CDM

Three Theorems

K. Sutner
Carnegie Mellon University

20-cardinality 2017/12/15 23:22

Measuring Things

Measuring objects to determine their "size" is an incredibly useful technique that is used in many places. Here are simple examples:

- Measure a list by its length, a natural number.
- Measure a polyhedron by its area, a real number.
- Measure movement of a particle by its velocity, a vector of reals.

In the same vein we would like be able to determine the "size" of a set.

Cardinality

Definition

The size of a set is called its cardinality.

Of course, this is not much of a definition. In the words of G. Cantor:

> Every aggregate M has a definite "power", which we also call its "cardinal number".
> ... the general concept which, by means of our active faculty of thought, arises from the aggregate M when we make abstraction of the nature of its various elements m and of the order in which they are given.

The Finite Case

If the set in question is finite

$$A = \{a_1, a_2, \ldots, a_{n-1}, a_n\}$$

then our notion of cardinality is straightforward: it's just n.

In other words, we can exploit natural numbers to describe the sizes of these sets.

Of course, the definition of "finiteness" usually involves the natural numbers, so the question is: how do we define the naturals?

Defining the Naturals

For the sake of this lecture, let us distinguish between

$\mathbb{N}$ the intuitive natural numbers

ω the naturals as defined in set theory

We can use the successor function $S(x) = x \cup \{x\}$ to represent a natural number n by a set $\underline{n}$, a von Neumann ordinal, as follows:

$$\underline{0} \rightsquigarrow \emptyset$$
$$\underline{n} \rightsquigarrow \underbrace{S(S(\ldots S(\emptyset)\ldots))}_{n}$$

So, $\underline{3} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ represents the number 3.

The Problem

Following our general principle of using set theory as our reference implementation for everything, we would like to give a formal definition of ω. Hopefully, this definition will clear up all questions one might have about $\mathbb{N}$.

Unfortunately, we cannot define ω by something along the lines of

$$\omega = \{\, \underline{n} \mid n \geq 0 \,\}$$

because this is fatally circular: the $n \geq 0$ already assumes $\mathbb{N}$.

Here is a nice way around these problems, using the machinery of set theory.

Successor Sets

Definition

A set X is a successor set if $\emptyset \in X$ and $x \in X \Rightarrow S(x) \in X$.

Define ω to be $\subseteq$-least successor set.

This definition works since successor sets are closed under intersection: the intersection of a family of successor sets is again a successor set.

So we can form

$$\omega = \bigcap \{\, X \mid X \text{ successor set } \}.$$

Yes, it's impredicative, but we don't care.

Does It Work?

So ω is the just least collection of von Neumann ordinals that contains $\underline{0}$ and is closed under successors.

We can now adopt the **definition** that ω represents $\mathbb{N}$: our informal n is made precise by the finite von Neumann ordinal $\underline{n}$ (never mind the infinite ones).

Experience shows that this works out very nicely. For example, the order relation on ω is given by $\in$; more precisely we have

$$\underline{n} = \{\underline{0}, \underline{1}, \ldots, \underline{n-1}\}$$

so that, as a set, each number consists precisely of all the smaller ones.

Defining Finiteness

We can now formally define finiteness.

Definition

A set A is finite if there is a bijection between some $\underline{n} \in \omega$ and A.

Again, this makes perfect intuitive sense, since we can think of the bijection as the standard enumeration (using 0-indexing):

$$A = \{a_0, a_1, \ldots, a_{n-2}, a_{n-1}\}$$

Infinite Cardinality

But for infinite sets things become a bit more complicated. We would like a collection Card of cardinal numbers that can be used to compare the sizes of (potentially infinite) sets. Here is step one in this direction.

Definition

For any set A, write $|A|$ for the cardinality of A.

Again, this is not really a definition, just notation for the time being. We will have to explain at some point what Card actually is.

How would we go about doing this?

Wishlist

It is usually a good idea to start with a list of desirable properties and then try to build something that matches them.

First, our cardinal numbers should extend ω so that:

- $\omega \subset \text{Card}$
- $\omega \in \text{Card}$
- For any set A there is some $|A| \in \text{Card}$
- Comparability: we want cardinal numbers to be totally ordered

$$\kappa < \lambda \vee \kappa = \lambda \vee \kappa > \lambda$$

Comparing Cardinality

G. Cantor suggests the following:

> We say that two aggregates M and N are "equivalent" if it is possible to put them, by some law, in such a relation to one another that to every element of each one of them corresponds one and only one element of the other.

