MA532 Lecture

Timothy Kohl

Boston University

March 31, 2020

Cardinality of Sets

We have an intuitive notion of what one means by the 'size' of a set. In particular there is an obvious distinction between finite sets like $\{1, 2, 3\}$ and infinite sets, the prototype example being $\omega = \{0, 1, 2, 3, \dots\}$.

Moreover, the step-wise building of ω via the successor function, starting from the empty set (which has zero elements) is the basis for our formal definition of what it means for a set to be finite.

Definition

A set X is finite if there exists a one-to-one function $f : X \to n$ for some natural number n.

Note that if there exists and injection $f : X \to n$ then there exists an injection $\tilde{f} : X \to n^+$ since if $f(x) \in n$ for each $x \in X$ then $f(x) \in n^+$ since $n \subseteq n^+$ obviously. (i.e. $\tilde{f}(x) = f(x)$ for each $x \in X$ where the codomain is now n^+)

e.g. $f : \{a, b, c\} \to \{0, 1, 2, 3, 4\}$ given by $a \mapsto 0$, $b \mapsto 1$,$c \mapsto 2$ is injective, as is $\tilde{f} : \{a, b, c\} \to \{0, 1, 2, 3, 4, 5\}$ given by $a \mapsto 0$, $b \mapsto 1$,$c \mapsto 2$ as well.

(i.e. the prescence of the extra element '5' in the co-domain does not 'disturb' the injectivity)

For precisely quantifying finiteness, we need to consider the *least* n for which there is a bijection from X to n.

Definition

We say that a set X has n elements, or has cardinality n, denoted $|X| = n$ if there exists an injection $f : X \to n$ but there does not exist an injection from X to any m such that $m < n$.

i.e. It's clear that there is an injection $X = \{x, y, z\} \to \{0, 1, 2\} = \mathbf{3}$, for example, $x \mapsto 0$, $y \mapsto 1$,$z \mapsto 2$, but that there is no injection $X = \{x, y, z\} \to \{0, 1\} = \mathbf{2}$ because at least two elements of X would have to map to the same element of $\{0, 1\}$.

Theorem

If $|X| = n$ then any one-to-one function $f : X \to n$ is onto. (surjective)

Before we examine the proof, we point out that this is a fundamental result which one uses commonly throughout mathematics, for example, in linear algebra if V and W are vector spaces where $dim(V) = dim(W) = n$ and $T : V \to W$ is a linear transformation, if T is 1-1 then T is onto.

Proof.

For $|X| = 0$ it's trivially true since any function $X \to 0 = \emptyset$ is onto.

If $f : X \to n$ is 1-1 but not onto, there exists $t \in n$ such that $\{x \in X \mid f(x) = t\}$ is empty.

Since $n > 0$ there exists m such that $m^+ = n$ and we may define a function $g : n - \{t\} \to m$ by

$$g(x) = \begin{cases} x & \text{if } x < t \\ x^+ & \text{if } x \geq t \end{cases}$$

and this function is one-to-one.
(e.g. $\{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5, 6\} - \{4\}$ where $1 \mapsto 1$, $2 \mapsto 2$, $3 \mapsto 3$, $4 \mapsto 4^+ = 5$ and $5 \mapsto 5^+ = 6$) Moreover, since $f(x) \neq t$ for any $x \in X$ then $\tilde{f} : X \to n - \{t\}$ given by $\tilde{f}(x) = f(x)$ is also injective.

So we have that $g \circ \tilde{f} : X \to m$ is injective, which contradicts the fact that $|X| = n$ since $m^+ = n$ implies that $m < n$. □

If $f : X \to Y$ is a bijection then $f^{-1} : Y \to X$ is a bijection as well, which gives the following easy fact.

Lemma

If we have two finite sets X and Y where $|X| = n$ and $|Y| = n$ then there exists a bijection $g : X \to Y$.

Proof.

Let $f_X : X \to n$ and $f_Y : Y \to n$ be two bijections which exist by virtue of $|X| = |Y| = n$ and define $g : X \to Y$ by $g = f_Y^{-1} \circ f_X : X \to n \to Y$ which is a bijection since it is a composition of bijections. $\square$

We need the following two lemmas for the things we wish to prove.

Lemma (Deletion 1)

If $g : X \to Y$ is injective then if $x \in X$ and $y = g(x)$ then $\tilde{g} : X - \{x\} \to Y - \{y\}$ given by $\tilde{g}(t) = g(t)$ is injective if $X - \{x\}$ is non-empty.

Lemma (Deletion 2)

If $M = m^+$ where $m > 0$ and $t \in M$ then $f : M - \{t\} \to m$ given by $f(x) = x$ is bijective.

Theorem

If $f : n \to m$ is injective then $n \leq m$.

Proof.

Let $I = \{n \in \omega \mid f : n \to m \text{ injective implies } n \leq m\}$ and observe that $0 \in I$ trivially since there are no functions with domain 0.

One could also observe that $1 \in I$ since then $m = 0$ is impossible since the codomain can't be empty, and if $m > 0$ then $f : 1 \to m$ is a function with domain consisting of a singleton set, so it's automatically injective and $1 \leq m$. So now assume $n \in I$ for some $n > 1$ then any $f : n \to m$ that is injective implies $n \leq m$.

