finite set with n elements, we simply associate it with the cardinal number n For infinite sets, it becomes less intuitive - for the set of natural numbers $\mathbb{N}$, we associate with it the cardinal number $\aleph_0$ (i.e. $|\mathbb{N}| = \aleph_0$). For other infinite sets, some have cardinality $\aleph_0$ while others do not.

2. Countability

If $|M| = \aleph_0$ for a set M, then we say that M is **countable**. In other words, if we can list all of the elements of M as $m_1, m_2, m_3, \dots$ then M is countable, as clearly there exists a bijection ϕ between $\mathbb{N}$ and M, namely $\phi(i) = m_i$, for $i \in \mathbb{N}$. It is easy to find examples of other countable sets by seeing if we can list them as above. For example, the set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ can be written in a list as such: $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$. Somewhat suprisingly, we can show in this way that the rational numbers are also countable.

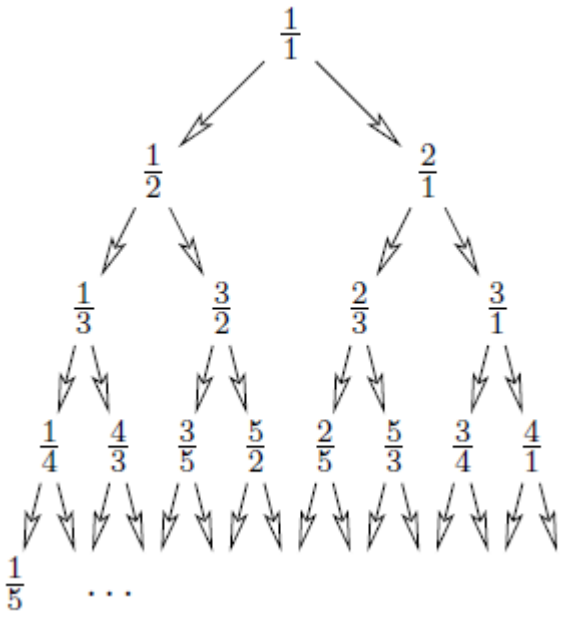
Date: 24th of October 2018.



Theorem 2.1. *The set $\mathbb{Q}$ of rational numbers is countable.*

Proof. We first list all of the elements of $\mathbb{Q}^+$ by following the pattern in the diagram above, and skipping any numbers already encountered. Thus, we have shown that $\mathbb{Q}^+$ is countable. Similar to how we listed the integers above, we begin the list of elements of $\mathbb{Q}$ with 0, then follow the list found for $\mathbb{Q}^+$ and insert the corresponding negatives of these elements directly after each element itself. i.e. $\mathbb{Q} = \{0, 1, -1, 2, -2, \frac{1}{2}, -\frac{1}{2}, \dots\}$. As displaying the elements of $\mathbb{Q}$ in this way shows that $\mathbb{Q}$ is countable, we are done. □

There is in fact a more elegant way of listing the elements of $\mathbb{Q}$. This nicer way doesn't require us to skip over duplicates, as we were forced to in the proof above. This list is found by observing the binary tree below.



We can see its recursive rule with ease:

- $\frac{1}{1}$ is on top of the tree
- every node $\frac{i}{j}$ has two "sons": the left son is $\frac{i}{i+j}$ and the right son is $\frac{i+j}{j}$

There are three properties of the tree that are easy to prove:

(1) All fractions in the tree are reduced, i.e. if $\frac{r}{s}$ appears in the tree, then r and s are relatively prime
(2) Every reduced fraction $\frac{r}{s} > 0$ appears in the tree
(3) Every reduced fraction appears exactly once

The first property can be proved by noting that it is true for the top of the tree $\frac{1}{1}$, and by then using induction downward: if r and s are relatively prime, then so are r and $r + s$, as well as s and $r + s$.

