Georg Cantor (1845-1918):
The man who tamed infinity

lecture by Eric Schechter
Associate Professor of Mathematics
Vanderbilt University
http://www.math.vanderbilt.edu/∼schectex/

In papers of 1873 and 1874, Georg Cantor outlined the basics of infinite set theory.

Prior to Cantor's time, ∞ was

- mainly a metaphor used by theologians
- not a precisely understood mathematical concept
- a source of paradoxes, disagreement, and confusion

One of Zeno's paradoxes

Zeno of Elea
(490 BC – 425 BC, in what is now Italy)

There is no motion, because to get anywhere you'd first have to get halfway, and before that you'd have to get a quarter of the way, etc.

Of course, Zeno didn't actually *believe* that. He was just pointing out how poorly ∞ was understood.

Today we might try to explain Zeno's paradox this way:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\frac{1}{32}+\cdots \quad = \quad 1$$

(The sum of an infinite series is defined to be the limit of the finite partial sums.)

But Zeno's contemporaries didn't understand summations so well. Zeno would claim that you never quite get to 1.

[reminder: insert here, joke about engineer and mathematician watching a dance]

Actually, Zeno's paradox is more like *this* equation:

$$\cdots + \frac{1}{32} + \frac{1}{16} + \frac{1}{8} + \frac{1}{4} + \frac{1}{2} \quad = \quad 1$$

This summation is *harder* to imagine — you have infinitely many steps before you get halfway, or before you get 1/4 of the way, etc. So if each step takes (for instance) 1 second, then you never really get anywhere!

Another series paradox

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \frac{1}{9} - \cdots$$

$$= \quad 0.6931471805599\cdots \quad = \quad \log_e(2)$$

However, if we add those same terms in a different order,

$$1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \frac{1}{11} - \frac{1}{6} + \cdots$$

$$= \quad 1.03972077084\cdots \quad = \quad \frac{3}{2}\log_e(2)$$

But that's not so surprising, if you think about how you turn the "hot" and "cold" knobs to adjust your shower's temperature.

Complaints about calculus

In the 17th century, Newton and Leibniz invented calculus. They knew how to do the computations but not the proofs.

> Their theory involved **infinitesimals** — i.e., nonzero numbers that are *infinitely small*.

Other mathematicians complained that the proofs were not rigorous, that infinitesimals didn't make sense.

> George Berkeley (1685 – 1753) derided infinitesimals as "ghosts of departed quantities."

In the early 19th century, Cauchy showed that *it is not necessary to use infinitesimals*; calculus can be explained without them.

In the late 19th century, Richard Dedekind gave the first rigorous theory of $\mathbb{R}$. He found that *it is necessary to not use infinitesimals*, because there aren't any.

Consequently, mathematicians stopped using infinitesimals. (Physicists continued to use them occasionally.)

In 1960 Abraham Robinson finally found a way to make sense out of infinitesimals, using a "real line" different from Dedekind's. This idea was even tried in a calculus book in the 1970's. But it didn't catch on; it's too complicated. — Probably the simplest example of an ordered field with infinitesimals is the set of all rational functions in one variable with real coefficients, ordered by the asymptotic behavior as the variable goes to $+\infty$.

Galileo's Paradox

Galileo Galilei (1564 – 1642), astronomer, physicist, mathematician

Some numbers are squares:

$$1^2 = 1, \qquad 2^2 = 4, \qquad 3^2 = 9, \qquad \ldots$$

But most positive integers are *not* squares; thus **the squares are far fewer**:

1	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$
1			4					9					$\cdots$

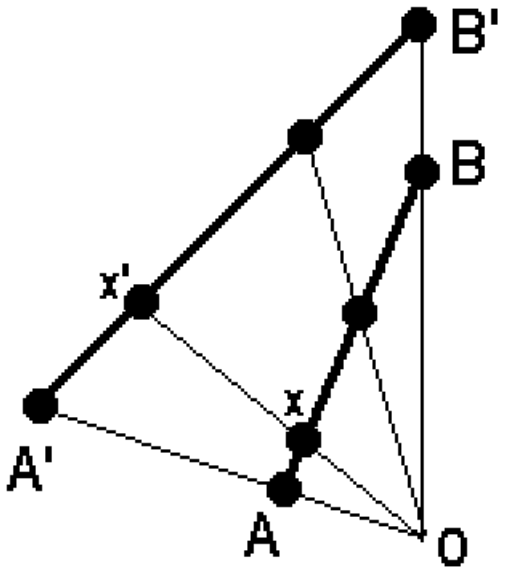
And yet, it seems that **the two sets have the** *same* **number of members** when we line them up this way:

1	2	3	4	5	6	7	$\cdots$
1	4	9	16	25	36	49	$\cdots$

(This is a *bijection* between the two sets of numbers.)

