Countability

Professor Cian Dorr

29th September 2022

New York University

Predecessors

Let pred be the function $\mathbb{N} \to \mathcal{P}\mathbb{N}$ defined recursively by

$$\begin{aligned} \operatorname{pred} 0 &= \varnothing \\ \operatorname{pred}(\operatorname{suc} n) &= \operatorname{pred} n \cup \{n\} \end{aligned}$$

We write $n < m$ as shorthand for '$n \in \operatorname{pred} m$', and $n \leq m$ as shorthand for '$n < m$ or $m = m$', so the recursion clauses can be written as follows:

$$\begin{aligned} n < 0 &\text{ never} \\ n < \operatorname{suc} m &\text{ iff } n \leq m \end{aligned}$$

Some facts about order

Useful facts

For all k, n, m:

1. $0 \leq n$
2. If $\operatorname{suc} n < m$ then $n < m$.
3. If $k < n$ and $n < m$ then $k < m$ (And thus if $k \leq n$ and $n \leq m$ then $k \leq m$.)
4. Not $n < n$.
5. Not $n < m$ and $m < n$. (And thus if $n \leq m$ and $m \leq n$, $n = m$.)
6. Either $n < m$ or $m < n$ or $n = m$ (And thus either $n \leq m$ or $m \leq n$.)
7. $n \leq m$ iff $m = n + k$ for some k.

These can all be proved by straightforward inductions.

Example

For example, here's the proof that $k < n$ and $n < m$ then $k < m$. By induction on m, generalizing over k and n.

Base case: trivial since it can't happen that $k < n$ and $m < 0$.

Induction step: suppose that whenever $k < n$ and $n < m$, $k < m$, and that for a certain k and n, $k < n$ and $n < \operatorname{suc} m$. Then either $n < m$, in which case $k < m$ by the IH, or else $n = m$, in which case $k < m$ by substitution; either way, we have $k < \operatorname{suc} m$ by the recursion clause for $<$.

Another example

Proof by induction that every n is such that there is no m for which $n < m$ and $m < n$.

Base case: trivial since there is no m for which $m < 0$.

Induction step: Suppose that there is no m for which $n < m$ and $m < n$, and that $m < \operatorname{suc} n$. So either $m < n$ or $m = n$. If $m < n$, then not $n < m$ by the IH; if $m = n$, then not $n < m$ by substitution. So either way, not $\operatorname{suc} n < m$ by fact 2.

One more useful fact

Least Number Principle

For every $X \subseteq \mathbb{N}$, either $X = \varnothing$ or there exists $n \in X$ such that $n \leq m$ for all $m \in X$.

This is equivalent to the claim that $<$ is *well-founded*:

Definition

Where R is a binary relation on A, R is *well-founded* iff for every $X \subseteq A$, either $X = \varnothing$ or there exists $x \in X$ such that there is no $y \in X$ for which Ryx.

This can be used to justify a different kind of proof by induction, so called "strong induction". If we want to prove that every number has property ϕ, we can do so by showing that for any n, if $\phi(m)$ for all $m < n$, then $\phi(n)$. (In other words: there is no least non-ϕ number; so by the Least Number Principle, there is no non-ϕ number.)

Proving the Least Number Principle

Suppose that X has no least element. First we will prove by induction that for all n, $X \cap \operatorname{pred} n = \varnothing$.

Base case: trivial since $\operatorname{pred} 0 = \varnothing$.

Induction hypothesis: supopose for contradiction that $X \cup \operatorname{pred} n = \varnothing$ and $m \in X \cup \operatorname{pred}(\operatorname{suc} n)$. Then we must have $m \in \operatorname{pred}(\operatorname{suc} n) \setminus \operatorname{pred} n$, hence $m = n$: but then n is a least element of X.

This implies that $X = \varnothing$. For suppose $n \in X$; then since $n \in \operatorname{pred}(\operatorname{suc} n)$, we would have $n \in X \cap \operatorname{pred}(\operatorname{suc} n)$.

Analogues for lists

For lists there are two analogues of $\leq$, the *initial segment* and *final segment* relations, and two analogues of $<$, the *proper initial segment* and *proper final segment* relations.

Everything we have said about $<$ applies *mutatis mutandis* to these principles, except that we don't have the analogue of the 'connectedness' fact: we can have two lists neither of which is an intial/final segment of the other.

Size n

Definition

$n \in \mathbb{N}$ is the *size* of $A :\!= A \sim \operatorname{pred} n$.

Finitude, again

In an earlier lecture, we defined 'A is finite' to mean '$A \in \mathcal{P}_{\mathsf{fin}} A$', where $\mathcal{P}_{\mathsf{fin}} A$ (the set of finite subsets of A) is defined as the closure of $\{\varnothing\}$ under the operation of adding one element of A.