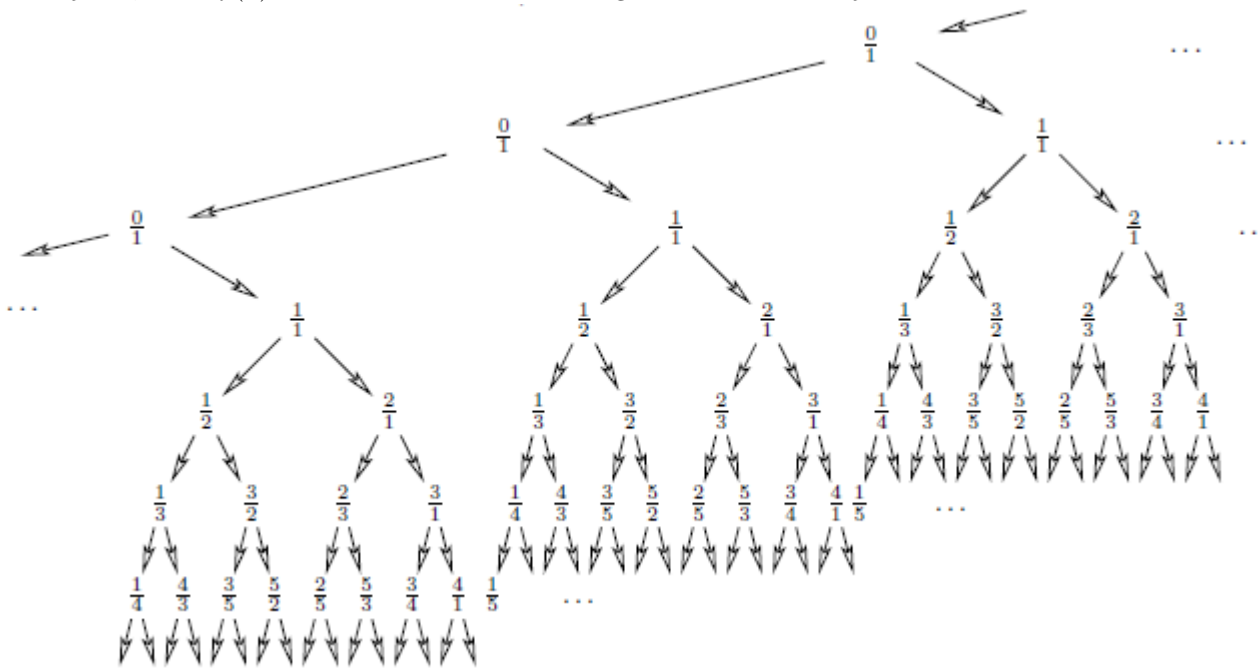
The second property can be proved by induction on the sum $r + s$. The smallest value is $r + s = 2$, which occurs at the top of the tree. If $r > s$, then $\frac{r-s}{s}$ appears in the tree by induction (considering the sum of its numerator and denominator), and we get $\frac{r}{s}$ as its right son. Similarly, if $r < s$, then $\frac{r}{s-r}$ appears in the tree by induction also, and has $\frac{r}{s}$ as its left son.

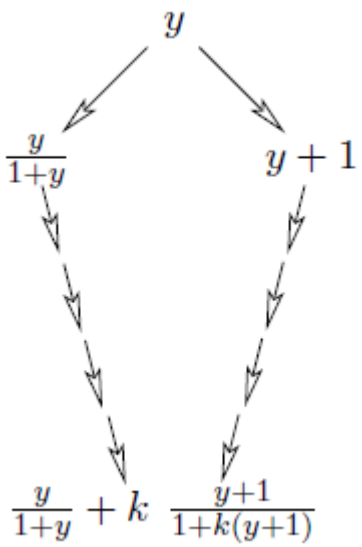
The third property can be proved using a similar argument. As all nodes of the tree are of the form $\frac{i}{i+j}$ or $\frac{i+j}{j}$ for $i, j \in \mathbb{N}$, except for the top of the tree, we have no nodes being equal to 1 (except for the top of the tree). Hence, if $\frac{r}{s}$ appears more than once, then $r \neq s$. For each case, $r < s$, $r > s$, we argue by induction as before.