Paradoxes of geometry

Line segments with different lengths have the same number of points.

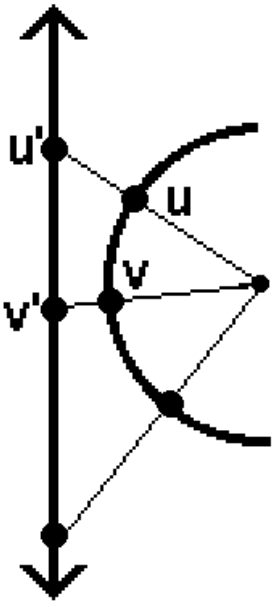


(This is a *bijection* between line segments AB and $A'B'$.)

A semicircle (with finite length)

and a whole line (with infinite length)

have the same number of points.



(This is a *bijection* between the line and the semicircle.)

Part of the confusion is just over our choice of words.

Who is bigger,

a man who is 6 feet tall and weighs 180 pounds,

or a man who is 5½ feet tall and weighs 220 pounds?

That depends on what "bigger" refers to -- height, weight, or something else.

We need more precise language.

We must distinguish between two different notions of "bigger": *subset* and *cardinality*.

Subsets:

Let S and T be sets.

We say S is a **subset** of T, written

$$S \subseteq T,$$

if every member of S is a member of T.

We say S is a **proper subset** of T, written

$$S \subsetneq T,$$

if moreover at least one member of T is not a member of S.

Example. $\{1, 4, 9, 16, \ldots\} \subsetneq \{1, 2, 3, 4, \ldots\}$. So in one sense, the set of positive integers is "bigger" than the set of squares.

Cardinality:

The **cardinality** of a set S is just "how many members the set has"; we will denote that by $|S|$. That's simple enough when the set is *finite*; for instance,

$$\Big|\{1, 3, 7, \pi\}\Big| \;=\; 4.$$

But it is difficult to define $|S|$ in a way that works for *all* sets. I won't do that today.

You might expect that "$|S| = |T|$" is even harder to define, but (surprisingly) it turns out to be fairly easy. We'll do that.

Let S and T be sets. Let $f : S \to T$ be a function from S to T — i.e., a rule assigning to each $s \in S$ some corresponding $f(s) \in T$.

f is **one-to-one** if $s_1 \neq s_2 \Rightarrow f(s_1) \neq f(s_2)$.

f is **onto** if each $t \in T$ is an $f(s)$.

f is a **bijection** if it is both one-to-one and onto. Such a function establishes a *matching* between members of S and members of T.

Two sets S, T are **equipollent**, or **have the same cardinality**, if there exists at least one bijection between them; then we write $|S| = |T|$.

Example. $\Big|\{1, 4, 9, 16, \ldots\}\Big| = \Big|\{1, 2, 3, 4, \ldots\}\Big|$. So in another sense, the set of positive integers is "the same size as" the set of squares.

Theorem. $|\mathbb{N}| = |\mathbb{Z}|$, where

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, 4, \ldots\} \\ \mathbb{Z} &= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \end{aligned}$$

Proof. Use this matching between the two sets:

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad \ldots$$

$$0 \quad 1 \quad -1 \quad 2 \quad -2 \quad 3 \quad -3 \quad 4 \quad -4 \quad \cdots$$

(Later I'll call this the "alternating signs technique." Note that the matching does not need to preserve the ordering.) □

Dedekind (1888)

A set is infinite if and only if it is equipollent with some proper subset of itself.

Next, some of Cantor's proofs.