In modern parlance: there has to be a bijection between the two sets:

$$f\colon M \longleftrightarrow N$$

Take the stipulation "by some law" with a grain of salt, the bijection need not have a simple description; it just has to exist.

The Key Insight

We can compare cardinalities without having to worry about details of the definition of a cardinal number.

Definition

Let A and B be two arbitrary sets.

$$|A| = |B| \iff \exists\, f \text{ bijective } (f\colon A \longleftrightarrow B)$$
$$|A| \leq |B| \iff \exists\, f \text{ injective } (f\colon A \longrightarrow B)$$

Sets with the same cardinality are called equipotent or equinumerous. In symbols: $A \approx B$.

Exercise

Verify that at least for finite sets this all makes perfect sense: we obtain the intuitive notion of size of a finite set.

Basic Sanity Check

At the very least, "same-cardinality" should be an equivalence relation.

- reflexive: $I_A\colon A \longleftrightarrow A$
- symmetric: $f\colon A \longleftrightarrow B$ yields $f^{-1}\colon B \longleftrightarrow A$
- transitive: $f\colon A \longleftrightarrow B$ and $g\colon B \longleftrightarrow C$ yields $f \circ g\colon A \longleftrightarrow C$

So far, so good.

Likewise, "at-most-same-cardinality" is a pre-order (reflexive and transitive).

But it's not a partial order: same cardinality is logical lightyears away from equality of sets.

Comparability holds, given sufficiently strong axioms of set theory (AC).

Important Cases

For us, the most interesting applications will be to find bijections

- $f\colon \nu \longleftrightarrow X$ for some $\nu < \omega$
- $f\colon \omega \longleftrightarrow X$, and
- $f\colon \mathfrak{P}(\omega) \longleftrightarrow X$.

corresponding to finite, infinite, and very infinite (size of the continuum).

Constructing such bijections by hand can be difficult, which is part of the reason Cantor's result came as such a surprise to many.

We begin with a number of helpful auxiliary lemmata. These are really all basic exercises in applying the set-theoretic definitions of injection, surjection and so on.

Notation Warning

In the context of cardinality, it is standard usage to write

$$\aleph_0$$

instead of ω for the first infinite cardinal.

As you might suspect, there are more cardinals floating around:

$$\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\omega, \aleph_{\omega\omega}$$

and so on – but we won't go there.

Injections versus Surjections

Lemma

There is an injection $f : A \to B$ if, and only if, there is a surjection $g : B \to A$.

Proof.

Assume $A \neq \emptyset$ and let f be the injection. Pick $a_0 \in A$ and set

$$g(b) = \begin{cases} a & \text{if } f(a) = b, \\ a_0 & \text{if } b \notin \operatorname{rng} f. \end{cases}$$

Assume g is the surjection. For each $b \in B$ there exists an $a \in A$ such that $g(a) = b$ by surjectivity. Pick one such a, say, a_0, and set $f(b) = a_0$.

□

Infinite versus Finite

Functions on finite sets are special.

Lemma

Let $f : A \to A$ where A is finite.
Then f is injective if, and only if, f is surjective if, and only if, f is bijective.

But for A infinite, we can always find functions $A \to A$ that are

- injective but not surjective, or
- surjective but not injective

Example

$$f : \mathbb{N} \to \mathbb{N} \qquad f(x) = 2x$$
$$g : \mathbb{N} \to \mathbb{N} \qquad g(x) = \lfloor x/2 \rfloor$$

Digression: Dedekind Infinity

One could even use this property to define infinity:

Definition

A set A is Dedekind-infinite if there an injective function $f : A \to A$ whose range is a proper subset of A.

Note that this is similar to but different from the traditional definition: a set A is infinite if there is an injective function $f : \omega \to A$.

One major advantage of Dedekind's definition is that it makes no reference to ω or $\mathbb{N}$. So there is no need to construct the naturals first, the concept of injectivity is enough.

Digression: Dedekind Infinity

If we argue in intuitive set theory, then the two definitions are equivalent.

Proposition

A set is infinite if, and only if, it is Dedekind-infinite.

Sketch of proof.

We know that for A finite any injection is surjective, so any Dedekind-infinite set must be infinite.

For the opposite direction, suppose we have an infinite set A. Hence there is a bijection $f : \kappa \to A$ where κ is an infinite cardinal. Then $a \mapsto f(f^{-1}(a) + 1)$ works.

