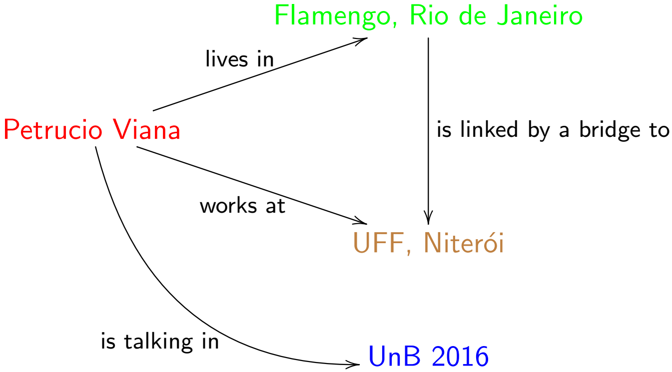
# Induction, iteration, recursion, and well ordering




*Paulo Borges* (CEFET-RJ), *Marcia Cerioli* (COPPE/IM-UFRJ), *Guilherme Silveira* (IM-RJ)

# Outline

1. Mathematical induction
2. Dedekind-Peano axioms
3. Iteration
4. The strength of the axioms
5. Recursion
6. Well ordering

# 1. Mathematical induction

# Mathematical induction

Intuitively, mathematical induction means
'$n$ is a natural number iff $n$ can be reached by a finite number of applications of adding 1 to 0'.

Formally, we cannot state the definition in this way, because in doing so we were defining 'natural number' using 'finite number'. But the latter is the same as the former.

How to scape from this circularity?

# The structure of natural numbers

We have:

- 0 : a natural number;
- $S(x) = x + 1$ : an operation on natural numbers;

We want to define $\mathbb{N}$, the set of natural numbers, in a such way that:

- $0 \in \mathbb{N}$;
- $n \in \mathbb{N}$ iff $n = \underbrace{S(S(\cdots S(0))\cdots)}_{n \text{ times}}$.

That is, $n$ is a natural number iff either it is zero or it is the successor of the successor of $\cdots$ of the successor of 0.

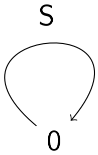
# The structure of natural numbers

We want ‘start in 0 and move on, with no move back’.

We assume:

- $\forall x[S(x) \neq 0]$.
- $\forall xy[s(x) = s(y) \Rightarrow x = y]$.

So, we can not have:



# The structure of natural numbers

We want 'start in 0 and move on, with no move back'.

We assume:

- $\forall x[S(x) \neq 0]$.

- $\forall xy[s(x) = s(y) \Rightarrow x = y]$.

Hence, we must have:

$$0 \xrightarrow{\text{S}} \text{S}(0)$$

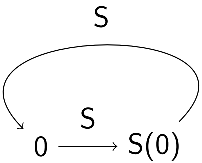
# The structure of natural numbers

We want 'start in 0 and move on, with no move back'.

We assume:

- $\forall x[S(x) \neq 0]$.
- $\forall xy[s(x) = s(y) \Rightarrow x = y]$.

So, we can not have:



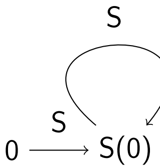
# The structure of natural numbers

We want 'start in 0 and move on, with no move back'.

We assume:

- $\forall x[S(x) \neq 0]$.
- $\forall xy[s(x) = s(y) \Rightarrow x = y]$.

Besides, we can not have:



# The structure of natural numbers

We want 'start in 0 and move on, with no move back'.

So, we assume:

- $\forall x[S(x) \neq 0]$.

- $\forall xy[s(x) = s(y) \Rightarrow x = y]$.

Hence, we must have:

$$0 \xrightarrow{\text{S}} \text{S}(0) \xrightarrow{\text{S}} \text{S}(\text{S}(0))$$

# The structure of natural numbers

And so on . . .

$$0 \xrightarrow{S} S(0) \xrightarrow{S} S(S(0)) \xrightarrow{S} S(S(S(0))) \xrightarrow{S} \cdots$$

# The structure of natural numbers

We want 'start in 0 and move on, with no move back'.

