# Schröder-Bernstein, numbers, and lists

Professor Cian Dorr

20th September 2022

New York University

# Schröder-Bernstein

Let's start with one piece of unfinished business: a proof of the following theorem:

**Schröder-Bernstein Theorem**

For any sets $A$ and $B$, if $A \lesssim B$ and $B \lesssim A$, then $A \sim B$.

We'll infer this from the following lemma:

**Lemma**

For any sets $A$ and $B$, if $A \subseteq B$ and $B \lesssim A$, then $A \sim B$.

# Schröder-Bernstein

**Lemma**

For any sets $A$ and $B$, if $A \subseteq B$ and $B \lesssim A$, then $A \sim B$.

Suppose $A \subseteq B$ and $B \lesssim A$. Then there is some $C \subseteq A$ such that $B \sim C$, i.e. there is a bijection $f : B \to C$. Define $Z$ to as the **closure of** $B \setminus A$ **under** $f$. And define a function $g : B \to A$ as follows:

$$gx = \begin{cases} fx & \text{if } x \in Z \\ x & \text{otherwise} \end{cases}$$

This determines a function from $B$ to $A$, since $B \setminus A \subseteq Z$. We will show that $g$ is a bijection from $B$ to $A$.

- To show $g$ is injective, note that it can't happen that $gx = gy$ if $x \in Z$ and $y \notin Z$, since in that case we'd have $fx = y$ and hence $y \notin Z$ since $Z$ is closed under $f$. So if $gx = gy$, either $x \in Z$ and $y \in Z$ in which case $fx = fy$ and hence $x = y$ by the injectivity of $f$, or $x \notin Z$ and $y \in Z$ in which case $x = gx = gy = y$.
- To show $g$ is surjective, consider an arbitrary $x \in A$. If $x \notin Z$ then $gx = x$ so $x$ is in the range of $g$. If $x \in Z$, then $x$ must be in $f[Z]$, since $f[Z] \cup (B \setminus A)$ is a superset of $B \setminus A$ closed under $f$, hence a superset of $Z$. Thus there exists $y \in Z$ such that $fy = x$ and thus $gy = x$.

*Notation:* when $f : X \to Y$ and $Z \subseteq X$, $f[Z] :- \{fx \mid x \in Z\}$.

Finally we need to get to the actual theorem:

**Schröder-Bernstein Theorem**

For any sets $A$ and $B$, if $A \precsim B$ and $B \precsim A$, then $A \sim B$.

So, suppose we have injections $f : A \to B$ and $g : B \to A$. We have $f[A] \subseteq B$. Also since $f[A] \sim A$, $B \precsim f[A]$. So by the lemma, $f[A] \sim B$, hence $A \sim B$.

# Numbers and Lists

# The Axiom of Numbers (recap)

**The Axiom of Numbers**

$\mathbb{N}$ is a set (the set of natural numbers), 0 is an element of $\mathbb{N}$, and suc is a function $\mathbb{N} \to \mathbb{N}$, such that:

**Inductive Property** $\mathbb{N}$ is the closure of $\{0\}$ under suc.

**Injective Property** (a) suc is injective.

(b) 0 is not in the range of suc.

*Notation:* we write '1' for $\mathrm{suc}\, 0$, '2' for $\mathrm{suc}(\mathrm{suc}\, 0)$), etc.

*Remark:* given our definition of addition, we can prove that $\mathrm{suc}\, n = n + 1$ for all $n \in \mathbb{N}$; once this is proved, we can feel free to write '$n + 1$ instead of '$\mathrm{suc}\, n$' if we prefer.

Let's just prove that last fact. Recall that $n + m$ is short for $\mathrm{add}_n\, m$, where $\mathrm{add}_n$ is the unique function $f : \mathbb{N} \to \mathbb{N}$ such that $f0 = n$ and $f(\mathrm{suc}\, m) = \mathrm{suc}(fm)$ for any $m \in \mathbb{N}$ (where we are assured of the existence of such a function by the Recursion Theorem). The definition thus secures the following two *recursion clauses* (for all $n, m \in \mathbb{N}$):

(i) $$n + 0 = n$$

(ii) $$n + \mathrm{suc}\, m = \mathrm{suc}(n + m)$$

**Proposition**

For all $n \in \mathbb{N}$, $n + 1 = \mathrm{suc}\, n$.

*Proof:* $n + 1 = n + \mathrm{suc}\, 0 = \mathrm{suc}(n + 0)$ (by (ii) $= \mathrm{suc}\, n$ (by (i)).

# The Axiom of Lists

## The Axiom of Lists

For every set $A$, there is a set $A^*$ (the set of finite lists of elements of $A$); an element $[]$ of $A^*$, and a family $(\mathrm{cons}_a)_{a \in A}$ of functions $A^* \to A^*$, such that:

**Inductive Property** $A^*$ is the closure of $\{[]\}$ under $(\mathrm{cons}_a)_{a \in A}$.

**Injective Property** (a) each $\mathrm{cons}_a$ is injective.

(b) $[]$ is not in the range of any $\mathrm{cons}_a$.