□

Pigeons

One way to think about the last argument is as a "counterexample" to the Pigeon Hole Principle: PHP falls apart in the infinite case, and that sometimes helps a lot with combinatorial proofs.

Lemma (Pigeon Hole Principle (PHP))

For $m > n$, m pigeons will not fit into n pigeon holes.

Less informally: There are no injections $[m] \to [n]$ when $m > n$.

As one might suspect, PHP does not work that well with infinite sets.

Hilbert's Hotel

As a matter of fact, PHP fails totally and miserably when we have an infinite ω sequence of pigeon holes

$$h_0, h_1, h_2, \ldots, h_n, \ldots$$

We can easily fit $\omega + 1$ pigeons in there:

Everybody just moves over by one hole.

Since there is no last hole (whose occupant would be kicked out) there is no problem. This device is also known as Hilbert's Hotel.

Scary Generalization

Nothing can stop us from repeating this move-over process.

So we can fit $\omega + 2$ pigeons, $\omega + 3$ pigeons, and even $\omega + k$ pigeons into ω holes, for all k.

All the this notation is informal, we have not said what this type of arithmetic should be, but trust me: it's all perfectly fine. In many ways it's much more interesting that ordinary arithmetic on the naturals.

A moment's thought shows that even $\omega + \omega$ pigeons, $\omega + \omega + \omega$ pigeons, ... will fit.

We can even push much, much further than this. Think about arrangements like

$$1, 3, 5, \ldots, 2, 6, 10, \ldots, 4, 12, 20, \ldots, 8, 24, 40, \ldots, 2^k, 2^k \cdot 3, 2^k \cdot 5, \ldots$$

This means we can store $\omega \times \omega = \omega^2$ pigeons in ω holes.

An so on, ad nauseam: ω^3, ω^4, ω^k and even ω^ω (this is not a statement about the cardinality of ω^ω).

To explain what is going on here one needs to discuss the order types of well-orderings; we'll pass.

Countability

Definition

Let A be a set.

- A is countable if there is a bijection $f : \omega \longleftrightarrow A$.
- A is uncountable if A is neither finite nor countable.

So a set is countable if it can be listed just like ω.

$$a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots$$

This is the same idea as being enumerable, but there is no restriction on computability here.

Notation Warning: Some people define countable to include finite.

Rationals are Countable

How large is the Cartesian product $\omega \times \omega$? For every $n \in \omega$ there are ω-many m so that (n, m) is in the product.

So $\omega \times \omega$ should be infinitely larger than ω. Nice try, but:

Theorem (Cantor)

ω and $\omega \times \omega$ have the same cardinality.

Proof.

Recall the pairing function from the lecture on register machines.

□

A Helpful lemma

Lemma

Let $f : \omega \to A$ be a surjection and $B \subseteq A$.
Then B is finite or countable.

Proof.

Here is a convoluted recursive definition:

$$g(n) = f\big(\min\big(\, j \in \omega \mid f(j) \in B \wedge \forall\, i \;< n(f(j) \neq g(i))\,\big)\big)$$

If B is finite, the domain of g is some $\nu < \omega$, otherwise it is all of ω.

Check that g is a bijection. □

For $A = B$ this means: if there is a surjection $\omega \to A$, there already is a bijection. Just redefine the function so it does not hit the same element in A twice.

Words are Countable

How many words over a fixed alphabet (say, ASCII) are there?

The easiest way to see that there are countably many is to arrange them into a sequence

$$a_0, a_1, a_2, \ldots, a_n, \ldots$$

The easiest way of doing this for words is to use length-lex order. E.g., for alphabet $\{a, b, c\}$ we get:

$$\varepsilon, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, \ldots$$

Note that standard lexicographic order does not work in this case:

$$b > ab > aab > aaab > \ldots > a^n b > a^{n+1} b > \ldots$$

Drastic Consequence

Theorem

There are only countably many algorithms.

Proof.

We already know that register machines can be coded as natural numbers, and algorithms are represented by register machines.

□

The last claim is of course a dirty lie, but it makes life pleasant.

At least in mathematics we encounter uncountably many objects; for example the set of reals is irreparably uncountable. So most reals are not computable (which fact is in part responsible for the fact that numerical methods can be very difficult).

Bizarre Results

Cantor's definitions raised a few eyebrows when applied to analysis.

