Cardinals*

Ana Sokolova

Department of Computer Sciences, University of Salzburg

anas@cs.uni-salzburg.at

January 9, 2021

The notions of cardinality and cardinals (also called cardinal numbers) are needed as a measure of the size of a set, in particular in order to be able to compare infinite sets.

Clearly, finite sets can be compared by simply counting their elements and so the notion of cardinality of a finite set can safely be defined as the number of elements. However, for infinite sets there is no number that we know of that could count the elements in a set. Therefore, we define an abstract notion of cardinality, and we will see later that on finite sets this notion amounts to the above mentioned possible definition via the number of elements in the set.

We start by defining an equivalence relation that relates sets.

Definition 1 (Equivalent sets, equal cardinality). *Let A and B be two sets. We say that A and B have the same cardinality, or are equivalent, and write $A \sim B$ or $|A| = |B|$ iff there exists a bijection $f\colon A \to B$.*

Proposition 1. *The relation $\sim$ is an equivalence relation on sets.*

Proof. $\sim$ is reflexive: For every set A, $id_A\colon A \to A$ is a bijection proving that $A \sim A$.

$\sim$ is symmetric: Let A, B be sets and assume $A \sim B$. This means, there is a bijection $f\colon A \to B$. But then $f^{-1}\colon B \to A$ is also a bijection, showing that $B \sim A$.

$\sim$ is transitive: Let A, B, C be sets and assume that $A \sim B$ and $B \sim C$. Hence there are bijections $f\colon A \to B$ and $g\colon B \to C$. Now, by Corollary 1 (page 8 in the lecture notes on Functions) $g \circ f\colon A \to C$ is a bijection too and hence $A \sim C$. □

This justifies saying that "A and B are equivalent sets" when $A \sim B$.

Definition 2 (Cardinality). *Given a set A, we write $|A|$ for the $\sim$-equivalence class*

$$\begin{aligned}[A]_\sim &= \{X \mid X \text{ is a set and } A \sim X\} \\ &= \{X \mid \text{ there exists a bijection } f\colon A \to X\}\end{aligned}$$

of A, and call it the cardinality of A.

Hence cardinalities, also called cardinals or cardinal numbers, are equivalence classes of the relation $\sim$ on sets!

* Notes from the lectures Formale Systeme on naive set theory. Many thanks to Luis Thiele for helping me with producing the notes.

1 Relations on Cardinals

Now that we know what cardinals are, we will define three relations ($\leq$ and $\geq$ and $<$) on cardinals and some operations.

These relations and operations are similar to known relations and operations on numbers and hence justify calling cardinals "cardinal numbers".

Definition 3. *The relation "$\leq$" is defined on cardinals by*

$$|A| \leq |B| \Leftrightarrow \textit{there exists an injection } f\colon A \to B$$

.

Definition 4. *The relation "$\geq$" is defined on cardinals by*

$$|A| \geq |B| \Leftrightarrow \textit{there exists an surjection } f\colon A \to B.$$

Definition 5. *The relation "$<$" is defined on cardinals by*

$$|A| < |B| \Leftrightarrow \textit{there exists an injection } f\colon A \to B \textit{ but no surjection } f\colon A \to B.$$

When $|A| \leq |B|$, we say, as expected, that the cardinality of A is less than or equal to the cardinality of B.

Similarly $|A| \geq |B|$ stands for the cardinality of A is larger than or equal to the cardinality of B.

Finally, if $|A| < |B|$ we say that the cardinality of A is less than the cardinality of B.

Since cardinals are equivalence classes, it is not obvious that these relations are well-defined. To prove that they are, we need to actually prove that the definitions are independent of the choice of representatives. We will do this for "$\leq$" and leave the proofs for the other relations as an exercise for the reader.

Lemma 1. *The relation $\leq$ on cardinals is well-defined, i.e., if A, B, C, D are sets such that $|A| = |C|$ and $|B| = |D|$ and $|A| \leq |B|$, then $|C| \leq |D|$.*

Note that this lemma guarantees that it does not matter which representative we choose: A or C vs. B or D, "$\leq$" is "stable on equivalence classes".