So, we assume:

- $\forall x[S(x) \neq 0]$.

- $\forall xy[s(x) = s(y) \Rightarrow x = y]$.

These imply our set $\mathbb{N}$ is infinite.

There is an injection from $\mathbb{N}$ onto a proper part of it (Dedekind, 1888).

# The structure of natural numbers

Let $X$ be a set.
We say that $X$ is *good* iff $0 \in X$ and $\forall x[x \in X \Rightarrow S(x) \in X]$.

Intuitively, $\mathbb{N}$ is good.

Besides, intuitively, if $X$ is good, then $\underbrace{S(S(\cdots S(0))\cdots)}_{n \text{ times}} \in X$, for every $n$.

We want $\mathbb{N}$ contains nothing else except the elements of the form $\underbrace{S(S(\cdots S(0))\cdots)}_{n \text{ times}}$.

# The structure of natural numbers

The idea is to define $\mathbb{N}$ as the least (wrt inclusion) good set.

**Statement:** There is a good set.

**Statement:** If $\{X_i : i \in I\}$ is a family of good sets, then $\bigcap\{X_i : i \in I\}$ is a good set.

# The birth of the induction axiom

**Definition:** $\mathbb{N} = \bigcap\{X : X \text{ is a good set}\}$.

By the definition of $\bigcap$, we have:
$\forall X[X \text{ is good } \Rightarrow \bigcap\{X : X \text{ is good}\} \subseteq X]$.

By the definition of $\mathbb{N}$, we have:
$\forall X[X \text{ is good } \Rightarrow \mathbb{N} \subseteq X]$.

By the definition of good, we have:
$\forall X[0 \in X \wedge \forall x[x \in X \Rightarrow S(x) \in X] \Rightarrow \mathbb{N} \subseteq X]$.

# A meaning for the induction axiom

The induction axiom states:
$\forall X[0 \in X \wedge \forall x[x \in X \Rightarrow S(x) \in X] \Rightarrow \mathbb{N} \subseteq X]$.

That is:
$\forall X[0 \in X \wedge \forall x[x \in X \Rightarrow S(x) \in X] \Rightarrow \forall y[y \in \mathbb{N} \Rightarrow y \in X]$.

So, to show that every element of $\mathbb{N}$ belongs to a set $X$ (possesses a property $X$) suffices to show $X$ is good:

- $0 \in X$.
- $\forall x[x \in X \Rightarrow S(x) \in X]$

# 2. Dedekind Peano axioms

# Background

We are going to be “formal, mas informal” . . .

. . . assuming an operational amount of second order logic (Siefkes, 1970).

# Structures

**Definition:** A structure is a triple $\langle N, z, s \rangle$, where:

1. $N$ is a set.
2. $z \in N$.
3. $s : N \to N$ is a function.

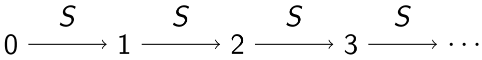
(a) $\mathcal{N}_1 = \langle \mathbb{N}, 0, S \rangle$ is the standard structure.

(b) $\mathcal{N}_2 = \langle \{a\}, a, f \rangle$, where $f(a) = a$ is a structure.

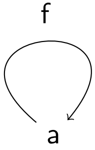
(c) $\mathcal{N}_3 = \langle \{b, c\}, b, g \rangle$, where $g(b) = g(c) = c$ is a structure.

# Examples of structures

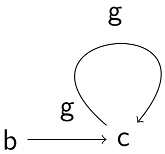
$\mathcal{N}_1$ :




$\mathcal{N}_2$ :




$\mathcal{N}_3$ :



# Dedekind Peano-Structures

**Definition:** Let $\mathcal{N} = \langle N, z, s \rangle$ be a structure.
We say that $\mathcal{N}$ is a DP-structure if it satisfies the following axioms:

Zer. $\forall x \in N[s(x) \neq z]$.

Inj. $\forall x, y \in N[s(x) = s(y) \rightarrow x = y]$.