We could equivalently have defined finitude in terms of the natural numbers:

Fact

A is finite iff $A \sim \operatorname{pred} n$ for some $n \in \mathbb{N}$.

Finitude, again

For the left to right direction, we prove by induction that for every $B \in \mathcal{P}_{fin}A$ there is some n such that $B \sim \operatorname{pred} n$. For $\varnothing$ it's 0; and when B' is the result of adding one element to B and $B \sim n$, $B' \sim \operatorname{suc} n$.

For the right to left direction, it suffices to note that $\operatorname{pred} n$ is finite for every n (since $\varnothing$ is finite, and adding one element to a finite set always produces a finite set). Then we have to show that if $A \sim B$ and A is finite, B is finite.

Finitude facts

Given that a finite set is one that has size n for some n, the following can readily be established by numerical induction:

Finitude Facts

1. If A and B are finite, $A \cup B$ is finite.
2. If A and B are finite, $A \times B$ is finite.
3. If A is a finite set of finite sets, $\bigcup A$ is finite.
4. If A is finite, $\mathcal{P}A$ is finite.
5. If A and B are finite, A^B is finite.

Countability

Definition

Set A is *countable* $:= A \lesssim \mathbb{N}$. (I.e.: there is an injection from A to $\mathbb{N}$.)

Don't confuse with:

Definition

Set A is *countably infinite* $:= A \sim \mathbb{N}$ (there is a bijection from A to $\mathbb{N}$.

Fact

A set is countable iff it is either finite or countably infinite.

To prove this, we show that every subset of $\mathbb{N}$ that is not a subset of $\mathrm{pred}\, n$ for any n is the same size as $\mathbb{N}$. We define an injection:

$$\begin{aligned} f\, 0 &= \min X \\ f\, \mathrm{suc}\, n &= \min(X \setminus (fn \cup \mathrm{pred}\, fn)) \end{aligned}$$

This is an injection from $\mathbb{N}$ to X.

Strings over a finite alphabet

Fact

If A is finite and $\neq \varnothing$, then A^* is countably infinite.

(Note that $\varnothing^* = \{[]\}$ which is not countably infinite, though it is countable.)

Intuitively, this is true because we can list all the members of A^* in alphabetical order.

Strings over a finite alphabet

To define an injective function f from A^* to $\mathbb{N}$, let n be the size of A, and let g be a bijection from A to $\mathrm{pred}\, n$. Let $g^+ a = \mathrm{suc}\, ga$ for every $a \in A$.

We define $f : A^* \to \mathbb{N}$ inductively as follows.

$$f\,[] = 0$$
$$f\,(a : s) = g^+ a + n \times fs$$

This turns out to be injective (in fact it's a bijection). To prove it's injective, we rely on the following well-known arithmetical fact:

Division Theorem

If $qn + r = q'n + r'$, where $r < n$ and $r' < n$, then $q = q'$ and $r = r'$.

Strings over a finite alphabet

We prove by induction (on t) that whenever $fs = ft$, $s = t$.

Base case: suppose $fs = f[\,] = 0$. Then it can't be that s is $(a : s')$ for some a and s', since then we'd have $fs = \mathrm{suc}(ga + nfs')$, and zero isn't a successor. So it must be that $s = [\,]$.

Induction step: suppose that s is such that whenever $fs = ft$, $s = t$, and suppose $f(a : s) = ft$. It can't be that $t = [\,]$ since $f(a : s) \neq 0$, so we must have $t = b : t'$ for some b, t'. So we have $\mathrm{suc}(nfs + ga) = \mathrm{suc}(ngt' + gb)$, and hence $nfs + ga = nft' + gb$. Since both $ga < n$ and $gb < n$, the division theorem implies $fs = ft'$ and $ga = gb$. But then $s = t'$ by the induction hypothesis, and $a = b$ by the injectivity of b, so $t = (b : t') = (a : s)$.

Proving the division theorem

Coding lists of lists as lists

Suppose a finite set $B = A \cup \{c\}$. Then we can define an injection from $(A^*)^*$ to B^* by using c as a 'comma' to join any list of A-lists into one big B-list.

We define $f : A^{**} \to B^*$ recursively as follows.

$$f\,[] = []$$

$$f(s : j) = \begin{cases} s & \text{if } j = [] \text{ and } s \neq [] \\ s \oplus (c : fj) & \text{otherwise} \end{cases}$$

To show that this is injective, we can define a 'decoding' function $g : B^* \to A^{**}$, and show that it's a left inverse of f.

$$g[] = []$$

$$g(a : s) = \begin{cases} [[a]] & \text{if } a \neq c \text{ and } s = [] \\ (a : t) : j & \text{if } a \neq c \text{ and } gs = t : j \\ [] : gs & \text{if } a = c \end{cases}$$

We then need to show that $g(f(j)) = j$ for all $j \in A^{**}$.