Proof. Let A, B, C, D be sets such that $A \sim C$ (i.e. $|A| = |C|$) and $B \sim D$ (i.e. $|B| = |D|$). This means there exists a bijection $f\colon A \to C$ and a bijection $g\colon B \to D$. Moreover, assume $|A| \leq |B|$, i.e., there exists an injection $i\colon A \to B$. We must prove $|C| \leq |D|$, i.e., we must prove that there exists an injection $j\colon C \to D$. We will construct such an injection j using the existing maps f, g and i. Let $j\colon C \to D$ be defined by:

$$j = \left(C \xrightarrow{f^{-1}} A \xrightarrow{i} B \xrightarrow{g} C \right),$$

i.e.,

$$j = g \circ i \circ f^{-1}.$$

Then since f and g are bijections, they are also injections, and hence by two application of Lemma 6 from the lecture notes on Functions, we get that j is injective. □

Even though the notation is very tempting, we have no reason yet to believe that, e.g.,

$$|A| \leq |B| \Leftrightarrow |A| < |B| \vee |A| = |B|$$

nor

$$|A| \geq |B| \Leftrightarrow |A| \leq |B|$$

These and other such properties do hold, but they require a proof. We will prove now the second one, to get an idea of what such proofs look like.

Lemma 2. *Let A and B be sets. Then $|A| \geq |B| \Leftrightarrow |B| \leq |A|$.*

Proof. Let $|A| \geq |B|$. This means that B is empty or there is a surjection $f\colon A \to B$. If B is empty, then there is a unique function which is an injection from B to A proving that $|B| \leq |A|$. Let B be non-empty and $f : A \to B$ a surjection. We now define a function $g\colon B \to A$ by

$$g(b) = a_b \quad \text{for a chosen element } a_b \in f^{-1}(\{b\}).$$

Since f is surjective, $f^{-1}(\{b\}) \neq \emptyset$ for all $b \in B$, so we can always choose such an a_b, i.e., g is well defined. Injectivity of g follows from f being a function: Assume $g(b_1) = g(b_2)$. This means $a_{b_1} = a_{b_2}$. But $a_{b_1} \in f^{-1}(\{b_1\})$, i.e., $f(a_{b_1}) = b_1$ whereas $a_{b_2} \in f^{-1}(\{b_2\})$, i.e., $f(a_{b_2}) = b_2$. Therefore, since f is a function and since $a_{b_1} = a_{b_2}$ we get $b_1 = f(a_{b_1}) = f(a_{b_2}) = b_2$. This proves that $\geq = \leq^{-1}$! □

The notation "$\leq$", "$\geq$", "$<$" suggests other things as well, namely, it suggests that these relations are partial/strict orders, respectively. This is also true.

Lemma 3. *The relation $\leq$ on cardinals is reflexive.*

Proof. The proof is immediate: We have $id_A\colon A \to A$ is a bijection and hence an injection. Therefore $|A| \leq |A|$. □

Lemma 4. *The relation $\leq$ on cardinals is transitive.*

Proof. Assume $|A| \leq |B|$, $|B| \leq |C|$. Then there is an injection $f\colon A \to B$ and an injection $g\colon B \to C$. From Lemma 6 in the lecture notes on functions, $g \circ f\colon A \to C$ is injective as well proving $|A| \leq |C|$. □

Antisymmetry of $\leq$ is a famous nontrivial result that we do not prove here, but state it in the following theorem.

Theorem 1 (Cantor-Schröder-Bernstein). *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Note that this statement actually says: "If there exists an injection $i_1\colon A \to B$ and there exists an injection $i_2\colon B \to A$, then there exists a bijection $b\colon A \to B$, for any sets A and B." If you are interested, I will gladly provide you a proof.

2 Operations on Cardinals

In this section we define and briefly discuss operations on cardinals.

Definition 6. *Let $|A|$ and $|B|$ be two cardinals with $A \cap B = \emptyset$. Then*

$$|A| + |B| \stackrel{def}{=} |A \cup B|.$$

Note that this defines an operation on all cardinals since if $|A|$, $|B|$ are such that $A \cap B \neq \emptyset$ we can always pick another representatives, say $\bar{A}$, $\bar{B}$ with $\bar{A} = \{(0, a) \mid a \in A\}$ and $\bar{B} = \{(1, b) \mid b \in B\}$ such that $|\bar{A}| = |A|$, $|\bar{B}| = |B|$ and $\bar{A} \cap \bar{B} = \emptyset$.