Theorem. $|\mathbb{N}| = |\mathbb{N}^2|$, where

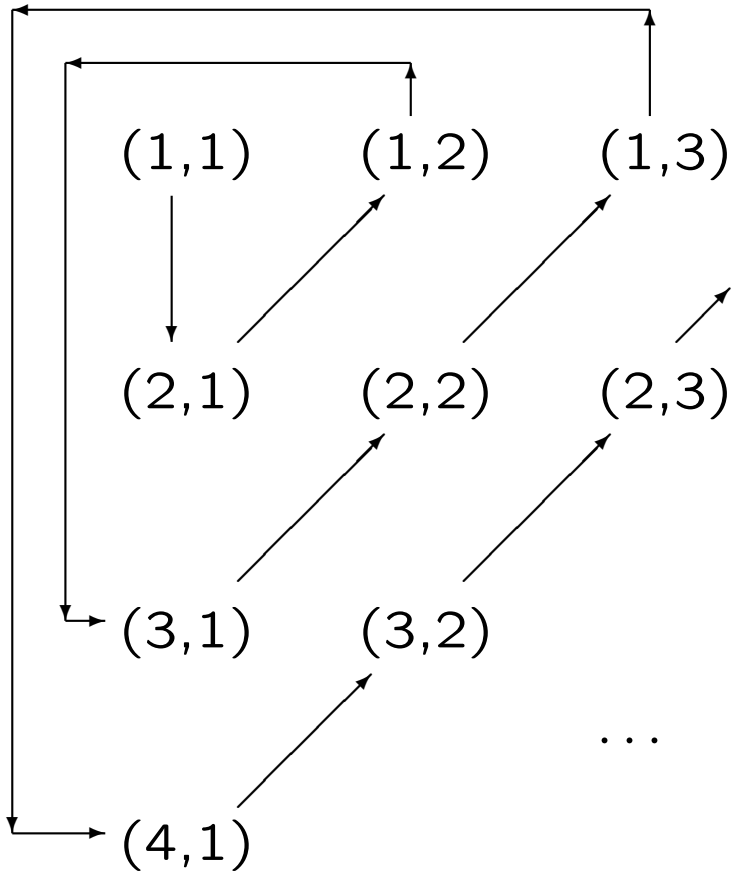
$$\mathbb{N}^2 = \{\text{ordered pairs of members of } \mathbb{N}\}.$$

Proof. First, make an array that includes all the ordered pairs of positive integers:

$$\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & \cdots \\
(2,1) & (2,2) & (2,3) & (2,4) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

And then ...

... make a path through all the pairs.



Following the path gives us a *sequence*:

1	2	3	4	5	6	···
(1,1)	(2,1)	(1,2)	(3,1)	(2,2)	(1,3)	···

hence our matching. □

Theorem. $|\mathbb{Q}| = |\mathbb{N}|$, where $\mathbb{Q} = \{\text{rationals}\}$.

Proof. First we prove it for *positive* rationals.

Start with the sequence from our last proof:

(1,1) (2,1) (1,2) (3,1) (2,2) (1,3) (4,1) (3,2) $\cdots$

Write each pair as a fraction:

$$\frac{1}{1} \quad \frac{2}{1} \quad \frac{1}{2} \quad \frac{3}{1} \quad \frac{2}{2} \quad \frac{1}{3} \quad \frac{4}{1} \quad \frac{3}{2} \quad \cdots$$

Delete any repetitions of earlier terms:

$$\frac{1}{1} \quad \frac{2}{1} \quad \frac{1}{2} \quad \frac{3}{1} \quad \frac{1}{3} \quad \frac{4}{1} \quad \frac{3}{2} \quad \cdots$$

Match with positive integers:

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad \cdots$$

Finally, to get *all* rational numbers, use the "alternating signs technique." $\square$

Some other countable sets

- Ordered triples of positive integers.
- Ordered quadruples of positive integers.
- The union of countably many countable sets. (Thus, for a set to be uncountable, it must be *much much bigger* than any countable set.)
- Finite sequences of positive integers.
- Finite sequences of letters and punctuation symbols.
- Paragraphs written in English.
- Descriptions of mathematical objects.
- Describable mathematical objects.

However, some sets of mathematical objects are uncountable. Hence **most mathematical objects are indescribable.** (But we work mostly with describable objects.)