Ind. $\forall X \subseteq N\{z \in X \wedge \forall y \in N[y \in X \Rightarrow s(y) \in X] \Rightarrow \forall z \in N[z \in X]\}$

# Examples and counterexamples of DP-structures

$\mathcal{N}_1 \models \mathsf{Zer}, \mathsf{Inj}, \mathsf{Ind}.$
$\mathcal{N}_1$ is a DP-structure.

$\mathcal{N}_2 \not\models \mathsf{Zer}$, $\mathcal{N}_2 \models \mathsf{Inj}$, $\mathcal{N}_2 \models \mathsf{Ind}$.
$\mathcal{N}_2$ is not a DP-structure.

$\mathcal{N}_3 \models \mathsf{Zer}$, $\mathcal{N}_3 \not\models \mathsf{Inj}$, $\mathcal{N}_3 \models \mathsf{Ind}$.
$\mathcal{N}_3$ is not a DP-structure.

# More independences

| Zer | Inj | Ind | |
|---|---|---|---|
| ✓ | ✓ | ✓ | $\langle \mathbb{N}, 0, S \rangle$ |
| ✓ | ✓ | × | $\langle \mathbb{N} \cup \{\sqrt{2}\}, 0, S \cup \{(\sqrt{2}, \sqrt{2})\} \rangle$ |
| ✓ | × | ✓ | $\langle \{a, b\}, a, \{(a, b), (b, b)\}$ |
| ✓ | × | × | $\langle \{a, b, c\}, a, \{(a, b), (b, b), (c, b)\}$ |
| × | ✓ | ✓ | $\langle \{a\}, a, \{(a, a)\}$ |
| × | ✓ | × | $\langle \{a, b, c\}, a, \{(a, b), (b, a), (c, c)\} \rangle$ |
| × | × | ✓ | ?????????? |
| × | × | × | $\langle \{a, b, c\}, a, \{(a, b), (b, a), (c, a)\} \rangle$ |

We found no $\mathcal{N}$ such that $\mathcal{N} \models \neg\mathrm{Zer}, \neg\mathrm{Inj}, \mathrm{Ind}$.

# Induction-Structures

We are interested in the structured where Ind holds.

**Definition:** Let $\mathcal{N} = \langle N, z, s \rangle$ be a structure.
We say that $\mathcal{N}$ is an Ind-structure if $\mathcal{N} \models \mathit{Ind}$.

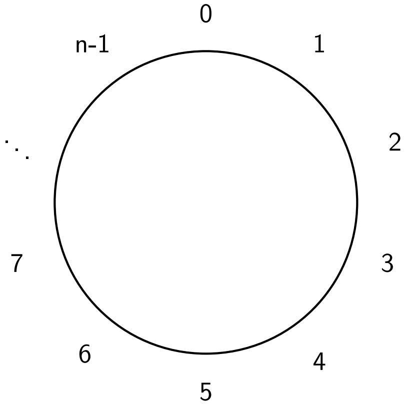
(a) $\mathcal{N} = \langle \mathbb{N}, 0, S \rangle$.

0 1 2 $\cdots$ n $\cdots$

# Induction-Structures

(b) For every $n \in \mathbb{N}$, the structure $\mathcal{N}_n = \langle \{0, 1, 2, \ldots, n-1\}, 0, s \rangle$, where:

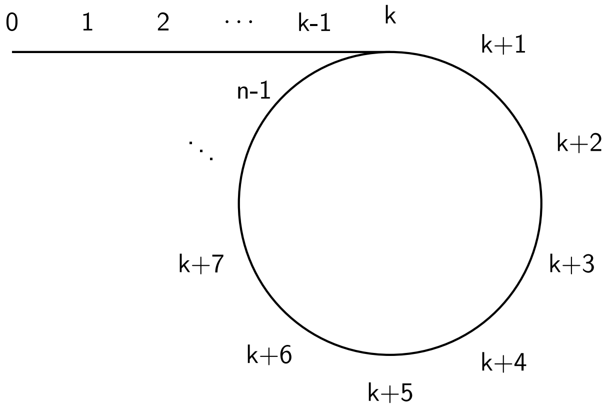
$$s(x) = \begin{cases} x+1 & \text{if } x < n-1 \\ 0 & \text{otherwise.} \end{cases}$$