(c) when $a \neq b$, the ranges of $\mathrm{cons}_a$ and $\mathrm{cons}_b$ do not overlap.

*Notation:* we write $a : s$ instead of $\mathrm{cons}_a\, s$ (for $a \in A, s \in A^*$).

*Notation:* we write $[a]$ for $a : []$, $[a, b]$ for $a : (b : [])$, $[a, b, c]$ for $a : (b : (c : []))$, etc.

*Notation:* when $A$ is a set of *characters in some alphabet*, we write ***.

# Recursive definitions for lists

Intuively, the Injective Property for lists means that every element of $A*$ can be constructed in *at most one way* by starting with [] and applying the functions $\mathrm{cons}_a$ (for $a \in A$).

This gives us the following (which we'll prove later):

**Recursion Theorem for Lists**

Suppose $B$ is a set; $z \in B$; and for every $a \in A$, $s_a : B \to B$. Then there is a *unique* function $f : A^* \to B$ such that $f[] = z$ and for all $t \in A^*$, $f(\mathrm{cons}_a\, t) = s_a(ft)$.

Compare this with the following, stated last week:

**Recursion Theorem for Numbers**

Suppose $B$ is a set; $z \in B$; and $s : B \to B$. Then there is a *unique* function $f : \mathbb{N} \to B$ such that $f0 = z$ and for all $n \in \mathbb{N}$, $f(\mathrm{suc}\, n) = s(fn)$.

For example, the following counts as a definition:

**Definition**

For any $A$, let length be the function $A^* \to \mathbb{N}$ such that $\text{length}[] = 0$ and $\text{length}(\text{cons}_a\, s) = \text{suc}(\text{length}\, s)$ for all $a \in A, s \in A^*$.

The Recursion Theorem for Lists assures us that there is a unique function $A^* \to \mathbb{N}$ meeting these conditions.

# The Recursion Theorem for Lists at work

**Definition**

For any $A$, let elements be the function $A^* \to \mathcal{P}A$ such that $\mathrm{elements}[] = \varnothing$ and $\mathrm{elements}(\mathrm{cons}_a\, s) = \mathrm{elements}\, s \cup \{a\}$ for all $a \in A, s \in A^*$.

**Definition**

For any $A$ and any $t \in A^*$ let $\mathrm{concat}_t$ be the function $A^* \to A^*$ such that $\mathrm{concat}_t[] = t$ and $\mathrm{concat}_t(\mathrm{cons}_a\, s) = \mathrm{cons}_a(\mathrm{concat}_t\, s)$ for all $a \in A, s \in A^*$.

*Notation:* we write '$s \oplus t$' for '$\mathrm{concat}_t\, s$', so the two clauses can be written as:

$$[] \oplus t = t$$
$$(a : s) \oplus t = a : (s \oplus t)$$

## Proofs by induction about lists

Thanks to the Inductive Property in the Axiom of Lists, we can prove that every element of $A^*$ has a certain property $\phi$ by proving:

- Base Case: $[]$ has $\phi$.
- Induction Step: for all $s \in A^*$, if $s$ has $\phi$, then for all $a \in A$, $a : s$ has $\phi$.

**Example**

For all $s, t \in A^*$, $\text{length}(s \oplus t) = \text{length}\, t + \text{length}\, s$.

*Proof:* By induction on $s$. Base case:

$$\begin{aligned}
\text{length}([] \oplus t) &= \text{length}\, t \\
&= \text{length}\, t + 0 \\
&= \text{length}\, t + \text{length}[]
\end{aligned}$$

Induction step: suppose $\text{length}(s \oplus t) = \text{length}\, t + \text{length}\, s$. Then

$$\begin{aligned}
\text{length}((a : s) \oplus t) &= \text{length}(a : (s \oplus t)) \\
&= \text{suc}(\text{length}(s \oplus t)) \\
&= \text{suc}(\text{length}\, t + \text{length}\, s) \\
&= \text{length}\, t + \text{suc}(\text{length}\, s) \\
&= \text{length}\, t + \text{length}(a : s)
\end{aligned}$$

# The Recursion Theorem

**The Recursion Theorem**

Suppose that $C$ is the closure of $B \subseteq A$ under a family $(R_i)_{i \in I}$ of relations on $A$ and a family $(S_k)_{k \in K}$ of relations from $A \times A$ to $A$, such that

(i) Each $R_i$ and $S_k$ is injective.

(ii) The ranges of the $R_i$ and $S_i$ are all disjoint from one another and from $B$.