Lemma

The unit interval $[0,1] \subseteq \mathbb{R}$ *has the same size as unit square* $[0,1]^2 \subseteq \mathbb{R}^2$*:*

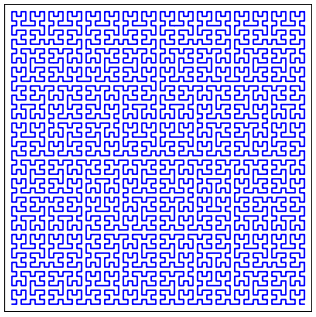
$$|[0,1] \times [0,1]| = |[0,1]|.$$

This is rather counter-intuitive; one automatically looks for "nice" functions (continuous, differentiable, etc.). Cantor himself wrote:

> "... I see it, but I can't believe it."

Again: the bijection which establishes this result is not a particularly natural map (i.e. not the kind of map one comes across naturally in analysis). But, it can be constructed very precisely, there is doubt that it exists.

Hilbert's Approach



One possible way of finding such a bijection is to design a sequence of curves that fill the whole unit square in the limit. This one is due to Hilbert.

Cardinality Quiz

Here are some infinite sets whose cardinality one would like to pin down.

set	cardinality
$\mathbb{N}$	???
$\mathbb{Z}$	???
$\mathbb{Q}$	???
algebraic numbers	???
$\mathbb{R}$	???
$\mathbb{R}^n$	???
$\mathfrak{P}(\mathbb{N})$	???
$\mathbb{N} \to \mathbb{N}$	???
$\mathbb{N} \to \mathbb{R}$	???
$\mathbb{R} \to \mathbb{R}$	???
continuous $\mathbb{R} \to \mathbb{R}$	???

Three Theorems

Theorem (Schröder-Bernstein)

Suppose $f : A \to B$ *and* $g : B \to A$ *are injective.*
Then A *and* B *have the same cardinality.*

Theorem (Cantor)

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

Theorem (Cantor)

For any set A*, the cardinality of* $\mathfrak{P}(A)$ *is greater than the cardinality of* A*.*

Say What? 37

Schröder-Bernstein is really a sanity check.
We want for all cardinals κ and λ

$$\kappa \leq \lambda \text{ and } \lambda \leq \kappa \text{ implies } \kappa = \lambda$$

Cantor's first theorem shows that there are at least two levels of infinity, and that they play a role in calculus.

Cantor's second theorem shows that there are infinitely many levels of infinity:

$$|\omega| < |\mathfrak{P}(\omega)| < |\mathfrak{P}^2(\omega)| < |\mathfrak{P}^3(\omega)| < \dots$$

Schröder-Bernstein 38

Given injective functions $f : A \to B$ and $g : B \to A$, we have to construct a bijection $h : A \to B$.

This is trivial if f or g is surjective. But what if not? Clearly, we have to use both f and g.

Basic Idea: Use f forward and g backward.

$$h(a) = f(a) \quad \text{and} \quad h^{-1}(b) = g(b)$$

for some $a \in A$ and $b \in B$.

We need to be careful to avoid clashes: we could have $a = g(b)$ and $b \neq f(a)$. And, this could happen indirectly.

Avoiding Clashes 39

To avoid clashes in the definition of the bijection, consider alternating chains of the form:

$$a_0 \xrightarrow{f} b_0 \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} a_2 \xrightarrow{f} b_2 \xrightarrow{g} \dots$$

A maximal chain is one that cannot be further extended, at either end.

Observation: Maximal chains must be of one of the following three types:

- Finite: starts and ends at same point.
- One-way infinite: extends forward forever.
- Two-way infinite: extends forward and backward forever.

Chains 40

Observation: In the finite case the cycle must have even length and wrap around at the starting point:

$$a_0 \xrightarrow{f} b_0 \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} a_2 \xrightarrow{f} b_2 \xrightarrow{g} a_0$$

This is really the old lasso problem: wrapping around anywhere else would break injectivity.

In the one-way infinite case, the starting point can be either in A or in B, more precisely in $A - \operatorname{rng} g$ or $B - \operatorname{rng} f$. In the second case we write

$$b_0 \xrightarrow{g} a_0 \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} b_2 \xrightarrow{g} a_2 \xrightarrow{f} \dots$$

Two-way infinite chains are similarly indexed by $\mathbb{Z}$.

Defining h 41

But then we can define a function h by setting

$$h(a_i) = b_i$$

The part of h coming from finite cycles, bi-infinite chains and one-way infinite chains starting in A is clearly injective: we have $h(a_i) = f(a_i)$. For a one-way infinite chain starting in B we have $b_0 \notin \operatorname{rng} f$, and injectivity is preserved.