# Induction-Structures

(c) For all $n, k \in \mathbb{N}$, $1 \leq k \leq n$, the structure $\mathcal{N}_{n,k} = \langle \{0, 1, 2, \ldots, n-1\}, 0, s \rangle$, where:

$$s(x) = \begin{cases} x+1 & \text{if } x < n-1 \\ k & \text{otherwise.} \end{cases}$$



# Intuitive independence

Intuitively, these are the only structures $\mathcal{N} \models \mathsf{Ind}$.

Observe that:

| Zer | Inj | Ind | |
|---|---|---|---|
| ✓ | ✓ | ✓ | $\mathcal{N}$ |
| ✓ | × | ✓ | $\mathcal{N}_{n,k}$ |
| × | ✓ | ✓ | $\mathcal{N}_n$ |
| × | × | ✓ | × |

L.Henkin presented an *algebraic proof* sketch of this fact in 1960.

# Intuitive independence

M. R. Cerioli, H. Nobrega, G. Silveira and P. Viana presenetd an alternative *logical proof* in 2015.

They also presented a set of axioms having examples for all lines of the table on independence.

At least for me, it is interesting that $\neg\mathrm{Zer} \wedge \mathrm{ind}$ is the same as modular arithmetics.

# 3. Iteration

# Iteraction

Intuitively, iteration means
'an operation may be repeated on its result on a given argument any finite number of times'.

Formally, we cannot state interation in this way, because in doing so we are defining 'iteration' using 'repeating any finite number of times on the result of a given argument'.
But the later is the same as the former.

How to scape from this circularity?

# Iteraction

Given a set $A$ and a function $f : A \to A$, an idea is to define the iteration of $f$ "by induction", according to the following clauses:

$$f^0(x) = x$$

$$f^{S(n)}(x) = f(f^n(x))$$

But observe that whereas $f$, $f^0$, and $f^{S(n)}$ (given $f^n$) make sense, $f^n$ do not.
We need to prove it exists!

# Iteration Theorem, first version

**Iteration Theorem (IT1v)**

Let $A$ be a set and $a \in A$.

Then, for every induction structure $\mathcal{N} = \langle N, z, s \rangle$ there is a family of functions $\mathcal{F} = \{f_n : A \to A \mid n \in N\}$ satisfying the following conditions:

1. $f_z(a) = a$.
2. $\forall n \in N[f_{S(n)}(a) = f(f_n(a))]$.

# Attempt of proof for ITfv

*Proof*: First, we define $\mathcal{F}$ "point-wise".

Let $X = \{n \in N : \exists$ an adequate function $f_n$ associated to $n\}$.

For $z$, we take $f_z ::= \mathrm{Id}_A$. So $z \in X$.

Suppose $n \in X$, that is, the adequate function $f_n$ is associated to $n$.

For $S(n)$, we take $f_{S(n)} ::= f \circ f_n$.

Now, we take $\mathcal{F} = \{f_n : n \in N\}$ and prove 1 and 2.

# Where is the mistake?

We have a counter-example.

Take $\mathcal{N}_3 = \langle \{0, 1, 2\}, 0, s \rangle$, where $s(0) = 1$, $s(1) = 2$, and $s(2) = 0$.

Recall that $\mathcal{N}_3 \models \mathsf{Ind}$.

Let $A$ be such that $\{a, b\} \subseteq A$, where $a \neq b$.

Take $f(a) = b$ and $f(b) = a$ (the rest of $f$ does not matter for which follows).

# Where is the mistake?

We have:

$f_0(a) = a$

$f_{s(0)}(a) = f(f_0(a)) = f(a) = b$

$f_{s(s(0))}(a) = f(f_{s(0)}(a)) = f(b) = a$

$f_{s(s(s(0)))}(a) = f(f_{s(s(0))}(a)) = f(a) = b$

But, $f_{s(s(s(0)))}(a) = f_0(a) = a$, a contradiction.

