$|A| = |B| \Leftrightarrow \exists_f : A \hookrightarrow\!\!\!\rightarrow B$ existe um f bijetivo que transforma A em B

$|\mathbb{N}| \neq |[0,1]|$

A CRASH COURSE ON TRANSFINITE CARDINALS

JOÃO ARAÚJO

1. Preliminaries

The cardinal of a set is the number of elements. For example, the set $\{a, b, c\}$ has cardinality 3. How do we know this? We stored in memory a set for each size, namely $\{\}$, $\{1\}$,$\{1, 2\}$, $\{1, 2, 3\}$, $\{1, 2, 3, 4\}$, etc., and we know that the symbol assigned to the size of each one of them is 0, 1, 2, 3, 4, etc. Then, when we want to find the size of a new set, say $\{a, b, c\}$, we *count* the elements, that is, we find a correspondence between the elements in this set and the elements in a set whose size we know: *we point to a and say (or count) 1; then point to b and say 2; then point to c and say 3. The set has 3 elements!*

More formally, we have the list of sets $\{\}$, $\{1\}$,$\{1, 2\}$, $\{1, 2, 3\}$, $\{1, 2, 3, 4\}$, etc.; when we want to find the cardinal of a new set, say $\{a, b, c\}$, we search a set S in the previous list such that there exists a bijection $f : S \to \{a, b, c\}$. The only solution to this problem is $S = \{1, 2, 3\}$ and we name the size of this set 3, thus we conclude that the set $\{a, b, c\}$ also has 3 elements.

This idea suggests the following definition.

Definition 1.1. In the class of all sets define the following relation: for any sets A and B,

$$A\, \mathcal{C} B \text{ iff there exists a bijection } f : A \to B.$$

If there is a bijection $f : A \to B$ then the sets A and B are said to be *equipotent* (*equipotentes*, in Portuguese). Therefore we can define the previous relation as follows:

$$A\, \mathcal{C} B \text{ iff } A \text{ and } B \text{ are equipotent.}$$

This relation $\mathcal{C}$ is in fact an equivalence relation as shown in the next result.

Proposition 1.2. *The relation $\mathcal{C}$ is reflexive, symmetric and transitive and hence is an equivalence relation.*

Proof. Regarding reflexivity, is it that $A\, \mathcal{C} A$? Clearly, the identity $\iota : A \to A$, defined by $x\iota = x$, is a bijection; thus $A\, \mathcal{C} A$ and the relation is reflexive.

Regarding symmetry, if $A\, \mathcal{C} B$, is it true that $B\, \mathcal{C} A$? Clearly if $f : A \to B$ is a bijection, then the inverse of f, $f^{-1} : B \to A$, is also a bijection. It is proved that $A\, \mathcal{C} B$ implies $B\, \mathcal{C} A$.

Regarding transitivity, if $A\, \mathcal{C} B$ and $B\, \mathcal{C} C$, is it true that $A\, \mathcal{C} C$? Clearly if $f : A \to B$ is a bijection and $g : B \to C$ is a bijection, then $f \circ g : A \to C$ is a bijection. It is proved that $A\, \mathcal{C} B$ and $B\, \mathcal{C} C$ implies $A\, \mathcal{C} C$. The result follows. □

As $\mathcal{C}$ is an equivalence relation, then it induces a partition $\mathcal{P} = \{P_1, P_2, P_3, \ldots\}$. For example, the part that contains the set $\{1, 2, 3\}$ is

$$\{\{1, 2, 3\}, \{2, 3, 4\}, \{a, b, c\}, \{Ariclene, Francisco, Iren\}, \ldots\},$$

the class that contais all sets A equipotent to $\{1, 2, 3\}$ (or, as we usually say, *the class that contains all the sets of size 3*). Therefore, counting the number of elements of a set A, that is, finding the cardinality of A, boils down to discover to which part P_1, $P_2, \ldots,$ does A belong.

So we introduce the following notation: the part P that contains the set A will be denoted by $|A|$. Therefore, $|\{1, 2, 3\}| = |\{2, 3, 4\}| = |\{a, b, c\}| = |\{\text{Clara, Diogo,Sahil}\}|$, etc. And with this notation we have $P = \{|\{\}|, |\{1\}|, |\{1, 2\}|, |\{1, 2, 3\}|, \ldots\}$.