Now that we have verified these properties, it is clear to see that every positive rational occurs exactly once in the tree, so we can list them level-by-level from left to right. We can then create a list of all of the rational numbers the same way as before (starting with 0 etc.)

However, one may ask, given $\frac{r}{s}$, is there an easy way to determine the next element in the list? The answer is yes. First, we construct another infinite binary

tree as shown in the first diagram below. We see that, given $\frac{r}{s} = x$, its right son is $x + 1$, and its left son is $\frac{x}{1+x}$. Continuing in this manner, we see that if we keep taking successive right sons, that the k-fold right son of x is $x + k$. Likewise, if we take successive left sons, we see that the k-fold left son of x is $\frac{x}{1+kx}$. Now, looking at a rational number $\frac{r}{s} = x$ and its successor $f(x)$ in the tree, as depicted in the second diagram below, we see that x is the k-fold right son of the left son of some rational $y \geq 0$, while $f(x)$ is the k-fold left son of the right son of the same y.





As $x = \frac{y}{1+y} + k$, we see that $\lfloor x \rfloor = k$, and that $\{x\} = \frac{y}{1+y}$ (since $0 < \frac{y}{1+y} < 1$). From this, we obtain $f(x) = \frac{y+1}{1+k(y+1)} = \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$. This generates the sequence of positive rationals found by listing the nodes of the tree level-by-level and left to right as discussed above.

Next, it is natural to enquire about the cardinality of $\mathbb{R}$. Is $|\mathbb{R}| = \aleph_0$? The answer is no, as we will see below.

Theorem 2.2. *The set $\mathbb{R}$ of real numbers is **not** countable.*

Proof. Any subset N of a countable set $M = \{m_1, m_2, \dots\}$ is either finite or countable, as can easily be checked. Therefore, if we can find a subset of $\mathbb{R}$ which is not countable, then $\mathbb{R}$ cannot be countable itself. We consider the subset $(0, 1]$ of $\mathbb{R}$. Suppose $H = (0, 1]$ is countable and let $H = \{r_1, r_2, \dots\}$ be a listing of H. We write r_n as its unique infinite decimal expansion without an infinite sequence of zeros at the end: $r_n = 0.a_{n1}a_{n2}\dots$ where $a_{ni} \in \{0, 1, \dots, 9\}$ for all n and i. For example, we write 0.5 as $0.49999\dots$. As we can list these elements as $H = \{r_1, r_2, \dots\}$, we obtain the following array:

$r_1 = 0.a_{11}a_{12}\dots$
$r_2 = 0.a_{21}a_{22}\dots$
$\dots$
$\dots$
$r_n = 0.a_{n1}a_{n2}\dots$
$\dots$

For every n, let b_n be the least element of $(1, 2)$ that is different from a_{nn}. Then $b = 0.b_1b_2\cdots \in H$ so $b = r_k$ for some $k \in \mathbb{N}$. But b_k is different from a_{kk} by definition, so we arrive at a contradiction. Hence, $H = (0, 1]$ is uncountable, which means $\mathbb{R}$ is uncountable itself. □

It can be shown that any open, half-open, or closed interval, both finite and infinite, has the same cardinality as $\mathbb{R}$ which we denote by c. This fact is very useful, as we will see in the proof of the following theorem.

Theorem 2.3. *The set $\mathbb{R}^2$ of all ordered pairs of real numbers (the real plane) has the same size as $\mathbb{R}$.*

Proof. We show that the set of all pairs $(x, y), 0 < x, y \leq 1$, can be mapped bijectively onto $(0, 1]$. The desired result follows directly from this, as there exists a bijection ϕ from $\mathbb{R}$ from $(0, 1]$ to $\mathbb{R}$ by the above fact.