For instance, we can describe 3, $\sqrt{17}$, and $\pi/2$, but most real numbers are indescribable.

Theorem. $|\mathbb{R}| > |\mathbb{N}|$, where $\mathbb{R} = \{\text{reals}\}$. That is, the reals are *uncountable*.

Proof. Since $(0,1) \subseteq \mathbb{R}$, it suffices to show that the interval $(0,1)$ is uncountable.

Assume (for contradiction) that $(0,1)$ is countable. Thus all the members of $(0,1)$ can be put into a *list*, something like this:

$$\begin{array}{lcccccccc} r_1 & = & 0 & . & 3 & 8 & 7 & 9 & \cdots \\ r_2 & = & 0 & . & 5 & 5 & 2 & 6 & \cdots \\ r_3 & = & 0 & . & 0 & 1 & 3 & 7 & \cdots \\ r_4 & = & 0 & . & 8 & 6 & 1 & 2 & \cdots \\ \vdots & & \vdots & & \vdots & \vdots & \vdots & \vdots & \end{array}$$

Put a box around the nth digit after the decimal point in r_n. Thus:

$$\begin{array}{lcccccccc} r_1 & = & 0 & . & \boxed{3} & 8 & 7 & 9 & \cdots \\ r_2 & = & 0 & . & 5 & \boxed{5} & 2 & 6 & \cdots \\ r_3 & = & 0 & . & 0 & 1 & \boxed{3} & 7 & \cdots \\ r_4 & = & 0 & . & 8 & 6 & 1 & \boxed{2} & \cdots \\ \vdots & & \vdots & & \vdots & \vdots & \vdots & \vdots & \end{array}$$

Use those boxed digits to make a number:

$$r = 0.3\,5\,3\,2\cdots$$

Now change all those digits, by this rule:

Replace any 5 with a 6. Replace any other digit with a 5.

(That yields no 0's or 9's, thus avoiding problems like $0.3849999\cdots = 0.385000\cdots$.)
Example:

$$\begin{array}{rrcccccccc} \text{diagonal \# is} & r & = & 0 & . & 3 & 5 & 3 & 2 & \cdots \\ & & & & & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{new \# is} & s & = & 0 & . & 5 & 6 & 5 & 5 & \cdots \end{array}$$

Now observe that

$$\begin{array}{ll} s \neq r_1 & \text{(different in 1st digit)} \\ s \neq r_2 & \text{(different in 2nd digit)} \\ s \neq r_3 & \text{(different in 3rd digit)} \end{array}$$

and so on. Thus $s \notin \{r_1, r_2, r_3, \ldots\}$, contradicting our assumption that the list contained *all* of $(0, 1)$. $\square$

Theorem. $|\mathbb{R}| = |\mathbb{R}^2| = |\mathbb{R}^3|$. That is, there are the same "number of points" in a line, a plane, or 3-dimensional space.

Sketch of the proof. We'll just prove $|\mathbb{R}| = |\mathbb{R}^2|$; the other proof is similar. We have to show how any real number corresponds to a pair of real numbers.

Here is a typical real number: $3701.3409536295\cdots$. Rewrite it this way:

3	7	0	1	.	3	4	0	9	5	3	6	2	9	5	$\cdots$
↓	↓	↓	↓		↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
3		0		.	3		0		5		6		9		$\cdots$
	7		1	.		4		9		3		2		5	$\cdots$

which yields the pair of numbers

$$\Big(30.30569\cdots, \quad 71.49325\cdots \Big)$$

This sketch glosses over a few technical details — e.g., minus signs, and pairs such as $0.38499999\cdots = 0.38500000\cdots$. □

For our next theorem, we'll need another definition. For any set S, the **powerset** of S is the set

$$\mathcal{P}(S) = \{\text{subsets of } S\}.$$

For instance, the set $\{1, 2, 3\}$ has these eight subsets:

$$\{\}, \{1\}, \{2\}, \{3\},$$

$$\{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}$$

and so it has this powerset:

$$\mathcal{P}\Big(\{1,2,3\}\Big) = \Big\{\{\}, \{1\}, \{2\}, \{3\},$$

$$\{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$$

Note that $8 = 2^3$. In fact, $|\mathcal{P}(S)| = 2^{|S|} > |S|$ for any finite set S; that's not hard to show.