Now we have a question: with this notation, what does it mean $|\mathbb{N}|$? By definition, $|\mathbb{N}|$ is the class of all sets having the same cardinality as $\mathbb{N}$. For example, the set of even numbers $2\mathbb{N}$ has the same cardinality as $\mathbb{N}$ as the following result shows.

Theorem 1.3. $|\mathbb{N}| = |2\mathbb{N}|$.

Proof. We have to show there is a bijection between those two sets. Clearly, $f : \mathbb{N} \to 2\mathbb{N}$, defined by $nf = 2n$, is a bijection. In fact, if $nf = mf$ then $2n = 2m$ and hence $n = m$, so that f is injective.

Regarding surjectivity, given an even number, say $2k$, then there exists a natural number, namely k, such that $kf = 2k$. Thus f is surjective.

It is proved that f is injective and surjective, so f is bijective, and hence $|\mathbb{N}| = |2\mathbb{N}|$. □

Now the student pauses a moment and thinks: *big deal,* $\mathbb{N}$ *and* $2\mathbb{N}$ *are both infinite, so no wonder their cardinalities are equal, namely, infinity; is it for these trivialities that I enrolled in this course?*

No, you enrolled for wonders like the following.

Theorem 1.4. *(Cantor, The Great)*

$|X| \neq |\wp(X)|$

$$|\mathbb{N}| \neq |\mathbb{R}|\,.$$

As you see, both sets have infinite cardinalities, but nevertheless the cardinalities are different!

Before proving that result we prove the following lemma.

Lemma 1.5. *There is no surjection* $f : \mathbb{N} \to]0,1[$ *and hence*

$$|\mathbb{N}| \neq |]0,1[|\,.$$

Proof. To prove the theorem we need to show that there are no bijections $f : \mathbb{N} \to]0,1[$. If there are no surjections, then there are no bijections. Thus we only need to prove that no function $f : \mathbb{N} \to]0,1[$ is surjective. Observe that a function $f : \mathbb{N} \to]0,1[$ is for example

$$\begin{array}{lcl}
1f & = & 0,122324\ldots \in\ ]0,1[\\
2f & = & 0,765231\ldots \in\ ]0,1[\\
3f & = & 0,089738\ldots \in\ ]0,1[\\
\ldots & &
\end{array}$$

More generally, the following table represents all possible functions $f : \mathbb{N} \to]0,1[$:

$$\begin{array}{lclcccccc}
1f & = & 0, & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & \ldots \\
2f & = & 0, & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & \ldots \\
3f & = & 0, & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & \ldots \\
4f & = & 0, & a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & \ldots \\
\ldots & & & & & & &
\end{array}$$

where $a_{i,j} \in \{0,1,2,\ldots,9\}$. So this is the question: is one of these functions surjective? The answer is no because we can always find an element $a \in\ ]0,1[$ such that $nf \neq a$, for all natural n. For instance, let

$$a = b_1 b_2 b_3 b_4 \ldots,$$

where $b_i \in \{1,2,3,\ldots,8\} \setminus \{a_{i,i}\}$.

For example, if we have, as above, $1f = 0,122324\ldots$, $2f = 0,765231\ldots$, $3f = 0,089738\ldots$, etc., then $a_{1,1} = 1$, $a_{2,2} = 6$, $a_{3,3} = 9$, etc., and hence $b_1 \in \{1,2,3,\ldots,8\} \setminus \{1\}$, say $b_1 = 2$; $b_2 \in \{1,2,3,\ldots,8\} \setminus \{6\}$, say $b_2 = 1$; $b_3 \in \{1,2,3,\ldots,8\} \setminus \{9\}$, say $b_3 = 8$, etc; thus

$$a = 0, b_1 b_2 b_3 \ldots = 0,218\ldots$$

Is there any natural n such that $nf = a$? Compare for example $1f$ and a:

$$\begin{array}{lclcccccc}
1f & = & 0, & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & \ldots \\
a & = & 0, & b_1 & b_2 & b_3 & b_4 & \ldots \\
\ldots & & & & & & &
\end{array}$$

For sure, the two numbers differ on the first decimal digit because $b_1 \in \{1,2,3,\ldots,8\} \setminus \{a_{1,1}\}$. So $1f \neq a$. Maybe we were unlucky; let us try, for example, $4f$:

$$\begin{array}{lclcccccc}
4f & = & 0, & a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & \ldots \\
a & = & 0, & b_1 & b_2 & b_3 & b_4 & \ldots \\
\ldots & & & & & & &
\end{array}$$

For sure, the two numbers differ on the fourth decimal digit because $b_4 \in \{1,2,3,\ldots,8\} \setminus \{a_{4,4}\}$. So $4f \neq a$.