If now $F : n^+ \to M$ is injective then if $M = m^+$ for some M consider the function

$$\tilde{F} : n = n^+ - \{\{n\}\} \underset{Deletion1}{\to} M - \{F(\{n\})\} \underset{Deletion2}{\to} m$$

which is injective so $n \leq m$ which implies $n^+ \leq m^+ = M$ and therefore $n^+ \in I$. Thus I

A natural and pretty obvious consequence of this is the following succinct statement.

Corollary

For any $n \in \omega$, $|n| = n$.

Proof.

If $|n| = m$ then if $f : n \to m$ is injective so $n \leq m$ by the previous result, but it is also bijective so $f^{-1} : m \to n$ exists and is also a bijection and, in particular, injective so (also by the previous result) $m \leq n$. $\square$

For finite sets X and Y then we can quantify injectivity and surjectivity in terms of their sizes directly.

Lemma

If X and Y are finite with $|X| = n$ and $|Y| = m$ then $h : X \to Y$ is injective if and only if $n \leq m$ and, it is also surjective only if $n = m$.

Proof.

By assumption there exist bijections $f : X \to n$ and $g : Y \to m$ so if $h : X \to Y$ is injective then $g \circ h : X \to m$ is injective, which since $|X| = n$ is true if and only if $n \leq m$.

And if h is surjective then $g \circ h \circ f^{-1} : n \to m$ is bijective which is equivalent to $n = m$. □

A consequence of this is the following fundamental result which is slightly different than how the book frames it.

Proposition (The Pigeonhole Principle)

If X and Y are finite sets with $|X| = |Y|$ then $f : X \to Y$ is injective if and only if it is surjective.

Proof.

The basic point is that we've already demonstrated this for the case of $X = n$ and $Y = m$ already, and any injection/surjection between X and Y corresponds to a injection/surjection between n and m.

$$\begin{array}{ccc} X & \longrightarrow & Y \\ \downarrow & & \downarrow \\ n & \longrightarrow & m \end{array}$$

Although we have started with injective functions and then deduced when these are surjective, we can, in the setting of finite sets, establish a number of 'dual' results about surjective functions.

Lemma

If $f : X \to Y$ where X and Y are finite then f surjective implies that $|X| \geq |Y|$.

Proof.

Exercise $\square$

Lemma

If $f : X \to Y$ where $|X| = |Y| = n$ then f surjective implies that f is injective.

Proof.

Exercise $\square$

A way to detect that a set is *not* finite is the following.

Lemma

If $f : X \to X$ is injective but not surjective then X cannot be finite.

Proof.

This is consequence of what we already know about injective functions from one finite set to another. □

And speaking of non-finite sets we have:

Proposition

If $g : \omega \to X$ is injective then X is not finite.

Proof.

If $g : \omega \to X$ and $|X| = n$ then there exists $h : X \to n$ which is bijective. As such we have an injection $h \circ g : \omega \to n$ and so it suffices to show that no function $f : \omega \to n$ is injective for any $n \in \omega$.

If $f : \omega \to n$ is injective then f restricts to $\tilde{f} : n^+ \to n$ which is injective, which, by the earlier theorem implies that $n^+ \leq n$ which is impossible. □

Note, we are deliberately using the phrase 'non finite' instead of infinite, because, as we shall see, there is some subtlety in the quantification of what 'infinite' means.

As we shall see, the distinction between different orders of infinity arises when one considers power sets.

For finite sets, we can prove some basic facts about their power sets.

Theorem

If $|X| = n$ then $\mathcal{P}(X)$ is finite.

Before we prove this, we establish some technical facts which will help with the proof.

As any finite set X is in bijective correspondence with some $n \in \omega$ we shall prove our results in terms of $n \in \omega$.

Theorem

For $m, n \in \omega$ one has that $|m \times n| = mn$.

Corollary

For $m_1, m_2, \ldots, m_k \in \omega$ one has $|m_1 \times \cdots \times m_k| = m_1 \cdots m_k$.

Proof.

Let $I = \{n \in \omega \mid |m \times n| = mn\}$ and we shall show that $I = \omega$.

For $n = 0$ the result is trivially true since $\emptyset \times X$ is empty for any set X.

We shall, however, also consider the case $n = 1$ since $f : m \times 1 \to m$ given by $f(\langle x, 0\rangle) = x$ is injective so $|m \times 1| \leq |m| = m$ and $g : m \to m \times 1$ given by $g(x) = \langle x, 0\rangle$ is injective so $m = |m| \leq |m \times 1|$ so $|m \times 1| = |m|$. Suppose $n \in I$ then there exists a bijection $F : m \times n \to mn$ so let's define $\tilde{F} : m \times n^+ \to mn^+$ by

$$\tilde{F}(\langle x, y\rangle) = \begin{cases} F(\langle x, y\rangle) \text{ if } y \in n \\ my + x \qquad\qquad \text{if } y = n \end{cases}$$

which is bijective since for $x \in m$,$y \in n$ one has $F(\langle x, y\rangle) \in mn < mn^+$ and if $y = n^+$ then $my + x = my + x'$ then $x = x'$ and every $z \in mn^+ - mn$ is of the form $my + x$ for $y = n$ and $x \in m$ and so $|m \times n| = mn^+$. As such $n^+ \in I$ so $I = \omega$. □

So now we prove that

Theorem

For $m \in \omega$ one has that $\mathcal{P}(m)$ is finite, and in fact $|\mathcal{P}(m)| = 2^m$.

