

CDM

Three Theorems

Klaus Sutner
Carnegie Mellon University
www.cs.cmu.edu/~sutner

Battleplan

- Counting: Finite vs. Infinite
- Cardinality
- Countable Sets
- Three Theorems
- Diagonalization

Cantor and Cardinality

Cardinality

Definition 1. *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.

Thus e.g. the finite set

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

has cardinality n (where we tacitly assume that $a_i \neq a_j$ for $i \neq j$).

Defining the Naturals

Note that we cannot define \mathbb{N} by something along the lines of

$$\mathbb{N} = \{S^n(0) \mid n \geq 0\}$$

where $S(x) = x \cup \{x\}$ is the successor function and $0 = \emptyset$: the index n ranges over the set we are trying to define. Requiring to apply S finitely often is also circular. Here is a way around these problems.

Definition 2. *A set X is a successor set if $\emptyset \in X$ and $x \in X \rightarrow S(x) \in X$.*

Define \mathbb{N} to be \subseteq -least successor set.

This definition works since successor sets are closed under intersection, so we can form

$$\mathbb{N} = \bigcap \{X \mid X \text{ successor set}\}.$$

Defining Finiteness

So \mathbb{N} is the least collection of von Neumann ordinals that contains N_0 and is closed under successors.

We can now adopt the **definition** that these are exactly the finite von Neumann ordinals.

As we have seen, these numbers are ordered by \in and we have

$$N_n = \{N_0, N_1, \dots, N_{n-1}\}$$

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

Finiteness of some set A now means that we can establish a bijection between some $N_n \in \mathbb{N}$ and A , which conforms nicely with our intuition (if we use 0-indexing).

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

Infinite Cardinality

But for infinite sets things become more complicated.

Definition 3. 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 a cardinal number is.

How would we go about doing this?

First, there are some properties that cardinal numbers should have. They should extend \mathbb{N} so that:

- A is finite iff $|A| \in \mathbb{N}$.
- For any $n \in \mathbb{N}$, we want $n < |\mathbb{N}|$.
- We want the cardinal numbers to be ordered:

$$|A| < |B| \vee |A| = |B| \vee |A| > |B|.$$

Reification

More abstractly, we can use an approach similar to Frege's association of an extension with each concept.

We would like to associate objects $|A|$ with sets A in such a way that

$$|A| = |B| \iff A \text{ has the same cardinality as } B$$

So the first question we need to answer carefully is this: what does it mean for two sets to have the same cardinality, to be equinumerous?

Then we will worry about how to obtain reasonable objects $|A|$. For example, we will have to figure out what the arithmetic of cardinal numbers should be.

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:

$$f : M \leftrightarrow N.$$

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 Definition

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

Definition 4.

$$|A| = |B| \iff \exists f \text{ bij. } (f : A \rightarrow B)$$

$$|A| \leq |B| \iff \exists f \text{ inj. } (f : A \rightarrow B)$$

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

Exercise 1. Verify that at least for finite sets this all makes perfect sense: we obtain the intuitive notion of size of a finite set.

Sanity Check

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

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

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 does not imply 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

- $f : [n] \rightarrow X$ for some natural number n ,
- $f : \mathbb{N} \rightarrow X$, and
- $f : \mathfrak{P}(\mathbb{N}) \rightarrow X$.

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.

Injections versus Surjections

Lemma 1. *There is an injection $f : A \rightarrow B$ if, and only if, there is a surjection $g : B \rightarrow A$.*

Proof.

Assume f . Pick $a_0 \in A$. Set

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

Assume g . 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 2. *Let $f : A \rightarrow A$ 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 $A \rightarrow A$ that are

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

Example 1.

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{N} & f(x) &= 2x \\ g : \mathbb{N} &\rightarrow \mathbb{N} & g(x) &= \lfloor x/2 \rfloor \end{aligned}$$

Dedekind Infinity

One could even use this property to define infinity:

Definition 5. *A set A is **Dedekind-infinite** if there an injective function $f : A \rightarrow A$ 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 $f : \mathbb{N} \rightarrow A$.