Strings over a countable alphabet

Note that whenever $A \lesssim B$, $A^* \lesssim B^*$, since any injection $f : A \to B$ can be lifted to an injection $f^* : A^* \to B^*$ by recursively defining

$$f^*[] = []$$
$$f^*(a : s) = fa : f^*s$$

So by the above, when A is finite and nonempty, and $B = A \cup \{c\}$ for some $c \notin A$, we have:

$$\mathbb{N}^* \sim A^{**} \sim B^* \sim \mathbb{N}$$

So we can conclude that whenever a set A is countable, A^* is countable too.

An easy corollary

Obviously $\mathbb{N} \times \mathbb{N} \lesssim \mathbb{N}^*$, since $[\langle n, m \rangle \to [n, m]]$ is injective.

And obviously $\mathbb{N} \lesssim \mathbb{N} \times \mathbb{N}$, since $[n \to \langle n, 0 \rangle]$ is injective.

So (by Schröder-Bernstein) we have $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$: there are as many ordered pairs of naturals as there are naturals.

Bijecting $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$

The particular bijections we get by following the proof above are a bit wacky. But there are much nicer bijections, e.g. the one diagrammed here:

$$
\begin{array}{c|cccccc}
 & 0 & 1 & 2 & 3 & 4 & \cdots \\
\hline
0 & 0 & 1 & 3 & 6 & 10 & \\
1 & 2 & 4 & 7 & 11 & & \\
2 & 5 & 8 & 12 & & & \\
3 & 9 & 13 & & & & \\
4 & 14 & & & & & \\
\vdots & & & & & &
\end{array}
$$

This is

$$f\langle n, m\rangle = \frac{(n+m)(n+m+1)}{2} + m$$

Countability facts

So we have analogues for countability for two of our facts about finitude.

Countability Fact 1

If A and B are countable, $A \cup B$ is countable.

Proof: suppose that $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$ are injections. Then so is $h : A \cup B \to \mathbb{N}$ defined by

$$hx = \begin{cases} 2fx & \text{if } x \in A \\ 2gx + 1 & \text{if } x \in B \setminus A \end{cases}$$

Countability Fact 2

If A and B are countable, $A \times B$ is countable.

Proof: In general, if $A \lesssim X$ and $B \lesssim Y$ then $A \times B \lesssim X \times Y$.

Countability facts

We do *not* have an analogue of Finitude Fact 4: by Cantor's theorem, the powerset of a countably infinite set is *not* countably infinite.

We do however have a restricted version of this:

Countability Fact 4

If A is countable, $\mathcal{P}_{\mathsf{fin}} A$ is countable.

Proof: We can injectively map sets in $\mathcal{P}_{\mathsf{fin}} A$ to lists in A^* by ordering the elements according to some fixed $f : A \to \mathbb{N}$ (using the least number theorem).

Countability facts

We also *not* have an analogue of Finitude Fact 5. For example, although $\{0,1\}$ and $\mathbb{N}$ are both countable, $\{0,1\}^{\mathbb{N}}$ is not countable, since there is a bijection between it and $\mathcal{P}\mathbb{N}$.

We do however have the following restricted version:

Countability Fact 5

If A is countable and B is *finite*, A^B is countable.

Proof: by induction on the size of B.

Base step: $A^{\varnothing}$ has size 1.

Inductive step: there is a bijection from $A^{\mathsf{pred}\,n} \times A$ to $A^{\mathsf{pred}\,\mathsf{suc}\,n}$, namely $[\langle f, a\rangle \mapsto f \cup \{\langle n, a\rangle\}]$.

Countable union of countable sets

It turns out that we also have a direct analogue of Finitude Fact 3:

Countability Fact 3

If $\mathbf{V}$ is countable and every element of $\mathbf{V}$ is countable, then $\bigcup V$ is countable.

Intuition: suppose for simplicity that no two elements of $\mathbf{V}$ overlap. Let f be an injection from $\mathbf{V}$ to $\mathbb{N}$, and for each $X \in \mathbf{V}$ let g_X be an injection from X to $\mathbb{N}$. Then the function h that maps each $y \in X$ to $\langle fX, g_X y \rangle$ is an injection from $\bigcup V$ to $\mathbb{N} \times \mathbb{N}$.

Making this proof rigorous turns out to involve an appeal to the Axiom of Choice.