Example: What are some subsets of $\mathbb{N}$?

Finite sets, such as $\{2, 3\}$ and $\{1, 6, 204\}$ and $\{1, 2, 3, \ldots, 999\}$. (There are only countably many of these.)

Cofinite sets (i.e., the complement is finite), such as {positive integers other than 2 or 3} and {positive integers other than 1, 6, 204}. (Countably many of these.)

Sets that are **neither finite nor cofinite** —

- Easily described ones, such as {even numbers} or {numbers whose names include an "n"}. (Countably many.)

- Ones that are harder to describe. (Countably many.)

- Ones that we can't describe. (Uncountably many, as we'll soon see.)

Theorem. $|\mathcal{P}(S)| > |S|$, for *every* set S.

Proof. Assume (for contradiction) that $|\mathcal{P}(S)| = |S|$ for some set S. Thus there is some bijection $f : S \to \mathcal{P}(S)$.

Whenever x is a *member* of S, then $f(x)$ is a *subset* of S. Let's say x is

self-membering if $x \in f(x)$,
non-self-membering if $x \notin f(x)$.

Let N be the collection of all the non-self-membering objects. That is,

$$N \quad = \quad \{x \in S \ : \ x \notin f(x)\}.$$

That's a subset of S.

So for each $x \in S$, we have

$$x \in N \quad \Leftrightarrow \quad x \notin f(x). \qquad (*)$$

Since f is bijective, there is some particular u such that $f(u) = N$.

Is u self-membering? It is if it isn't, and it isn't if it is! Indeed, (*) holds for *every* x. In particular, plug in $x = u$ and $N = f(u)$. We get this contradiction:

$$u \in N \quad \Leftrightarrow \quad u \notin N.$$

Corollary. There are infinitely many different infinities; for instance,

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \cdots$$

Two things Cantor *tried* to prove

The Schröder-Bernstein Theorem. If $|S| \leq |T|$ and $|T| \leq |S|$ then $|S| = |T|$.

That *looks obvious*, but only because our "$\leq$" notation is misleadingly suggestive. What the theorem *really* says is:

If there exists a bijection from S onto a subset of T,

and there exists a bijection from T onto a subset of S,

then there exists a bijection between S and T.

The proof of this is complicated, but still "elementary" in the sense that it doesn't require anything more advanced than what we've done. I'll show you the proof if time permits.

We've seen that $|\mathbb{N}| < |\mathbb{R}|$. Are there any cardinalities *between* those? Or is this true:

The Continuum Hypothesis (CH). There doesn't exist a set S satisfying $|\mathbb{N}| < |S| < |\mathbb{R}|$.

This was finally answered many years later, in a way that Cantor never would have imagined: It's *neither* provable *nor* disprovable!

> Kurt Gödel (1940) showed that adding CH to the usual axioms of set theory does not produce a contradiction.
>
> Paul Cohen (1960) showed that adding *not*-CH to the usual axioms of set theory does not produce a contradiction.

To answer the question we need more axioms!

More about Cantor

At first Cantor's ideas were not received well; they were simply too innovative. In particular, Kronecker (one of Cantor's teachers) opposed Cantor's ideas and blocked his career.

Cantor had mental illness during his last few years, probably aggravated (but not caused) by this poor reception and by his frustration over the Continuum Hypothesis.

Eventually Cantor's ideas won out and became part of mainstream mathematics. David Hilbert, the greatest mathematician of the early 20th century, said in 1926 that

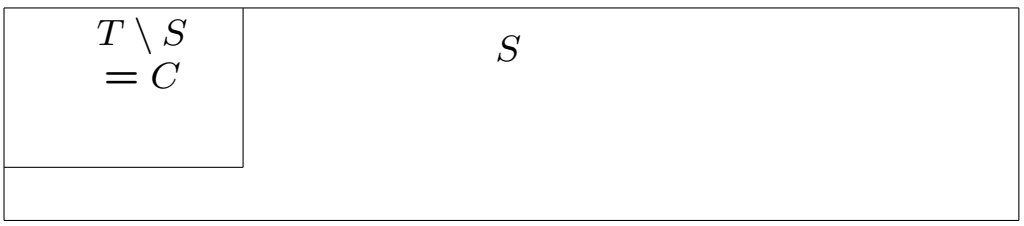
> "No one can expel us from the paradise Cantor has created."