One advantage of Dedekind's definition is that it makes no reference to \mathbb{N} . So there is no need to construct the naturals first.

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

Proposition 1. *A set is infinite if, and only if, it is Dedekind-infinite.*

Exercise 2. *Prove the last proposition.*

Pigeons

Here is one interesting principle for finite sets that falls apart in the infinite case, and that sometimes helps a lot with combinatorial proofs.

Lemma 3. *Pigeon Hole Principle (PHP)*
For $m > n$, m pigeons will not fit into n pigeon holes.

Less informally:

There are no injections $[m] \rightarrow [n]$ when $m > n$.

Expressed this way, we can prove the PHP by induction.

PHP Proof

Proof.

It suffices to show the result for $m = n + 1$. We use Induction on n .

Base case $n = 0$ is clear: $[0] = \emptyset$ but $[1] = \{1\}$.

Step $n > 0$: For the sake of a contradiction, suppose $f : [n + 1] \rightarrow [n]$ is an injection.

Let $a = f(n + 1)$, define function $g : [n] \rightarrow [n - 1]$ by

$$g(i) = \begin{cases} f(i) & \text{if } f(i) < a, \\ f(i) - 1 & \text{otherwise.} \end{cases}$$

It is easy to check that g is an injection.

But this contradicts the IH, done. □

Application

Proposition 2. *Let $A \subseteq [2n]$ of size $n + 1$. Then there exists $a, b \in A$ such that a divides b .*

Proof.

Here is a trick: consider the odd part of a number: $a = 2^k \cdot a_0$.

For $a \in A$, the odd parts range over $1, 3, 5, \dots, 2n - 1$.

By PHP, there must be two elements in A with the same odd part:

$$a = 2^k \cdot a_0 \text{ and } b = 2^l \cdot a_0.$$

Done. □

Try to do this without PHP. Let me know if you come up with some elegant argument.

Application 2

Proposition 3. Choose n positive integers a_1, \dots, a_n , not necessarily distinct. Then there are $1 \leq r \leq s \leq n$ such that n divides $\sum_{i=r}^s a_i$.

Proof.

Consider the set of all partial sums

$$S = \left\{ \sum_{i=1}^k a_i \mid k = 0, \dots, n \right\}$$

Then S has size $n + 1$.

By the PHP, two partial sums must have the same remainder upon division by n .

But then their difference does the job. □

\mathbb{N} Pigeon Holes

Before we talk about cardinals, let us take a closer look at the Pigeon Hole Principle. PHP fails miserably when we have an infinite sequence of pigeon holes

$$h_0, h_1, h_2, \dots, h_n, \dots$$

We can fit $\mathbb{N} + 1$ pigeons in there:

$$\begin{array}{l} \text{holes : } h_0 \ h_1 \ h_2 \ h_3 \ \dots \ h_n \ \dots \\ \text{pigeons: } q \ p_0 \ p_1 \ p_2 \ \dots \ p_{n-1} \ \dots \end{array}$$

Everybody just moves over by one hole.

Since there is no last hole (whose occupant would be kicked out) there is no problem.

Iceberg

Of course, we can repeat.

So we can fit $\mathbb{N} + 2$ pigeons, $\mathbb{N} + 3$ pigeons, and even $\mathbb{N} + k$ pigeons into \mathbb{N} holes, for all k . All the this notation is informal, we have not said what this type of arithmetic should (or could possibly) be.

A moment's thought shows that even $\mathbb{N} + \mathbb{N}$ pigeons, $\mathbb{N} + \mathbb{N} + \mathbb{N}$ pigeons, \dots will fit.

We can even push further. Think about arrangements like

$$1, 3, 5, \dots, 2, 6, 10, \dots, 4, 12, 20, \dots, 8, 24, 40, \dots$$

This means we can store $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ pigeons in \mathbb{N} holes.

An so on, ad nauseam: \mathbb{N}^3 , \mathbb{N}^4 , \mathbb{N}^k and even $\mathbb{N}^{\mathbb{N}}$ (this is not a statement about the cardinality of $\mathbb{N}^{\mathbb{N}}$).