In general,

$$\begin{array}{lclllllll} nf & = & 0, & a_{n,1} & a_{n,2} & \dots & a_{n,n} & \dots \\ a & = & 0, & b_1 & b_2 & \dots & b_n & \dots \\ \dots & & & & & & & \end{array}$$

For sure, the two numbers differ on the nth decimal digit because $b_n \in \{1, 2, 3, \dots, 8\} \setminus \{a_{n,n}\}$. So $nf \neq a$. As n was generic, it follows that f is not surjective because there is no natural number n such that $nf = a$.

As f was also a generic function, it follows that no function $f : \mathbb{N} \to]0, 1[$ is surjective. If there is no surjection, there is no bijection and hence $\mathbb{N}$ and $]0, 1[$ are not equipotent, thus they belong to different $\mathcal{C}$-parts, that is, $|\mathbb{N}| \neq |]0, 1[|$. The theorem is proved. □

Now we can prove Theorem 1.4:

Proof. The idea of the proof is easy: if there is no surjection $f : \mathbb{N} \to]0, 1[$, there can be no surjection to $\mathbb{R}$, a set that contains $]0, 1[$.

We will prove by contradiction. Suppose there is a surjection $f : \mathbb{N} \to \mathbb{R}$. It is obvious there is a surjection $g : \mathbb{R} \to]0, 1[$ defined by $xg = x$, for all $x \in]0, 1[$, and $xg = 1/2$, for all other real numbers. Now $fg : \mathbb{N} \to]0, 1[$ is the composition of two surjections and hence is a surjection. This contradicts the previous lemma. □

This result provides a better picture of our old class P:

$$P = \{|\{\}|, |\{1\}|, |\{1, 2\}|, |\{1, 2, 3\}|, \dots, |\mathbb{N}|, |\mathbb{R}|\}.$$

We have proved that there are infinite sets that have different cardinalities. But the surprises will not stop here!

2. The partial ordered set of cardinalities

Suppose we have a partition $Q = \{Q_1, Q_2, Q_3\}$, where $Q_1 = \{\{1\}, \{5\}, \{a\}\}$, $Q_2 = \{\{1, 2\}, \{1, 5\}, \{1, a\}\}$, $Q_3 = \{\{1, 2, 5\}, \{1, 5, a\}\}$.

Now in Q we define the relation: for $A, B \in Q$,

$$A \leq B \text{ iff there exists a set } C \in A \text{ such that } C \subset D, \text{ for all } D \in B.$$

Is this relation a partial order in Q?

Regarding reflexivity, is it true that $A \leq A$? We have to check if there exists a set $C \in A$ that is contained in every $D \in A$. But this is not true; for example, when $A = Q_1$, no element in Q_1 is contained in all other elements of Q_1: $\{1\}$ is neither contained in $\{5\}$ nor in $\{a\}$; etc. So this relation is not reflexive and hence it is not a partial order.

Similarly, we can define a relation on the partition $P = \{|\{\}|, |\{1\}|, |\{1, 2\}|, |\{1, 2, 3\}|, \dots, |\mathbb{N}|, |\mathbb{R}|\}$ as follows: for $|A|, |B| \in P$,

$$|A| \leq |B| \text{ iff there exists an injective function } f : A \to B.$$

For example, there is an injective function $f : \{1\} \to \{1, 2\}$ and hence we get the amazing conclusion (joking here) that $|\{1\}| \leq |\{1, 2\}|$.

Before proving that $(P, \leq)$ is a partial ordered set we introduce a result which has a funny story.

Theorem 2.1. *(Cantor-Schröder-Bernstein). Let A and B be two sets. If there exists to injections $f : A \to B$ and $g : B \to A$, then there exists a bijection $h : A \to B$.*

We are not going to prove this result as the proof is a bit more complicated than the easy proofs we want in this crash course. The funny story is that Cantor announced the theorem, but never provided a proof; Schröder then claimed to have a proof, but it was shown the proof was wrong; finally, Bernstein, a 19 years old student, found a correct proof.

Now we turn to our next result.