Also for this definition of addition on cardinals, one would have to prove that it is well defined. We will omit this tedious proof, but I want you to keep in mind that a proof is needed. We proceed with the definitions of two more operations on cardinals: multiplication and exponentiation.

Definition 7. *Let $|A|$ and $|B|$ be two cardinals. Then $|A| \circ |B| \stackrel{def}{=} |A \times B|$.*

Definition 8. *Let $|A|$ and $|B|$ be two cardinals. Then $|A|^{|B|} \stackrel{def}{=} |A^B|$ where $A^B = \{f \mid f \colon B \to A\}$ denotes the set of all functions from B to A.*

Proposition 2. *Let A be a set. Then $|\mathcal{P}(A)| = 2^{|A|}$ where $2 = |\{0, 1\}|$ denotes the cardinality of any 2-element set.*

We will give the full proof this property as it provides a nice example.

Proof. Note that, by the definition of exponent of cardinalities, we need to prove

$$|\mathcal{P}(A)| = |\{0, 1\}|^{|A|} = |\{0, 1\}^A| = |\{f \mid f \colon A \to \{0, 1\}\}|$$

Hence we need to show that there is a bijection $\Phi \colon \mathcal{P}(A) \to \{f \mid f \colon A \to \{0, 1\}\}$. We will show this by constructing a bijection Φ.

Let $X \subseteq A$, i.e., $X \in \mathcal{P}(A)$. We define $\Phi(X) = f_X$ where f_X (sometimes denoted by χ_X) is the so-called characteristic function of X, i.e., the function $f_X \colon A \to \{0, 1\}$ given by

$$f_X(x) = \begin{cases} 1, & x \in X \\ 0, & x \notin X \end{cases}$$

Note that this means $f_X(x) = 1 \stackrel{val}{=} x \in X$. We will prove that this Φ is bijective.

In order to prove injectivity, let $X_1, X_2 \subseteq A$ with $\Phi(X_1) = \Phi(X_2)$. Hence $f_{X_1} = f_{X_2}$. But then, for arbitrary $x \in A$,

$$\begin{aligned} x \in X_1 &\stackrel{val}{=} (f_{X_1}(x) = 1) \\ &\stackrel{val}{=} (f_{X_2}(x) = 1) \\ &\stackrel{val}{=} x \in X_2 \end{aligned}$$

and hence $X_1 = X_2$.

In order to prove surjectivity, let $f \colon A \to \{0, 1\}$ be a function. Let $X = f^{-1}(\{1\})$. Then $\Phi(X) = f$, since $f(x) = 1$ iff $x \in X$, which shows that $f = f_X$. □

3 Finite Sets, Finite Cardinals

We write $\mathbb{N}_k$ for the set $\{0, 1, ..., k-1\}$, hence $\mathbb{N}_0 = \emptyset$. We write k for $|\mathbb{N}_k|$.

Definition 9 (Finite set). *A set A is finite iff $|A| = k$ for some $k \in \mathbb{N}$.*

Hence, a set A is finite iff there is a natural number $k \in \mathbb{N}$ and a bijection $f\colon A \to \mathbb{N}_k$. It is easy to see that a set A is finite iff A has k elements for some $k \in \mathbb{N}$.

The following observation justifies calling cardinals "cardinal numbers": The operations on cardinals when restricted to finite cardinals coincide with the operations on natural numbers.

This means, if $|A| = k$ and $|B| = m$, then $|A| + |B| = k + m$. $|A| \cdot |B| = k \cdot m$. $|A|^{|B|} = k^m$, with "+", "$\cdot$", and the exponent on the right denoting the corresponding operation on $\mathbb{N}$.

4 Infinite, Countable and Uncountable Sets

We write $\aleph_0$, and read it "Aleph 0" for the cardinality of the set of natural numbers. Hence, $\aleph_0 = |\mathbb{N}|$.

The story about Hilbert's Hotel actually proves the following two lemmas, essential for understanding countable sets.

Lemma 5. $\aleph_0 + 1 = \aleph_0$.