# From iteration to homomorphism

Above, we started with an induction structure $\mathcal{N}_1 = \langle N, z, s \rangle$ and tried to define an adequate family $\mathcal{F} = \{f_n : n \in N\}$.

Now, considering the structure

$$\mathcal{N}_2 = \langle \mathcal{F}, f_z, \mathcal{S} \rangle,$$

where

$$\mathcal{S}(f_n) = f_{s(n)},$$

for every $n \in N$.

We can see the mistaken "proof" above as a tentative of defining a function $h : N \to \mathcal{F}$, such that:

1. $h(z) = f_z$.

2. $\forall n \in N[h(s(n)) = f_{s(n)} = \mathcal{S}(f_n) = \mathcal{S}(h(n))]$.

# The homomorphism theorem, second version

**Homomorphism Theorem, second version (HoT2v)**

Let $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ be a induction structure and $\mathcal{N}_2 = \langle N_2, z_2, s_2 \rangle$ be a structure whatsoever ($s_2$ does not need to behave like a successor function).

Then, there exists a unique function $h : N_1 \to N_2$ satisfying the following conditions:

1. $h(z_1) = z_2$.
2. $\forall n \in N_1 [h(s_1(n)) = s_2(h(n))]$.

That is, there exists a unique homomorphism from $\mathcal{N}_1$ to $\mathcal{N}_2$.

# Attempt of proof for HoT2v

*Proof, second attempt*: Let $X = \{n \in N : h(n) \text{ is defined}\}$.

For $z$, we take $h(z_1) ::= z_2$. So $z \in X$.

Suppose $n \in X$, that is, $h(n)$ is defined.

For $s(n)$, we take $h(s_1(n)) ::= s_2(h(n))$. So, $s(n) \in X$.

Now, by induction, we prove $h$ is defined and $h$ is unique.

# Where is the mistake?

Of course, this proof is also wrong.
The same counterexample works . . .

Whith a slight change (this is a fuzzy concep) in the statement we will have a proper version.

But, first, let us see that the proper HoT gives us what we want.

# From homomorphism to iteration

Given a set $X$, a function $f : X \to X$, and $x \in X$.

Take the canonical structure $\mathcal{N}_1 = \langle \mathbb{N}, 0, S \rangle$ and the structure $\mathcal{N}_2 = \langle X, x, f \rangle$.

By the HoT, there is a unique homomorphism $h_x : \mathbb{N} \to X$ such that $h_x(0) = x$ and $h_x(S(n)) = f(h_x(n))$, for all $n \in \mathbb{N}$.

# From homomorphism to iteration

Now, given a set $A$ and a function $f : A \to A$, the iteration of $f$ on elements of $A$ is the function $F : \mathbb{N} \times A \to A$, defined by

$$F(n, x) = h_x(n),$$

for all $n \in \mathbb{N}$ and $x \in A$.

In fact, given an element $a$ on which want to iterate the applications of $f$, we have:

$F(0, a) = h_a(0) = a$

$F(S(0), a) = h_a(S(0)) = f(h_a(0)) = f(a).$

$F(S(S(0)), a) = h_a(S(S(0))) = f(h_a(S(0))) = f(f(a)).$

And so on ...

# The homomorphism theorem

**Homomorphism Theorem (HoT)**
(Dedekind, 1888)

Let $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ be a DP-strucure and $\mathcal{N}_2 = \langle N_2, z_2, s_2 \rangle$ be a structure whatsoever.

Then, there exists a unique function $h : N_1 \to N_2$ satisfying the following conditions:

1. $h(z_1) = z_2$.
2. $\forall n \in N_1 [h(s_1(n)) = s_2(h(n))]$.

That is, there exists a unique homomorphism from $\mathcal{N}_1$ to $\mathcal{N}_2$.

# Proofs of HoT

Ind warrants the unicity.

To prove the existence, we need Zer and Inj.