To explain what is going on here we have to discuss the *order types* of well-orderings.

Countability

Countability

Definition 6. Let A be a set.

- A is **countable** if there is a bijection $f : \mathbb{N} \rightarrow A$.
- A is **uncountable** if A is neither finite nor countable.

So a set is countable if it can be listed just like \mathbb{N} .

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

Example 2. The integers are countable:

$$0, 1, -1, 2, -2, 3, -3, \dots, n, -n, \dots$$

Question: Are the rationals and reals countable?

Rationals are Countable

How large is $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$? For every $n \in \mathbb{N}$ there are \mathbb{N} -many m so that $(n, m) \in \mathbb{N}^2$.

So \mathbb{N}^2 should be infinitely larger than \mathbb{N} . But:

Theorem 1. Cantor

\mathbb{N} and $\mathbb{N} \times \mathbb{N}$ have the same cardinality.

Proof. To prove this, we need a bijection $\pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, a so-called *pairing function*. Here is a particularly simple one:

$$\begin{aligned} \pi(x, y) &= \frac{(x+y+1)(x+y)}{2} + x \\ &= \binom{x+y+1}{2} + x \end{aligned}$$

□

Not So Fast

It is not clear that this function is really a bijection, but look at a table of the first few values:

0	1	3	6	10	15	21	28
2	4	7	11	16	22	29	37
5	8	12	17	23	30	38	47
9	13	18	24	31	39	48	58
14	19	25	32	40	49	59	70
20	26	33	41	50	60	71	83
27	34	42	51	61	72	84	97

Exercise 3. Give a proof that the pairing function π is a bijection.

Exercise 4. Determine the “inverse” functions

$$\pi_1, \pi_2 : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$$

$$x = \pi_1(\pi(x, y)), y = \pi_2(\pi(x, y))$$

A Helpful Lemma

Lemma 4. Let $f : \mathbb{N} \rightarrow A$ be a surjection and $B \subseteq A$. Then B is finite or countable.

Proof.

Here is a convoluted recursive definition:

$$g(n) = f(\min(j \in \mathbb{N} \mid f(j) \in B \wedge \forall i < n(f(j) \neq g(i))))$$

If B is finite, the domain of g is some $[m]$, otherwise it is all of \mathbb{N} .

Check that g is a bijection. □

For $A = B$ this means: if there is a surjection $\mathbb{N} \rightarrow A$, 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

$$a_0, a_1, a_2, \dots, a_n, \dots$$

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

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

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

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

Drastic Consequence

Theorem 2. There are only countably many algorithms.

Proof.

To see this, note that any conceivable algorithm could be represented by a finite string over some fixed, finite alphabet. For example, we could use a standard programming language or specify a Turing machine.

Since there are only countably many words over any finite alphabet there are only countably many programs by the lemma. □

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 5. 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.).

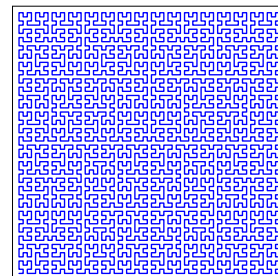
G. Cantor, who discovered this fact, himself wrote:

“... 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}	???
\mathbb{R}	???
$\mathfrak{P}(\mathbb{N})$???
List($\mathbb{2}$)	???
List(\mathbb{N})	???
$\mathbb{R} \rightarrow \mathbb{R}$???
C programs	???

Three Theorems

Three Theorems

Theorem 3. Schröder-Bernstein

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

Theorem 4. Cantor

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

Theorem 5. Cantor

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

Say What?

► Schröder-Bernstein is really a sanity check.
We want for all cardinals κ and λ (represented by sets of this size)

$$\kappa \leq \lambda \wedge \lambda \leq \kappa \rightarrow \kappa = \lambda$$

► 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:

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

Schröder-Bernstein

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

Trivial if f or g is surjective. But what if not?

Have to use both f and g .