Proof. Since $\aleph_0 = |\mathbb{N}|$ and $1 = \{*\}$ is such that $1 \cap \mathbb{N} = \emptyset$, it suffices to prove that $|\mathbb{N} \cup \{*\}| = |\mathbb{N} \cup 1| = |\mathbb{N}|$, i.e., to prove that $\mathbb{N} \cup \{*\} \sim \mathbb{N}$, i.e., to prove that there exists a bijection

$$f\colon \mathbb{N} \cup \{*\} \to \mathbb{N}.$$

We will construct such a bijection. We set: $f(*) = 0$ and $f(n) = n + 1$ (in analogy with Hilbert's hotel, when a new guest, modelled here by $*$, arrives)

We show that f is surjective: Let $n \in \mathbb{N}$ be arbitrary. If $n = 0$, then $n = f(*)$. If $n > 0$, then $n - 1 \in \mathbb{N}$ and $n = f(n-1)$. Hence $\forall n \in \mathbb{N}.\, \exists o \in \mathbb{N} \cup \{*\}.\, n = f(o)$.

We also show that f is injective: Let $o_1, o_2 \in \mathbb{N} \cup \{*\}$ be such that $f(o_1) = f(o_2)$. There are 4 cases to consider:

1. $o_1, o_2 \in \{*\}$, i.e., $o_1 = o_2 = *$. Then clearly $o_1 = o_2$.
2. $o_1 \in \{*\}, o_2 \in \mathbb{N}$. But then $f(o_1) = 0 \neq o_2 + 1 = f(o_2)$, hence this case is impossible under the assumption $f(o_1) = f(o_2)$.
3. $o_1 \in \mathbb{N}$, $o_2 \in \{*\}$. Symmetric to case 2., this case is also impossible.
4. $o_1, o_2 \in \mathbb{N}$. Then $f(o_1) = o_1 + 1$, $f(o_2) = o_2 + 1$ and hence $o_1 + 1 = o_2 + 1$ which implies $o_1 = o_2$.

□

Lemma 6. $\aleph_0 + \aleph_0 = \aleph_0$

Proof. Let $\bar{\mathbb{N}} = \{\bar{n} \mid n \in \mathbb{N}\}$. We first show that $|\bar{\mathbb{N}}| = |\mathbb{N}|$. We define $\bar{f}\colon \mathbb{N} \to \bar{\mathbb{N}}$ by $\bar{f}(n) = \bar{n}$ and show that it is bijective. Let $\bar{n} \in \bar{\mathbb{N}}$. Then $n \in \mathbb{N}$ and $\bar{n} = \bar{f}(n)$, showing

that $\bar{f}$ is surjective. Let $\bar{f}(n_1) = \bar{f}(n_2)$. Then $\bar{n}_1 = \bar{n}_2$, but this means $n_1 = n_2$ and proves that $\bar{f}$ is injective.

Since $|\mathbb{N} \cap \bar{\mathbb{N}}| = \emptyset$, it suffices to show that $|\mathbb{N} \cup \bar{\mathbb{N}}| = |\mathbb{N}|$ as then

$$|\mathbb{N} \cup \bar{\mathbb{N}}| \stackrel{\text{def}}{=} |\mathbb{N}| + |\bar{\mathbb{N}}|| = \aleph_0 + \aleph_0.$$

We show that there is a bijection $b\colon \mathbb{N} \cup \bar{\mathbb{N}} \to \mathbb{N}$ (this will mimic the part of the Hilbert's Hotel story when infinitely many new guests modelled by $\bar{\mathbb{N}}$ arrive).

Consider $b\colon \mathbb{N} \cup \bar{\mathbb{N}} \to \mathbb{N}$ defined by $b(n) = 2n$ for $n \in \mathbb{N}$ and $b(\bar{n}) = 2n + 1$ for $\bar{n} \in$
$bar\mathbb{N}$.

To see that b is surjective, take $m \in \mathbb{N}$. Then m is either odd or even, i.e., we have two cases to consider:

(1) m is even, i.e., $m = 2n$ for some $n \in \mathbb{N}$. Then $m = b(n)$.
(2) m is odd, i.e., $m = 2n + 1$ for some $n \in \mathbb{N}$. Then $m = b(\bar{n})$.