Proof.

For $2 = \{0, 1\}$, let $T = \prod_{k \in m} 2 = 2 \times 2 \cdots \times 2$ which equals the set of all functions $f : m \to 2$.

We can define $F : \mathcal{P}(m) \to T$ as follows: For $A \subset m$ let $f_A \in T$ be defined by $f_A(k) = 0$ if $k \notin A$ and $f_A(k) = 1$ if $k \in A$ and let $F(A) = f_A$.

It is clear that F is bijective so therefore not only is $\mathcal{P}(m)$ finite, but $|\mathcal{P}(m)| = |T| = 2^m$. □

Countable Sets

Our first class of infinite sets is familiar of course, namely the natural numbers $\mathbb{N} = \omega$.

However, we can characterize what makes other sets similarly infinite.

Definition

A set X is countable if there exists an injection $f : X \to \omega$.

You'll note that this is not given in terms of a map $\omega \to X$ as this would allow for the possibility that X is 'larger' which indeed is the case for some sets X, but rather we view X as somehow 'embeddable' as a subset of ω.

Our first example is this
Fact: $\mathbb{Z}$ is countable.

This can be seen by 'reordering' the integers in a way which (as a bonus) well orders them:

$$0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$$

that is

$$0 \mapsto \mathbf{0}, 1 \mapsto \mathbf{1}, -1 \mapsto \mathbf{2}, 2 \mapsto \mathbf{3}, -2 \mapsto \mathbf{4}, 3 \mapsto \mathbf{5}, -3 \mapsto \mathbf{6}$$

which can actually be given by an explicit function, namely

$$f(x) = \begin{cases} 2x - 1 & \text{if } x > 0 \\ 2(-x) & \text{if } x \leq 0 \end{cases}$$

which is readily seen to be injective, and, in fact, bijective.

There are a number of relatively easy facts about countability one can show.

Proposition

If A is countable and $g : B \to A$ is injective then B is countable as well.

Proof.

If $f : A \to \omega$ is injective then so is $g \circ f : B \to \omega$. □

Proposition

If A is countable and $B \subseteq A$ then B is countable as well.

Proof.

If $f : A \to \omega$ is injective then so is $f\big|_B : B \to \omega$, i.e. restrict f to B. □

What the previous proposition showed is that countability is inherited by subsets.

So in particular the restriction of an injective function to a subset of its domain is still injective and thus we have this.

Proposition

If A and B are countable, so is $A \cap B$.

We can also show that the class of countable sets is closed under other set operations.

Proposition

If A,B are countable then so is $A \cup B$.

Proof.

If we let $X = A$ and $Y = B - (A \cap B)$ then $X \cap Y = \emptyset$ and $A \cup B = X \cup Y$ and if $f : A \to \omega$ and $g : B \to \omega$ are injective then so are $f : X \to \omega$ (since $A = X$) and $g\big|_Y$.

As such, we can define $F : X \cup Y \to \omega$ as follows, for $x \in X$ let $F(x) = 2f(x)$ and for $y \in Y$ let $F(y) = 2g(y) + 1$.

As $X \cap Y = \emptyset$ then we observe first that $F(X) \cap F(Y) = \emptyset$ since all the elements of $F(X)$ are even and the elements of $F(Y)$ are odd.

Moreover, for $x_1, x_2 \in X$, $2f(x_1) = 2f(x_2)$ iff $f(x_1) = f(x_2)$ and as f is injective we find that $x_1 = x_2$, and a similar analysis holds for $y \in Y$ and so F is injective. □

Now, the definition of countable implies that a finite set is countable since, if $|X| = n$ then there is an injection $f : X \to n$ where $n \in \omega$ where also $n \subseteq \omega$.

So to exclude finite examples, one defines:

Definition

A set X is countably infinite if it is countable and infinite (non-finite).

If we examine the definition of countable and infinite we have the following.

Proposition

X is countably infinite if and only if there is a bijection $f : X \to \omega$.

We showed earlier that $\mathbb{Z}$ is countable, but in fact we proved that it is countably infinite.

Moreover, our proof demonstrated that the bijection $\mathbb{Z} \to \omega$ allows us to order the integers where the ordering is inherited by the ordering that exists on ω.

Theorem

Every countably infinite set can be ordered in such a way as to be order isomorphic to ω.

The book uses the term 'denumerable' to indicate the ability to list out the elements of a countably infinite X set as sequence $\{x_0, x_1, x_2, \dots\}$ and points out that, later on, it will be shown that the real numbers $\mathbb{R}$ are **not** denumerable.