For surjectivity note that every element b of B appears in exactly one maximal chain. Thus, b is in the range of h.

□

Application 42

It is easy to show that the open interval $(0, 1) \subseteq \mathbb{R}$ has the same cardinality as all of $\mathbb{R}$:

$$f : (0, 1) \to \mathbb{R}$$
$$f(x) = \tan \pi(x - 1/2).$$

How about the half-open interval $[0, 1) \subseteq \mathbb{R}$?

This is trivial with Schröder-Bernstein: all we need is 2 injections

$$f^{-1} : \mathbb{R} \to (0, 1) \subseteq [0, 1)$$
$$\mathsf{Id} : [0, 1) \to \mathbb{R}$$

Exercises

Exercise

Construct a bijection $g : [0, 1) \to \mathbb{R}$ by hand, without using the theorem.

Exercise

Likewise, show that $\text{card}([0, 1]) = \text{card}(\mathbb{R})$ *without using the theorem.*

Another Cardinality Result

Here is a proof I found in a textbook (the author will go unnamed and unmentioned; actually, by now I have forgotten).

Problem: Show that $\mathfrak{P}(\omega)$ and $[0, 1] \subseteq \mathbb{R}$ have the same cardinality.

At this point you should protest and ask: what on earth are the reals, in the strict sense of set theory? Don't say: the numberline.

We will forego the opportunity to inflict cognitive pain on the student body and simply repeat the argument from the book.

"Argument"

Think of any subset $A \subseteq \omega$ as a binary expansion:

$$x_A = 0.d_1d_2d_3 \ldots = \sum d_i 2^{-i}$$

where

$$d_{i+1} = \begin{cases} 1 & \text{if } i \in A, \\ 0 & \text{otherwise.} \end{cases}$$

For example, we have

$x_\emptyset = 0$, $x_\omega = 1$, $x_{\{0\}} = 1/2$, $x_{\{2\}} = 1/8$

$x_{even} = 1/4 + 1/16 + 1/64 + \ldots = 1/3$

$x_{prime} = 1/4 + 1/8 + 1/32 + \ldots \approx 0.414683$

Moving right along

This defines a map

$$f : \mathfrak{P}(\omega) \to [0, 1]$$
$$f(A) = x_A$$

and, according to our anonymous author, one can check that the map is a bijection.

Exercise

Give a detailed critique of this argument.

Cantor: Diagonalization

Warm-up: The number of binary sequences of length n is larger than n.

Yes, yes, we can do this by counting, but ordinary counting does not work for infinite sets; we need a different approach.

We will prove something more constructive:
Given n binary sequences s_i, $i < n$, of length n, there is a binary sequence t that differs from all of them.

Here goes: given s, define t by

$$t(i) = 1 - s_i(i).$$

where $i < n$. Then t differs from all the s_i in at least one bit, so $t \neq s_i$ for all $i < n$.

Note that t is obtained by mucking with the diagonal sequence $s_i(i)$.

Flipping Bits

We get t by flipping each bit along the diagonal of a matrix. Hence the resulting sequence cannot be a row in the matrix.

$$\begin{array}{ccccc} s_0(0) & s_0(1) & s_0(2) & \ldots & s_0(n-1) \\ s_1(0) & s_1(1) & s_1(2) & \ldots & s_1(n-1) \\ s_2(0) & s_2(1) & s_2(2) & \ldots & s_2(n-1) \\ \vdots & & & & \vdots \\ s_{n-1}(0) & s_{n-1}(1) & s_{n-1}(2) & \ldots & s_{n-1}(n-1) \end{array}$$

In general, it does not matter how we change the element $s_i(i)$ in t, it just has to be different. With bits there is only one choice, of course.

The Key Insight

This also works for infinite sequences.

Simply replace $i < n$ by $i < \omega$ and everything works just fine.

Claim

There are uncountably many binary sequences: $\omega \to \mathbf{2}$ is uncountable.

Note that $|\mathfrak{P}(\omega)| = |\omega \to \mathbf{2}|$: a map $f : \omega \to \mathbf{2}$ is just a bitvector (characteristic function) for a subset of ω. So we know that $\mathfrak{P}(\omega)$ is uncountable.