To see that b is injective, let $x_1, x_2 \in \mathbb{N} \cup \bar{\mathbb{N}}$ be such that $b(x_1) = b(x_2)$. We have four cases to consider:

(a) $x_1, x_2 \in \mathbb{N}$. Then $b(x_1) = 2x_1$, $b(x_2) = 2x_2$ and from $2x_1 = 2x_2$ we get $x_1 = x_2$.
(b) $x_1, x_2 \in \bar{\mathbb{N}}$. Then $x_1 = \bar{n}_1$, $x_2 = \bar{n}_2$ for $n_1, n_2 \in \mathbb{N}$ and $b(x_1) = 2n_1 + 1$, $b(x_2) = 2n_2 + 1$ so from $2n_1 + 1 = 2n_2 + 1$ we get $n_1 = n_2$, and hence $x_1 = x_2$.
(c) $x_1 \in \mathbb{N}$, $x_2 \in \bar{\mathbb{N}}$. But this case is impossible as $b(x_1)$ is even and $b(x_2)$ is odd, contradicting $b(x_1) = b(x_2)$.
(d) Similair like in case (c), the last case $x_1 \in \bar{\mathbb{N}}$, $x_2 \in \mathbb{N}$ is impossible too.

Hence b is injective. □

Definition 10 (Countable set). *A set A is countable (D. abzehlbar) iff $|A| = \aleph_0$.*

Clearly, $\mathbb{N}$ is countable by definition. This, together with two more interesting facts, is stated in the next proposition.

Proposition 3. *$\mathbb{N}$ is countable, $\mathbb{Z}$ is countable, and $\mathbb{Q}$ is countable.*

The proofs of these properties for $\mathbb{Z}$ and $\mathbb{Q}$ are nice but partly more involved, in particular for $\mathbb{Q}$. Do not let that scare you. I write them here for those of you who are interested to read or have a look. You can also read the proof(s sketches) in the book [LR].

Proof (for $\mathbb{Z}$). We have $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$ for $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$, $\mathbb{Z}^- = \{-k \mid k \in \mathbb{Z}^+\}$.

We show two things:

I. We first prove that $|\mathbb{Z}^+| = \aleph_0$, using that $f\colon \mathbb{N} \to \mathbb{Z}^+$ defined by $f(n) = n + 1$ is the needed bijection. The function f is surjective, as for $k \in \mathbb{Z}^+$, $k - 1 \in \mathbb{N}$ and $k = f(k - 1)$. The function f is injective as if $f(n_1) = f(n_2)$ for $n_1, n_2 \in \mathbb{N}$, then $n_1 + 1 = n_2 + 1$ and hence $n_1 = n_2$.

II. Next, we show that $|\mathbb{Z}^-| = |\mathbb{Z}^+|$ using that the function $g\colon \mathbb{Z}^- \to \mathbb{Z}^+$ given by $g(-k) = k$ is the needed bijection. The function g is surjective as for $k \in \mathbb{Z}^+$, $-k \in \mathbb{Z}^-$ and $k = g(-k)$. It is injective since if $g(-k_1) = g(-k_2)$, then $k_1 = k_2$ and so $-k_1 = -k_2$. This shows that $|\mathbb{Z}^-| = \aleph_0$ too.

The rest is a consequence of Lemma 5 and Lemma 6 related to Hilbert's Hotel:

$$\begin{aligned}
|\mathbb{Z}| &= |\mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+| \\
&= |\mathbb{Z}^-| + |\{0\}| + |\mathbb{Z}^+| \quad \{\text{ as the union is disjoint!}\} \\
&= \aleph_0 + 1 + \aleph_0 \\
&\overset{Lem.\ 5}{=} \aleph_0 + \aleph_0 \\
&\overset{Lem.\ 6}{=} \aleph_0
\end{aligned}$$

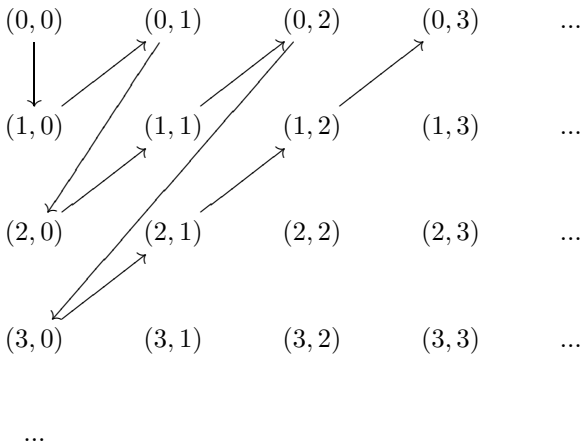
□

Proof ($\mathbb{Q}$ is countable). The proof proceeds in several stages.