Basic idea: use f forward and g backward.

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

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

Careful to avoid clashes: we could have $a = g(b)$ and $b \neq f(a)$.

And, this could happen more indirectly.

Avoiding Clashes

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

$$a_1 \xrightarrow{f} b_1 \xrightarrow{g} a_2 \xrightarrow{f} b_2 \xrightarrow{g} a_3 \xrightarrow{f} b_3 \xrightarrow{g} \dots$$

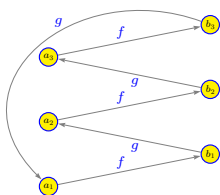
A **maximal chain** is one that cannot be further extended, at either end.

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.
Can start in A or in B .
- Two-way infinite: extends forward and backward forever.

Tricky part: why can't we wrap around just anywhere?

Cycles



In each case, define the bijection h by setting

$$h(a_i) = b_i$$

except for a one-way infinite chain starting in B , in which case

$$h(a_i) = b_{i-1}$$

It is routine to check that h is in fact a bijection. □

Application

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

$$f : (0, 1) \rightarrow \mathbb{R}$$

$$f(x) = \tan \pi(x - 1/2).$$

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

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

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

$$\text{Id} : [0, 1) \rightarrow \mathbb{R}$$

Exercise

Exercise 5. Construct a bijection $g : [0, 1) \rightarrow \mathbb{R}$ by hand, without using the theorem.

Exercise 6. 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).

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

Solution:

Think of any subset $A \subseteq \mathbb{N}$ as a binary expansion:

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

where

$$d_i = \begin{cases} 1 & \text{if } (i-1) \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Another Result . . .

For example, we have

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

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

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

This defines a map

$$f : \mathfrak{P}(\mathbb{N}) \rightarrow [0, 1]$$

$$f(A) = x_A$$

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

Exercise 7. 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.

So: assume there are only n many binary sequences s_1, \dots, s_n .

Construct a binary sequence t by

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

Then t differs from all the s_1, \dots, s_n in at least one bit.

But then $t \neq s_i$ for all $i = 1, \dots, n$.

So there must be more than n sequences.

Flipping Bits

Think of this as flipping each bit along the diagonal of a matrix. The resulting sequence cannot be a row in the matrix.

$$\begin{array}{cccccc} s_1(1) & s_1(2) & s_1(3) & \dots & s_1(n) \\ s_2(1) & s_2(2) & s_2(3) & \dots & s_2(n) \\ s_3(1) & s_3(2) & s_3(3) & \dots & s_3(n) \\ \vdots & & & & \vdots \\ s_n(1) & s_n(2) & s_n(3) & \dots & s_n(n) \end{array}$$

Easy observation: This also works for infinite sequences.

Hence there are uncountably many binary sequences: $\mathbb{N} \rightarrow \mathbb{B}$ is uncountable.

Note that $|\mathfrak{P}(\mathbb{N})| = |\mathbb{N} \rightarrow \mathbb{B}|$: a map $f: \mathbb{N} \rightarrow \mathbb{B}$ is just a bitvector (characteristic function) for a subset of \mathbb{N} . So we know that $\mathfrak{P}(\mathbb{N})$ 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

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

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

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

This representation is ambiguous, so let's agree 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...

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

$$\begin{aligned} a &= \sum a_i \cdot 10^{-i} \\ b &= \sum b_i \cdot 10^{-i} \\ a &= b \end{aligned}$$

implies

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

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 $f: A \rightarrow \mathfrak{P}(A)$.

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.

$$\begin{aligned} S &= \{x \mid x \notin x\} \\ B &= \{a \in A \mid a \notin f(a)\} \end{aligned}$$

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.

To keep things simple, we only consider programs that take as input a single natural number. That's actually no restriction at all: we already know how to express sequences of natural numbers as single numbers, and that is enough to code any data structure whatsoever.

So, we have functions $f : \mathbb{N} \rightarrow \mathbb{N}$. Certainly, some of these functions can be computed by programs, say, C-programs, that take a single integer as input, and return an integer as output.