The Real Thing

To show that $\mathbb{R}$ is uncountable it clearly suffices to show that the open interval $(0, 1) \subseteq \mathbb{R}$ is uncountable. Assume we have an enumeration of $(0, 1)$, i.e., a list

$$x_0, x_1, x_2, \ldots, x_n, x_{n+1}, \ldots$$

that contains each real in $(0, 1)$ exactly once. Since $0 < x_i < 1$, we have decimal expansions

$$x_i = 0.x_{i1}x_{i2}x_{i3}\ldots$$

This representation is potentially ambiguous, so let's agree that that there are no trailing infinite blocks of 9's: increment previous digit, and replace by 0's.

E.g., write 0.1235, not $0.1234999999\ldots$.

Contd.

Now define digits y_j by

$$y_j = \begin{cases} 3 & \text{if } x_{jj} = 2, \\ 2 & \text{otherwise.} \end{cases}$$

and let $y = \sum y_j \cdot 10^{-j}$.

Note that y has only decimal digits 2 and 3, and in particular no trailing 9's. Hence $0 < y < 1$.

Now suppose $y = x_i$ for some i.

Then x_i also has only decimal digits 2 and 3, and we must have $x_{ij} = y_j$ for all j, clearly contradicting the construction: $x_{ii} \neq y_i$.

□

Again . . .

Just to hammer this home: It is not true in general that

$$\sum a_i \cdot 10^{-i} = \sum b_i \cdot 10^{-i}$$

implies

$$a_i = b_i \qquad \text{for all } i.$$

In fact, we could have $a_i \neq b_i$ for all i.

It is really necessary to deal with the trailing 9's issue.

Cantor II

The next task is to show that the cardinality of $\mathfrak{P}(A)$ is strictly greater than the cardinality of A.

There is a trivial injection from A to $\mathfrak{P}(A)$: $a \mapsto \{a\}$.

So suppose there is a surjection $f : A \to \mathfrak{P}(A)$.

Think of a as a "name" for $f(a)$.

Define a set

$$B = \{\, a \in A \mid a \notin f(a) \,\} \subseteq A.$$

Since f is surjective, we must have $B = f(b)$ for some $b \in A$.

But then $b \in B$ implies $b \notin B$, and conversely; contradiction.

Cantor vs. Russell

Note that Cantor's construction is very similar to Russell's paradox, surprisingly Cantor never made the transition.

$$S = \{\, x \mid x \notin x \,\}$$

$$B = \{\, a \in A \mid a \notin f(a) \,\}$$

The existence of S is contradictory, but can be proved from Frege's axioms (though presumably not in Zermelo-Fränkel set theory).

But there is nothing wrong with B, it just shows that f cannot be surjective (and can be proved to exist in Zermelo-Fränkel set theory).

More on Diagonalization

Diagonalization is a key technique in computability and complexity theory.

Go back to the undecidability proof of the Halting Problem and you can see the exact same idea in action.

The only difference is that we are dealing with computable maps, rather that set-theoretic ones.

So Cantor inadvertently also provided a fundamental technique for computability theory.

Cardinal Numbers

A few last comments on cardinals: it would lead us too far astray to really discuss the theory of cardinals, but the principal idea is easy to convey:

Definition

A cardinal is an ordinal κ such that there is no injection $\kappa \to \alpha$ where $\alpha < \kappa$.

For example, ω is a cardinal, but $\omega + \omega$ is not: there is an injection into ω.

The same is true for ω^ω and the like.

In fact, the least uncountable cardinal $\aleph_1$ cannot really be constructed via ordinal arithmetic from below.

Cardinal Arithmetic

For cardinals to be truly useful we also need some kind of arithmetic on them; operations like addition, multiplication and so on: we need these operations to express the cardinality of a compound set in terms of the cardinalities of its components.

Occasionally, infinite arithmetic is quite straightforward. For example, it is true for any infinite cardinal κ that

$$\kappa + \kappa = \kappa \cdot \kappa = \kappa$$

In fact, with (AC) we even have

$$\kappa + \lambda = \kappa\lambda = \max(\kappa, \lambda)$$

The Swamp

Alas, overall cardinal arithmetic is hugely complicated and very difficult to analyze. For example, in ordinary set theory one cannot even determine the relative size of

$$2^{\aleph_0} \text{ versus } \aleph_1.$$

Of course, $2^{\aleph_0} \geq \aleph_1$ but equality is open. This is the famous Continuum Hypothesis and caused Cantor endless grief. As it turns out, things could go either way and one can choose $2^{\aleph_0}$ to be just about anything one would like it to be.

Summary