Consider the pair (x, y) with x, y written as their unique infinite decimal expansions as described earlier. For example:

$x = 0.3$	01	2	007	$08\dots$
$y = 0.009$	2	05	1	$0008\dots$

We have separated the digits of x, y into groups, allowing precisely one non-zero digit per group, with each group ending with that digit. We now define $z = \phi(x, y) \in (0, 1]$ by writing down for the infinite decimal expansion of z the first x-group, then the first y-group, and then the second x-group, and so on. Using our example, $z = 0.30090122050071080008\dots$. To see that this mapping is bijective, we consider injectivity and surjectivity separately.

It is injective as given any $z \in (0, 1]$ such that $z = \phi(x, y)$ for some (x, y) with $0 < x, y \leq 1$, we can find the corresponding x, y by identifying each group of digits in z (as described above) and separating them out one-by-one into the infinite

decimal expansions for x and y, alternating between them and starting with x. There is only one way to follow this procedure, which results in unique values for x and y. Therefore, ϕ is injective.

It is obviously surjective, as given any $z \in (0, 1]$ we can apply the procedure detailed in the previous paragraph to find a pair (x, y) such that $0 < x, y \leq 1$.

So ϕ is bijective, and we are done. □

3. Cantor-Bernstein Theorem

We say that the cardinal number $\mathbf{m}$ is less than or equal to $\mathbf{n}$, if for sets M and N with $|M| = \mathbf{m}$, $|N| = \mathbf{n}$, there exists an injection from M into N. The relation $\mathbf{m} \leq \mathbf{n}$ is independent of the sets M and N chosen, due to the bijection definition of equal cardinality. We would now like to see if $\mathbf{m} \leq \mathbf{n}$, $\mathbf{n} \leq \mathbf{m}$ imply $\mathbf{m} = \mathbf{n}$. In fact, this is true, as we will see from the proceeding theorem.

Theorem 3.1 (Cantor-Bernstein)**.** *If each of two sets M and N can be mapped injectively into the other, then there is a bijection from M to N, that is, $|M| = |N|$.*

Proof. Let f be an injection from M into N, and let g be an injection from N into M. We will partition the union of the two sets M and N, $M \cup N$ into chains of elements. Take an arbitrary element $m_0 \in M$ and generate a chain of elements by applying f, then g, then f again, then g again, and so on. There are four different types of chain that can occur.

If the chain loops back to an element that it has already "passed", it is finite and the first "duplicate" in the chain is m_0 due to injectivity. This is the first type of chain - a diagram is shown below.

$m_0 \to n_0 \to m_1 \to \ldots m_k \to n_k \to m_0$

Otherwise, the chain continues with distinct elements indefinitely. We will follow the chain backwards in this case - we start with m_0 and find $g^{-1}(m_0)$, then $f^{-1}(g^{-1}(m_0))$, and so on. We can only do this in the case that m_0 is in the image of g, $g^{-1}(m_0)$ is in the image of f, and so on. The three other types of chains are found in this way.

If the process of following the chain backwards continues indefinitely, we have the second type of chain, as shown below.

$\cdots \to m_0 \to n_0 \to m_1 \to \ldots$

If we finish on an element of M that does not lie in the image of g, we have the third type.

$m_0 \to n_0 \to m_1 \to n_1 \to \ldots$

If we finish on an element of N that does not lie in the image of f, we have the fourth type.

$n_0 \to m_0 \to n_1 \to m_1 \to \ldots$

Every element of $M \cup N$ must belong to one of these chains, as can easily be checked. We now define a bijection F from M onto N by $F(m_i) = n_i$, and we are done. □

As a consequence of the Cantor-Bernstein Theorem, we can prove that the set $\mathcal{P}(\mathbb{N})$ of all subsets of $\mathbb{N}$ has cardinality c. It suffices to show that $|\mathcal{P}(\mathbb{N}) - \{\emptyset\}| = |(0, 1]|$ as removing an element of an infinite set leaves its cardinality unchanged. An injective map from the first set to the second is $f(A) = \sum_{i \in A} 10^{-i}$. An injective

map from the second set to the first set is $g(0.b_1b_2b_3\dots) = \{b_i 10^i : i \in \mathbb{N}\}$ where we have used the infinite decimal expansion as described previously.