(I) We prove $|\mathbb{N} \times \mathbb{N}| = \aleph_0$. Here we do just a sketch. Write $\mathbb{N}^2$ as an infinite matrix

$$\begin{array}{cccccc}
(0,0) & (0,1) & (0,2) & (0,3) & \ldots \\
(1,0) & (1,1) & (1,2) & (1,3) & \ldots \\
(2,0) & (2,1) & (2,2) & (2,3) & \ldots \\
(3,0) & (3,1) & (3,2) & (3,3) & \ldots \\
\ldots
\end{array}$$

We can now order the elements of $\mathbb{N}^2$ in one infinite sequence $(e_i \mid i \in \mathbb{N})$ by following the arrows:



$$\begin{array}{cccccccc}
(0,0) & (1,0) & (0,1) & (2,0) & (1,1) & (0,2) & (3,0) & \ldots \\
\| & \| & \| & \| & \| & \| & \| & \ldots \\
e_0 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & \ldots \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & \ldots
\end{array}$$

and we thus get a bijection $f\colon \mathbb{N} \to \mathbb{N}^2$ by $f(n) = e_n$.
The idea is that we visit $(0,0)$ first, then starting from $(1,0)$ all (m,n) with $m+n=1$, then starting from $(2,0)$ all (m,n) with $m+n=2$, etc. This function f provides the needed bijection. It is possible, but slightly tedious, to write an explicit formula for $f(n)$ or for $g(k,m)$ where $g\colon \mathbb{N}^2 \to \mathbb{N}$ is the inverse function, you may wish to do that as an exercise.

(II) We show $|\mathbb{Q}^+| \leq \aleph_0$ where $\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\}$. For this, using (I) it's enough to construct an injection $i\colon \mathbb{Q}^+ \to \mathbb{N}^2$. We define i by $i(\frac{m}{n}) = (m,n)$. Now, if $i(\frac{m}{n}) = i(\frac{k}{l})$, then $(m,n) = (k,l)$, i.e., $m = k$ and $n = l$ and hence $\frac{m}{n} = \frac{k}{l}$. (The function i is not a surjection, e.g. $(0,0)$ is not an image of anything in $\mathbb{Q}^+$ under i, but we don't care for that now.)

(III) We show $\aleph_0 \leq |\mathbb{Q}^+|$. This is easy, we need an injection from $\mathbb{N}$ to $\mathbb{Q}^+$ (or from any other countable set). We define $h\colon \mathbb{N} \to \mathbb{Q}^+$ by $h(n) = n+1$. This is well defined, as $n+1 \in \mathbb{Q}^+$, and injective.

(IV) $\aleph_0 = |\mathbb{Q}^+|$. This is a direct consequence of (II), (III) and the Cantor-Schröder-Bernstein theorem.

(V) $|\mathbb{Q}| = \aleph_0$. This holds since $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ and $|\mathbb{Q}^-| = |\mathbb{Q}^+| = \aleph_0$ as $b\colon \mathbb{Q}^+ \to \mathbb{Q}^-$ given by $b(x) = -x$ is a bijection (similar as for $\mathbb{Z}^+$, $\mathbb{Z}^-$). Moreover, the union above is disjoint. This shows

$$\begin{array}{rcl}
|\mathbb{Q}| = |\mathbb{Q}^+| + |\mathbb{Q}^-| + 1 & = & \aleph_0 + \aleph_0 + 1 \\
& \overset{Lem.\ 6}{=} & \aleph_0 + 1 \\
& \overset{Lem.\ 5}{=} & \aleph_0
\end{array}$$

and completes the proof. □

Definition 11 (Infinite set). *A set A is infinite iff $|A| \geq \aleph_0$.*

Clesrly, any countable set is infinite.

Definition 12 (Uncountble set). *A set A is uncountable (D. überabzehlbar) iff $|A| > \aleph_0$.*

Proposition 4. *$\mathbb{R}$ is uncountable.*

This is a very interesting property, whose proof also goes back to Cantor. The idea behind this proof is known as "the diagonalisation method" and is very useful in showing undecidability of problems, which is at the core of the theory of computation. We will prove this property in order to show you the diagonaisation method.