It is straightforward to write an interpreter Eval which, on input the program text P and an integer n , will return the result of evaluating P on n :

$$P(n) = \text{Eval}(P, n).$$

Some programs do not stop on all inputs, so sometimes $\text{Eval}(P, n)$ will not terminate.

Halting Problem

How about a program Stop that tests if P on input n halts?

Theorem 6. *Halting Problem*

The Halting Problem is unsolvable: there is no algorithm to test whether a given program halts on a given input.

Proof. Assume otherwise, so we have a program Stop that on input P and n determines whether P on input n halts.

Fix an enumeration of all programs, P_0, P_1, P_2, \dots

Now define a function $f : \mathbb{N} \rightarrow \mathbb{N}$ as follows.

- On input n , first use Stop to check if P_n halts on input n .
- If so, say the output is m , set $f(n) = m + 1$.
- Otherwise, set $f(n) = 0$.

Clearly, f is computable: we could turn the description above into a C program (with actually not too much effort).

But then f must be computed by some program, say, P_e .

From the definitions, $f(e) = P_e(e) + 1$, contradiction. \square

Hence, the Halting Problem is unsolvable (or *undecidable*), regardless of questions of computational resources.

You can turn the whole universe into a computer (about 10^{80} stable particles), think of each particle as a super computer (10^{13} ops/sec), and assume the whole virtual device has been running since the Big Bang (10^{18} sec): it still won't work.

More Undecidability

A great many other questions in math and computer science are also undecidable.

- Check whether a program halts on all inputs.
- Check whether a Diophantine equation (polynomial integer equation) has an integer solution (Hilbert's 10th).
- Check whether one can cover the plane with colored tiles.
- Check whether a formula is a theorem of, say, arithmetic.

This is undecidability in principle, not just in practice.

Feasible Computations

In reality, we have a more complicated hierarchy:

- highly undecidable
- undecidable
- non-feasible
- feasible

Undecidability surfaced in the 1930's, non-feasible problems in the 1960's (computational complexity theory).

Only feasible problems really yield to computational attack.

The non-feasible ones have algorithms that solve them, but they are too slow to be of any use.

Typical example: Satisfiability testing for propositional formulae.

OK, so what?

Some combinatorial problems that turn out to be non-feasible, like Satisfiability, are a fairly direct analogue of the problems that were recognized to be unsolvable some 60 years ago.

So, undecidability casts shadows into the world of efficient algorithms.

► Truth in Advertising

Satisfiability is actually not known to be non-feasible at this point (2006): all we have is a result that says a complexity hierarchy collapses if a polynomial time algorithm for Satisfiability exists.

But, a lot of people will jump out of very tall buildings if such an algorithm should materialize.

Also, in many practical case there are algorithms (Davis/Putnam) that successfully handle propositional formulae of enormous size.

Cardinal Numbers

Time to pin down what we really mean *cardinal numbers*. We would like to define a collection Card that is a natural extension of \mathbb{N} to the transfinite realm. Clearly we want Card to be a total order.

In fact, we even want some kind of cardinal arithmetic such as addition, multiplication and so on: we will need these operations to express the cardinality of a compound set in terms of the cardinalities of its components.

Conceptually, the infinite case is more difficult since infinite cardinals are harder to explain than natural numbers. Surprisingly, though, in practice finite counting is often harder, there are lots of very difficult technical problems.

Infinite counting, on the other hand, is often a piece of cake: we don't have to worry about details as much. For example, it is true for any infinite cardinal κ that

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

This simplifies arithmetic quite a bit.

Summary

- The concept of size of a set can be captured in the notion of cardinality.
- The comparison of cardinalities is based on the existence of injective and bijective functions between the sets in question.
- The Schröder-Bernstein theorem guarantees that this approach is sound.
- Given the right set theory, we obtain a total order of all sets by size.
- We can reify cardinality by defining cardinal numbers as sets, and develop their arithmetic.
- For computer science, one fundamental result is that the collection of all algorithms is countable (whereas the reals e.g. are uncountable).