4. Ordinal Numbers and the Continuum Hypothesis

A set M is ordered by a relation $\prec$ if $\prec$ is transitive and either $a \prec b$ or $b \prec a$ for all distinct $a, b \in M$.

An ordered set M is well-ordered if each non-empty subset of M has a first element.

The **Well-Ordering Theorem**, implied by the **Axiom of Choice**, states that every set M can be well-ordered.

Two well-ordered sets M and N are similar if there exists a bijection ϕ from M onto N such that for $m, n \in M$, $m \prec n$ implies $\phi(m) \prec \phi(n)$. We denote this as $M \sim N$. Similarity is obviously an equivalence relation - we denote α as the **ordinal number** associated with a class of equivalent sets.

For a well-ordered set M, and $m \in M$, we define the **initial segment** of M determined by m: $M_m = \{x \in M : x < m\}$. We define for ordinal numbers α and β of the respective well-ordered sets M, N: $\alpha < \beta$ if M is similar to a segment of N.

Transfinite Induction states that if for each $m \in M$, a property P being true for all elements in the initial segment M_m implies that it is true for m itself, then P is true for all $n \in M$.

It can be proved that for each pair of ordinal numbers α, β, exactly one of the following relations is true: $\alpha < \beta, \alpha = \beta, \alpha > \beta$. It can also be proved that every set of ordinal numbers (ordered according to magnitude) is well-ordered.

The **Contiunuum Hypothesis** is the statement $c = \aleph_1$, or in other words, that the next cardinal number after $\aleph_0$ is c.

Theorem 4.1. *Let $\{f_\alpha\}$ be a family of pairwise distinct analytic functions on $\mathbb{C}$, the complex numbers, such that for each $z \in \mathbb{C}$ the set of values $\{f_\alpha(z)\}$ is at most countable. If $c > \aleph_1$, then $\{f_\alpha\}$ is countable. If $c = \aleph_1$, then there exists some family $\{f_\alpha\}$ with this property, that has size c.*

Proof. Assume $c > \aleph_1$. We will show that for any family $\{f_\alpha\}$ of size $\aleph_1$ that there exists some $z_0 \in \mathbb{C}$ such that all $\aleph_1$ values $f_\alpha(z_0)$ are distinct. If a family of functions satisfies the hypothesis of the theorem, it must then be countable.

We well-order the family $\{f_\alpha\}$ according to the initial ordinal number ω_1 of $\aleph_1$. (This exists due to the fact that every set of ordinal numbers ordered according to magnitude is well-ordered - we take the first element in the ordered set of all ordinal numbers with cardinality $\aleph_1$.) The index set runs through all ordinal numbers α which are smaller than ω_1. We now show that the set of pairs $(\alpha, \beta), \alpha < \beta < \omega_1$ has size $\aleph_1$. Since any $\beta < \omega_1$ is a countable ordinal, the set of pairs $(\alpha, \beta), \alpha < \beta$ is countable for every fixed β. Taking the union over all $\aleph_1$-many β, we see that the set of pairs $(\alpha, \beta), \alpha < \beta$ has size $\aleph_1$.