Appendix: Proof of the Schröder-Bernstein Theorem.

Since there is a bijection between S and a subset of T, by relabelling everything we may actually assume that S **is** a subset of T; that will simplify our notation.

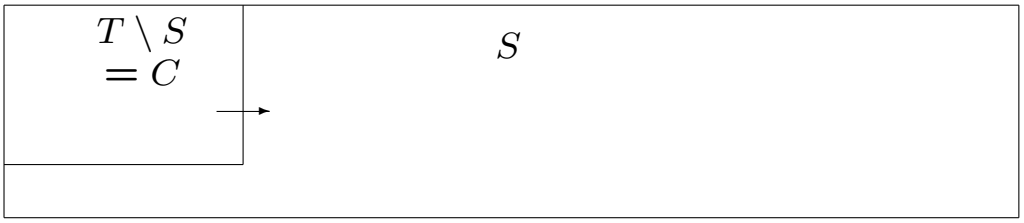
Thus, we assume that $S \subseteq T$. In the diagram below, T is the big box, and S is everything except the little box in the upper left corner. Let's call that little box "C"; thus $C = T \setminus S$.

We assume that we are given a one-to-one function $f : T \to S$. (We want to find a *bijection* between T and S.)



Since Range(f) $\subseteq S$, any points that are in $C = T \setminus S$ get mapped out of C by f. Moreover, anything in S gets mapped into S by f.

So the arrow represents a one-directional movement: Anything in the little box gets moved across the border, and anything in S gets mapped to somewhere in S.

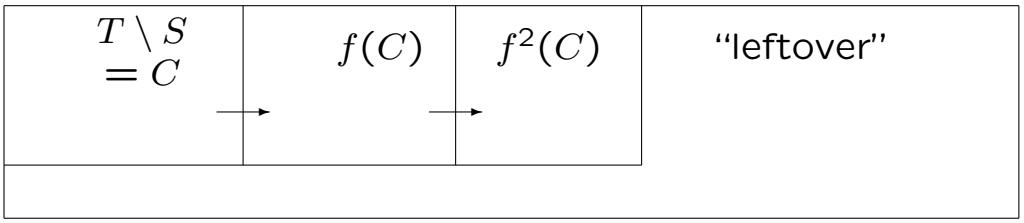


So C gets mapped to $f(C)$, which is a subset of S.

Since C and $f(C)$ are disjoint and f is one to one, $f(C)$ and $f^2(C)$ are also disjoint.

Also $f^2(C) \subseteq \text{Range}(f) \subseteq S$.

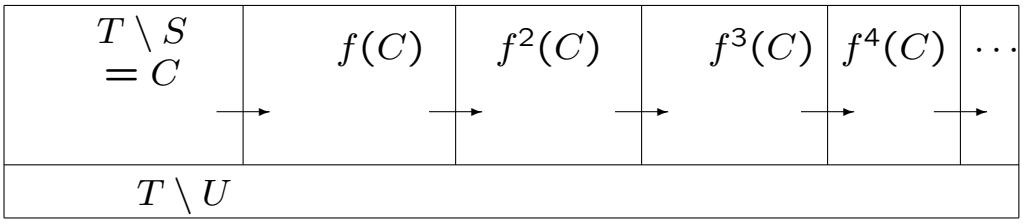
Anything in the "leftover" set gets mapped by f to somewhere in the "leftover" set.



This process continues. All the sets $C, f(C), f^2(C), f^3(C), f^4(C), \ldots$ are disjoint, and any point in any one of those sets gets mapped to the next of those sets by f. Let U be the union of all those sets.

Nothing gets mapped into C.

The "leftover" set now is just $T \setminus U$; anything in it gets mapped to somewhere in it by the function f.



Define a function $h : T \to S$ by taking

$$h(z) = \begin{cases} f(z) & \text{when } z \in U, \\ z & \text{when } z \in T \setminus U. \end{cases}$$

Then h is a bijection from T onto S. □