Proof. We will actually prove that the open interval

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

is uncountable. Since $(0,1) \subseteq \mathbb{R}$, we have $i\colon (0,1) \to \mathbb{R}$ defined by $i(x) = x$ is an injection and hence $|\mathbb{R}| \geq |(0,1)|$. So proving $|(0,1)| > \aleph_0$ shows $|\mathbb{R}| > \aleph_0$. Now, we first note that there is an injection from $\mathbb{N}$ to $(0,1)$. Namely, $f\colon \mathbb{N} \to (0,1)$ defined by $f(n) = \frac{1}{n+1}$ is: if $f(n_1) = f(n_2)$, then $\frac{1}{n_1+1} = \frac{1}{n_2+1}$ which implies $n_1 + 1 = n_2 + 1$ and this further that $n_1 = n_2$. We still need to show that there is no surjection $g\colon \mathbb{N} \to (0,1)$. This we do with a proof by contradiction, using the diagonalization idea.

Assume, towards a contradiction that there is a function $g\colon \mathbb{N} \to (0,1)$ that is surjective. At this point we need to recall that any number $x \in (0,1)$ has a decimal notation $x = 0, x_1x_2x_3...$ We consider now $g(0), g(1), ...$ in their decimal notation (D. Dezimaldarstellung)

$$\begin{aligned} g(0) &= 0, d_{00}d_{01}d_{02}... \\ g(1) &= 0, d_{10}d_{11}d_{12}... \\ g(2) &= 0, d_{20}d_{21}d_{22}... \\ &... \end{aligned}$$

and we construct $y \in (0,1)$ with $y = 0, y_0y_1y_2...$ where

$$y_i = \begin{cases} 0, & d_{ii} \neq 0 \\ 1, & d_{ii} = 0 \end{cases}$$

From our construction, we get $y \neq g(n)$ for any $n \in \mathbb{N}$ (as y differs from $g(n)$ in the n-th digit of the decimal representation, $y_n \neq d_{nn}$. Hence g is not surjective. This completes the proof. □

Definition 13. *We write c for the cardinality of $\mathbb{R}$, i.e. $c = |\mathbb{R}|$. Here, c stands for "continuum".*

One can prove, e.g. using Cantor-Schröder-Bernstein, that $c = 2^{\aleph_0}$ (you can find such a proof on the web). Note that we refer to the Theorem by Cantor-Schröder-Bernstein sometimes as "the big theorem of Cantor". The following simpler property is known as "the small theorem of Cantor" but it has an interesting consequence as we discuss below.

Theorem 2 (small Cantor theorem). *Let A be any set. Then $|A| < |\mathcal{P}(A)|$, i.e., $|A| < 2^{|A|}$.*

Corollary 1. *Cardinals are unbounded, i.e., for any cardinal $|A|$ we can construct an infinite ascending chain of cardinals:*

$$|A| < |\mathcal{P}(A)| < |\mathcal{P}(\mathcal{P}(A))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))| < ...$$

Corollary 2. $\aleph_0 < c$.

This last corollary is a consequence of $2^{\aleph_0} = c$.

Let us prove the small Cantor theorem. The proof is very short but very cute, with a taste of set-theory paradoxes.

Proof (small Cantor theorem). We need to show that there exists an injection $i\colon A \to \mathcal{P}(A)$ but no surjection. It is easy to construct i, just define $i(a) = \{a\}$. This is injective and shows $|A| \leq |\mathcal{P}(A)|$. We prove that there is no surjection, by contradiction. Asume, towards a contradiction, that there is a surjection $g\colon A \to \mathcal{P}(A)$. Consider the set

$$B = \{x \in A \mid x \notin g(x)\}$$

Clearly $B \subseteq A$, so $B \in \mathcal{P}(A)$. There are two possibilities for a, namely: (1) $a \in B$; and (2) $a \notin B$. We will show that both of these lead to contradiction. If $a \in B$, then $a \notin g(a) = B$, which is a contradiction. If $a \notin B$, then $a \in g(a) = B$, again a contradiction. Hence our assumption can not hold, i.e., there is no such surjection $g\colon A \to \mathcal{P}(A)$. □