Suppose we have $z : B \to D$; $s_i : D \to D$ for each $i \in I$, and $t_k : D^2 \to D$ for each $k \in K$. Then there is a unique function $f : C \to D$ such that

a. $fx = zx$ for all $x \in B$.

b. Whenever $R_i xy$, $fy = s_i(fx)$.

c. Whenever $S_k \langle x, y \rangle z$, $fz = t_k \langle fx, fy \rangle$.

# Proving the Recursion Theorem

*Proof:* For each $R_i$, let $R_i^+$ be the relation on $C \times D$ such that $R_i^+\langle x, u\rangle\langle y, v\rangle$ iff $R_ixy$ and $v = s_iu$, and for each $S_k$, let $S_k^+$ be the relation from $(C \times D)^2$ to $C \times D$ such that $S_k^+\langle\langle x, u\rangle, \langle y, v\rangle\rangle\langle z, w\rangle$ iff $S_k\langle x, y\rangle z$ and $w = t_k\langle u, v\rangle$.

Let $F$ be the closure of $z$ under $(R_i^+)$ and $(S_k^+)$. We will prove that $F$ is a function from $C$ to $D$. This suffices to prove the theorem, since clearly we have:

a. $Fx(zx)$ for all $x \in B$ (since $z \subseteq F$).
b. Whenever $R_ixy$ and $Fxu$, $Fy(s_iu)$ (since in that case $R_i^+\langle x, u\rangle\langle y, s_iu\rangle$, and $F$ is closed under $R_i^+$).
c. Whenever $S_k\langle x, y\rangle z$, $Fxu$, and $Fyv$, $Fz(t_k\langle u, v\rangle)$ (since in that case $S_k^+\langle\langle x, u\rangle, \langle y, v\rangle\rangle\langle z, t_k\langle u, v\rangle\rangle$, and $F$ is closed under $S_k^+$).

Moreover $F \subseteq F'$ for any other relation $F'$ meeting these three conditions, and so $F = F'$ for any other *function* $F'$ meeting these three conditions (since no function is a subset of any other function with the same domain).

# Proving the Recursion Theorem

(i) $F$ is serial, i.e. for all $x \in C$ there exists $u \in D$ such that $Fxu$. By induction.

*Base case:* if $x \in B$ then $Fx(zx)$: case (a) from the previous slide.

*Induction step for $R_i$:* if $Fxu$ and $R_i xy$, then $Fy(s_i u)$: case (b) from the previous slide.

*Induction step for $S_k$:* suppose $Fxu$, $Fyv$, and $S_k\langle x, y\rangle z$. Then $Fz(t_k\langle u, v\rangle)$: case (c) from the previous slide

## Proving the Recursion Theorem

(ii) $F$ is functional, i.e. for any $x \in C$, if $Fxu$ and $Fxv$ then $u = v$. By induction.

*Base case:* suppose $x \in B$. Then since $x$ isn't in the range of any $R_i$ or $S_k$, no ordered pair $\langle x, u \rangle$ is in the range of any $R_i^+$ or $S_k^+$. So if $\langle x, u \rangle$ and $\langle x, v \rangle$ are in $F$, they are both in $z$, and hence $u = v$ since $z$ is functional.

*Induction step for $R_i$:* suppose that $x$ is $F$-related to a unique $u$, $R_i xy$, and $Fyv$. We will show that $v = s_i u$. Since $y$ isn't in $B$, isn't in the range of any $R_j$ for $j \neq i$, and isn't in the range of any $S_k$, $\langle y, v \rangle$ isn't in $z$, isn't in the range of any $R^+ j$ for $j \neq i$, and isn't in the range of any $S_k^+$. So it must be in the range of $R_i^+$: i.e. $R_i^+ \langle x', u' \rangle \langle y, v \rangle$ for some $x' \in C$, $u' \in D$. But then $R_i x' y$, hence $x' = x$ (since $R_i$ is injective), hence $u' = u$ (by the induction hypothesis), hence $v = s_i u$ (by the definition of $R_i^+$).

# Proving the Recursion Theorem

*Induction step for $S_k$:* suppose that $x$ is $F$-related to a unique $u$, $y$ is $F$-related to a unique $v$, $S_k\langle x, y\rangle z$, and $Fzw$. We will show that $v = t_k\langle u, v\rangle$. Since $z$ isn't in $B$, isn't in the range of any $R_i$, and isn't in the range of $S_j$ for $j \neq k$, $\langle z, w\rangle$ isn't in $z$, isn't in the range of any $R^+j$ for $j \neq i$, and isn't in the range of any $S_k^+$. So it must be in the range of $S_k^+$: i.e. $S_i^+\langle\langle x', u'\rangle, \langle y', v'\rangle\rangle\langle z, w\rangle$ for some $x', y' \in C$, $u', v' \in D$. But then $S_k\langle x', y'\rangle z$, hence $x' = x$ and $y' = y$ since $S_k$ is injective, hence $u' = u$ and $v' = v$ by the induction hypothesis, hence $w = t_k\langle u, v\rangle$ by the definition of $S_k^+$.