# Proofs of HoT

*Proof by "bottom-up"* (Kálmar, 1939):

Let $X \subseteq N_1$.
We say $X$ is a *segment* if $z \in X$ and $\forall n \in N_1[s_1(n) \in X \to n \in X]$.

That is, $X$ contains zero and is closed to predecessor.

Let $H : X \to N_2$.
We say $H$ is a *partial homomorphism* if $X$ is a segment,
$H(z_1) = z_2$, and $\forall n \in N_1[H(s_1(n) = s_2(H(n))]$.

That is, $H$ is a finite approximation of $h$.

# Proofs of HoT

For every $n \in N_1$ there exists a segment $X_n$ and a partial homomorphism $H_n : X_n \to N_2$, such that $n \in X_n$.

That is, we know how to construct finite approximations of $h$ up to any element of $N_1$.
To prove this we need Zer.

If $H_1 : X_1 \to N_2$ and $H_2 : X_2 \to N_2$ are partial homomorphisms, and $n \in X_1 \cap X_2$, then $H_1(n) = H_2(n)$.

That is, new finite approximations do not destroy what we already have acchieved.
To prove this we need Inj.

# Proofs of HoT

Now, define $h : N_1 \to N_2$ by setting for every $n \in N_1$ and $m \in N_2$:

$$h(n) = m \text{ iff } \exists \text{ partial homomorphism } H \text{ such that } H(n) = m$$

We prove that $h$ is well defined, satisfies 1 and 2, and is unique. To prove these we need Ind. □

# Proofs of HoT

*Proof by "top-down"* (P. Lorenzen, 1939):

Let $X \times Y \subseteq N_1 \times N_2$.
We say $X \times Y$ is *regular* if $(z_1, z_2) \in X \times Y$ and
$\forall (x, y) \in N_1 \times N_2 [(x, y) \in X \times Y \to (s_1(x), s_2(y)) \in X \times Y]$.

There are regular sets.

Let $\mathcal{R}$ be a family of regular sets, then $\bigcap \mathcal{R}$ is regular.

Let $h = \bigcap \{X \times Y : X \times Y \text{ is regular}\}$.

# Proofs of HoT

Given $n \in N_1$, we prove that there exists only one $m \in N_2$ such that $(n, m) \in h$.
To prove this we need Zer, Inj, and Ind,

We prove that $h$ satisfies 1 and 2, and that $h$ is unique.
This follows by definition and Ind. $\square$

# 4. The strength of the DP axioms

# The converse of the homomorphism theorem

The strength of Zer $\wedge$ Inj $\wedge$ Ind is given by:

**The Converse of the Homomorphism Theorem (CHoT)**

Let $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ be a structure whatsoever.

Then, the following conditions are equivalent:

(a) $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ is a DP-strucure.

(b) For every structure $\mathcal{N}_2 = \langle N_2, z_2, s_2 \rangle$, there exists a unique function $h : N_1 \to N_2$ satisfying the following conditions:

1. $h(z_1) = z_2$.
2. $\forall n \in N_1 [h(s_1(n)) = s_2(h(n))]$.

# The converse of the homomorphism theorem

That is . . .

$\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ is a DP-strucure.
iff
it satisfies the Homomorphism Theorem.

This is a categorical (in the sense of category theory) characterization of $\langle \mathbb{N}, 0, S \rangle$ (Lawvere, 1965).

# Proof of CHoT

Let us skip the proofs of Zer and Inj.

To prove Ind, let $X \subseteq N_1$ be good.

Let $Y = N_1 \setminus X$.
Suppose, for RA, that $Y \neq \emptyset$.

Let $Z$ be such that $N_1 \cap Z = \emptyset$ and there is a bijection $b : Y \to Z$.