Theorem 2.2. *$(P, \leq)$ is a partially ordered set.*

Proof. Let $|A| \in P$. Is it true that $|A| \leq |A|$? This is equivalent to ask if there is an injective function $f : A \to A$, but the answer is obvious: the identity function is injective. Thus $\leq$ is reflexive.

Let $|A|, |B|, |C| \in P$ such that $|A| \leq |B| \leq |C|$. Is it true that $|A| \leq |C|$? By definition, $|A| \leq |B|$ means that there exists an injection $f : A \to B$; similarly $|B| \leq |C|$ means that there exists an injection $g : B \to C$. Therefore $f \circ g : A \to C$ is injective and hence $|A| \leq |C|$. It is proved that $\leq$ is transitive.

Let $|A|, |B| \in P$ such that $|A| \leq |B|$ and $|B| \leq |A|$. Then, by definition, there exist two injective functions $f : A \to B$ and $g : B \to A$. Thus, by the Cantor-Schröder-Bernstein Theorem, there exists a bijection $h : A \to B$; therefore A and B are equipotent sets, that is, $|A| = |B|$. It is proved that $\leq$ is anti-symmetric.

So the relation $\leq$ is reflexive, anti-symmetric and transitive.

It remains only a small technical detail to sort out. It is necessary to show that $\leq$ is a well defined relation, that is, if $|A| = |A_1|$, $|B| = |B_1|$ and $|A| \leq |B|$, then $|A_1| \leq |B_1|$. But this is easy to prove. $|A| = |A_1|$ means that there exists a bijection $f : A \to A_1$; similarly, $|B| = |B_1|$ means that there exists a bijection $g : B \to B_1$; finally, $|A| \leq |B|$ means that there exists an injective map $f_1 : A \to B$. Therefore, $f^{-1} \circ f_1 \circ g : A_1 \to B_1$ is the composition of three injections and hence is an injection. Thus $|A_1| \leq |B_1|$. The result follows. □

When there is an injection $f : A \to B$, but $|A| \neq |B|$, then we write $|A| < |B|$. For example, there is an injection $\iota : \mathbb{N} \to \mathbb{R}$, namely $n\iota = n \in \mathbb{R}$, and hence $|\mathbb{N}| \leq |\mathbb{R}|$. But we already proved that $|\mathbb{N}| \neq |\mathbb{R}|$; thus we really have $|\mathbb{N}| < |\mathbb{R}|$.

Are there more infinite sets A and B such that $|A| < |B|$? Yes, that is another result proved by Cantor. Recall that the power set of X is the set of all its subsets (*conjunto das partes* in Portuguese), and is denoted by $\mathcal{P}(X)$. For example, if $X = \{1, 2\}$, then $\mathcal{P}(X) = \{\{\}, \{1\}, \{2\}, \{1, 2\}\}$. Note that a map $f : X \to \mathcal{P}(X)$ is something like $1f = \{2\}$ and $2f = \{1, 2\}$; or $g : X \to \mathcal{P}(X)$ with $1g = \{2\}$ and $2g = \{\}$. Observe now that in some cases $x \in xf$ and in some other cases $x \notin xf$. For example, $2 \in 2f = \{1, 2\}$, but $1 \notin 1f = \{2\}$. In the case of g, $1 \notin 1g$ and $2 \notin 2g$.

Theorem 2.3. *Let X be a set. Then*

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

Proof. (If X is finite, then $|X| = n$ implies $|\mathcal{P}(X)| = 2^n$, and it is easy to prove by induction that $2^n > n$. But here we want to prove the result in general, for the case when X is finite or infinite.)

We have to prove that there is an injective function $f : X \to \mathcal{P}(X)$ (easy, $xf = \{x\}$), but there is no bijection $g : X \to \mathcal{P}(X)$. As before, we are going to prove that there is no surjection from X to $\mathcal{P}(X)$. We will argue by contradiction.

Suppose $h : X \to \mathcal{P}(X)$ is surjective. Let

$$S := \{x \in X \mid x \notin xh\} \in \mathcal{P}(X).$$

As h is surjective, it follows that there is $x \in X$ such that $xh = S$. Now, $x \in S = xh$ implies that $x \in xh$ and hence $x \notin S$, a contradiction. So the only option left is that $x \notin S = xh$. But if $x \notin xh$, then $x \in S$ (by definition of S); again a contradiction.