Consider for any pair $\alpha < \beta$, the set $S(\alpha, \beta) = \{z \in \mathbb{C} : f_\alpha(z) = f_\beta(z)\}$. We will now show that each set $S(\alpha, \beta)$ is countable. Consider the disks C_k of radius $k = 1, 2, 3, \dots$ around the origin in the complex plane. By a result on analytic functions, if f_α and f_β agree on infinitely many points in one of the C_k, then f_α and f_β are identical. Consequently, f_α and f_β agree on only finitely many points in each C_k, so on at most countably many points altogether. Setting S as the union

of all $S(\alpha, \beta)$ for which $\alpha < \beta$, we find that S has size $\aleph_1$, as each set $S(\alpha, \beta)$ is countable. As $\mathbb{C}$ has size c - there is clearly a bijection from $\mathbb{R}^2$ to $\mathbb{C}$ - and $c > \aleph_1$ by assumption, there exists a complex number z_0 not in S with all $\aleph_1$ values $f_\alpha(z_0)$ distinct.

Now assume that $c = \aleph_1$. Consider the set D of complex numbers $p + iq$ with rational real and imaginary part. This is clearly countable, as it is a countable union of countable sets. Note that every open disk in the complex plane contains some point of D. Let $\{z_\alpha : 0 \leq \alpha < \omega_1\}$ be a well-ordering of $\mathbb{C}$. We will now construct a family of $\aleph_1$-many distinct anaytic funtions - $\{f_\beta : 0 \leq \beta < \omega_1\}$ - such that $f_\beta(z_\alpha) \in D$ whenever $\alpha < \beta$. Any such family satisfies the hypothesis of the theorem.

Each complex number z has some index, say $z = z_\alpha$. For all $\beta > \alpha$, the values $\{f_\beta(z_\alpha)\}$ lie in the countable set D. Since α is a countable ordinal number, the functions f_β with $\beta \leq \alpha$ will contribute at most countably further values $f_\beta(z_\alpha)$, so that the set of all values $\{f_\beta(z_\alpha)\}$ is also at most countable. So if we can construct such a family $\{f_\beta\}$, the second part of the theorem is proved.

We construct $\{f_\beta\}$ by transfinite induction. We take f_0 constant, although this would work for any analytic function. Suppose f_β has already been constructed for all $\beta < \gamma$. Since γ is a countable ordinal, we may reorder $\{f_\beta : 0 \leq \beta < \gamma\}$ into a sequence $g_1, g_2, g_3 \ldots$. The same reordering of $\{z_\alpha : 0 \leq < \gamma\}$ gives a sequence $\omega_1, \omega_2, \omega_3, \ldots$. We now construct a function f_γ satisfying for each n the conditions $f_\gamma(\omega_n) \in D$ and $f_\gamma(\omega_n) \neq g_n(\omega_n)$. The second condition ensures that all functions $f_\gamma(0 \leq \gamma < \omega_1)$ are distinct, and the first condition is just the same as $f_\beta(z_\alpha) \in D$ whenever $\alpha < \beta$ from above. Note that the condition $f_\gamma(\omega_n) \neq g_n(\omega_n)$ is another diagonalisation argument.

To construct f_γ, we write $f_\gamma(z) = \epsilon_0 + \epsilon_1(z - \omega_1) + \epsilon_2(z - \omega_1)(z - \omega_2) + \ldots$. If γ is a finite ordinal, then f_γ is a polynomial and hence analytic, and we can choose numbers ϵ_i such that both the conditions are satsified. Now suppose γ is a countable ordinal, then $f_\gamma(z) = \sum_{n=0}^{\infty} \epsilon_n(z - \omega_1) \ldots (z - \omega_n)$. The values of $\epsilon_m(m \geq n)$ have no influence on the value $f_\gamma(\omega_n)$, hence we may choose the ϵ_n step by step. If the sequence (ϵ_n) converges to 0 sufficiently fast, then the expression for $f_\gamma(z)$ defines an analytic function. Finally, as every open disk in the complex plane contains some point of D, i.e. D is dense in $\mathbb{C}$ we may choose this sequence so that f_γ meets the conditions above, and the proof is finally complete. □

5. References

Proofs from THE BOOK, Fifth Edition - Martin Aigner, Gunter M. Ziegler, SPRINGER-VERLAG BERLIN HEIDELBERG 2014