Let $\mathcal{N}_2 = \langle X \cup Y \cup Z, z_1, T \rangle$, where $T$ is defined by:

$$T(x) = \begin{cases} s_1(x) & \text{if } x \in N_1 \\ b(s_1(y)) & \text{if } x \in Z, b(y) = x, \text{ and } s_1(y) \in Y \\ s_1(y) & \text{if } x \in Z, b(y) = x, \text{ and } s_1(y) \in X. \end{cases}$$

# A characterization of Ind-structures

The strength of Ind is given by:

**Characterization of Ind-structures (CIS)**

Let $\mathcal{N}_2 = \langle N_2, z_2, s_2 \rangle$ be a structure whatsoever.

Then, the following conditions are equivalent:

(a) $\mathcal{N}_2 = \langle N_2, z_2, s_2 \rangle$ is a Ind-strucure.

(b) For every DP-structure $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$, there exists a surjective function $h : N_1 \to N_2$ satisfying the following conditions:

1. $h(z_1) = z_2$.
2. $\forall n \in N_1 [h(s_1(n)) = s_2(h(n))]$.

□

# A characterization of Ind-structures

That is . . .

$\mathcal{N}_2 = \langle N_2, z_2, s_2 \rangle$ is a Ind-strucure.
iff
it is the homomorphic image of a DP-structures.

# Proof of CIS

($\Longrightarrow$) Let $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ be a DP-structure.

By HoT, there exists a unique homomorphism $h : N_1 \to N_2$.

We prove that $Y = \{y \in N_2 : \exists x \in N_1 \text{ such that } h(x) = y\}$ is good.

Hence, by Ind, $N_2 = Y$, that is, $h$ is surjective.

# Proof of CIS

($\Longleftarrow$) Let $\mathcal{N}_1 = \langle N_1, z_1, s_1 \rangle$ be a DP-structure and $h : N_1 \rightarrow N_2$ be a surjective homomorphism.

Let $Y \subseteq N_2$ be a good set.
We want to prove that $N_2 \subseteq Y$.

To this, consider $X = \{x \in N_1 : h(x) \in Y\}$.

We prove, by Ind and $Y$ is good, that $X = N_1$.

Hence, for every $x \in N_1$, we have $h(x) \in Y$, that is Ran(h) $\subseteq Y$.

Now, since $h$ is surjective, $N_2 \subseteq Y$. $\square$

# A characterization of infinite sets

The strength of $\mathrm{Zer} \wedge \mathrm{Inj}$ is given by:

**A characterization of infinite sets**

Let $X$ be a set.

Then, the following conditions are equivalent (Dedekind, 1888):

(a) $X$ is infinite.

(b) There is a proper subset $Y \subset X$ and a function $b : X \to Y$ such that $b$ is a bijection.

# A characterization of infinite sets

This is exactly what Zer and Inj are saying.

Given $\langle N, z, s \rangle \models \text{Zer} \wedge \text{Inj}$,
take $X = N$, $Y = \text{Ran}(s)$, and $b = s$.

Zer warrants Y is a proper subset of $X$ and Inj warrants $s$ is bijective.

# 5. Recursion

# Primitive Recursion

Intuitively, primitive recursion means
'the value of a function $f$ at an argument $n$ is defined by using its value at the previous argument $n-1$.

So, iteration is a kind of recursion:

$$f(s(n)) = f(f(n)).$$

We define $f(s(n))$ using $f(n)$.

# Recursion in Ind-structures

Not all recursion is possible in Ind-structures.
But some are . . .

**Recursion in Ind-strutures (RIS)**

Let $\mathcal{N} = \langle N, z, s \rangle$ be an Ind-structure and $x \in N$.

Then, there exists a unique function $h_x : N \to N$ satisfying the following conditions:

1. $h_x(z) = x$.
2. $\forall n \in N[h_x(s(n)) = s(h_x(n))]$.

That is, whereas almost no iteration of 'external functions' is possible, iteration of $s$ still is possible!

# Proof of RIS

*Proof* (Kálmar, before 1939):

Let $X = \{x \in N \mid \exists f_x : N \to N$ satisfying 1 and 2$\}$.

For $z$, take $f_z : N \to N$ such that $f_z(x) = z$, for every $x \in N$.

We prove that $f_z$ satisfies 1 and 2.
So, $z \in X$.