The contradiction comes from the assumption that there is a surjection $h : X \to \mathcal{P}(X)$. The theorem is proved. □

So now we have a better picture of our old partition:

$$P = \{|\{\}|, |\{1\}|, |\{1, 2\}|, |\{1, 2, 3\}|, \ldots, |\mathbb{N}|, |\mathcal{P}(\mathbb{N})|, |\mathcal{P}(\mathcal{P}(\mathbb{N}))|, |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|, \ldots\}.$$

In particular this implies that there is no such a thing as the *largest* set; as big as X might be, we know that $\mathcal{P}(X)$ will be bigger.

3. Curiosities

3.1. **Transfinite cardinals.** For finite sets there is a *canonical* sequence of sets of each cardinality, say $\{\}$, $\{0\}$, $\{0, 1\}$, $\{0, 1, 2\}$, etc., and the corresponding cardinalities are represented by the symbols 0, 1, 2, 3, etc., respectively.

The same happens for infinite sets; for each cardinality there is a canonical set and the corresponding cardinalities are represented by symbols representing these *transfinite cardinalities*; for that we use the letters of the Hebraic alphabet whose first is $\aleph$ (read *aleph*); the smallest infinite is denoted by $\aleph_0$, the next one is $\aleph_1$, etc., but the symbology gets much more complicated. The set of natural numbers is the smallest infinite set and hence $|\mathbb{N}| = \aleph_0$.

3.2. **Is it possible to have a transfinite cardinal smaller than $|\mathbb{N}|$?** No, it is not. The cardinality of any set X contained in $\mathbb{N}$ either is finite or $\aleph_0$.

3.3. **Arithmetic.** There are rules of arithmetics for transfinite cardinals. For example, $\aleph_0 + \aleph_0 = \aleph_0$, $\aleph_1 + \aleph_0 = \aleph_1$, $\aleph_0 + 2020^{2020} = \aleph_0$, etc. There are rules also for the multiplication and for exponentiation. For example, $\aleph_0^2 = \aleph_0$ and $2^{\aleph_0} > \aleph_0$.

Let a and b be transfinite numbers and A, B two disjoint sets such that $|A| = a$, $|B| = b$. Then $a + b$ is $|A \cup B|$, $a \times b = |A \times B|$ and a^b is $|\{f : B \to A \mid f \text{ is a function}\}|$. In particular,

$$2^{\aleph_0} = |\{f : \mathbb{N} \to \{1, 2\} \mid f \text{ is a function}\}|.$$

3.4. **Is it possible to have an infinite strictly between $\aleph_0$ and $\aleph_1$?** No. It is not possible.

3.5. **Is $|\mathcal{P}(\mathbb{N})| = \aleph_1$?** This is a natural question. If $\aleph_0 < \aleph_1$ and $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$, is it true that $|\mathcal{P}(\mathbb{N})| = \aleph_1$?

It is known that $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. The sentence *there is no set X such that* $|\mathbb{N}| < |X| < |\mathbb{R}|$ is known as the *continuum hypothesis (CH).* Cantor tried to prove it, but failed. In 1940 it was proved that the CH cannot be disproved; and in 1964 it was proved that the CH cannot be proved. This means that we can start two different mathematics: one that assumes CH and another one that does not.

3.6. **What is the factorial of $\aleph_0$?** It is the number of bijections $f : \mathbb{N} \to \mathbb{N}$. It is possible to prove that

$$\aleph_0! = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = 2^{\aleph_0}.$$

3.7. **The Fundamental Theorem of Arithmetics.** This theorem is very important to prove many theorems in the context of this module. Therefore I state it here without complete proof.

Theorem 3.1. *Let $n > 1$ be a natural number. Then:*

(1) *n can be written as a product of primes;*
(2) *if the primes are ordered $p_1, p_2, p_3, \dots$, then there is one and only one way of writing n in the form:*

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots,$$

where $a_i \geq 0$.

The first claim of the theorem is easy to prove using an argument that appears everywhere in mathematics: let n be a natural number; if n is prime, the result follows. If n is not prime, then it has two proper divisors, say $n = ab$. We can repeat this argument finitely many times until all the factors appearing in the decomposition of n are prime.

Complete and easy proofs of the theorem can be found all over the internet.

(Araújo) Departamento de Matemática, Centro de Matemática e Aplicações (CMA), Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, 2829–516 Caparica, Portugal, and CEMAT-CIÊNCIAS Universidade de Lisboa, Portugal

Email address: jj.araujo@fct.unl.pt