# Proofs of RIS

Suppose $n \in X$.
So, $\exists f_n : N \to N$ satisfying 1 and 2.

For $S(n)$, take $f_{S(n)} = s \circ f_n$.
We prove that $f_{S(n)}$ satisfies 1 and 2.
So, $S(n) \in X$.

Now, by induction, we can proof that, $h_x$ exists and is unique, for every $n \in N$. □

# Recursion in Ind-structures

From RIS we can prove that every Ind-structure has an operation of addition.

**Addition in Ind-Structures (AIS)**

For every Ind-structure $\langle N, z, s\rangle$ there is a unique binary operation $+ : N \times N \to N$, such that, for all $x, y \in N$:

$$\begin{aligned} x + z &= x \\ x + s(y) &= s(x + y). \end{aligned}$$

Just take $x + y = f_x(y)$.

# Recursion in Ind-structures

Besides, from RIS we can prove that every Ind-structure has an operation of multiplication.

**Multiplication in Ind-Structures (MIS)**

For every Ind-structure $\langle N, z, s \rangle$ there is a unique binary operation $\times : N \times N \to N$, such that, for all $x, y \in N$:

$$\begin{array}{rcl} x \times z & = & z \\ x \times s(y) & = & (x \times y) + x. \end{array}$$

*Idea of proof*: For $z$, we take $g_z(x) = z$.
Given $g_x$, for $s(x)$, we take $g_{s(x)} = g_x(y) + x$.
By induction, we prove $\times$ is well defined and unique.

# Recursion in Ind-structures

Now, the natural question is whether we can prove that every Ind-structure has an operation of exponentiation.

**Tentative of exponentiation in Ind-Structures**

For every Ind-structure $\langle N, z, s \rangle$ there is a unique binary operation $\curlywedge : N \times N \to N$, such that, for all $x, y \in N$:

$$\begin{array}{lcl} x \curlywedge z & = & s(z) \\ x \curlywedge s(y) & = & (x \curlywedge y) \times x. \end{array}$$

# Recursion in Ind-structures

But this is false.

Take $\langle\{0,1\},0,s\rangle$, where $0 \neq 1$, $s(0) = 1$, and $s(1) = 0$.

We have:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\times$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Besides, $0 \curlywedge 0 = 0 \curlywedge s(1) = s(0 \curlywedge 0) \times 1 = 1 \times 1 = 1$.

Moreover, $0 \curlywedge 0 = s(1) \curlywedge 0 = s(1) = 0$, a contradiction.

# Recursion in Ind-structures

It seems that no Ind-structure of the form $\mathcal{N}_n$, with $n \geq 2$, have an exponentiation.

But this is false.

**Exponentiation in Ind-Structures $\mathcal{N}_n$ (EIS)**

For every Ind-structure $\mathcal{N}_n$, the following are equivalent:

(a) $\mathcal{N}_n$ has an operation of exponentiation.

(b) $n = 1, 2, 6, 42$ and $1806$.

# Proof of RIS

*Sketch of Proof*: (Dyer-Bennet, 1940)

If $p$ is prime, and $p^2|n$, then $\mathcal{N}_n$ has no exponentiation.

If $p$ is prime, $p|n$, but $p-1 \not| n$, then $\mathcal{N}_n$ has no exponentiation.

If $n = p_1 \times p_2 \times \cdots \times p_k$, $p_i$ prime, $p_i \neq p_j$, and $p_i - 1|n$, then $\mathcal{N}_n$ has exponentiation.

Using these, we can prove that $\mathcal{N}_n$ has exponentiation iff $n = 1, 2, 6, 42$ and $1806$.

# Proof of RIS

We have:

$$1$$

$$1 \times 2$$

$$1 \times 2 \times 3$$

$$1 \times 2 \times 3 \times 7$$

$$1 \times 2 \times 3 \times 7 \times 43$$

Observe that $2 = 1 + 1$, $3 = (1 \times 2) + 1$, $7 = (1 \times 2 \times 3) + 1$, and $43 = (1 \times 2 \times 3 \times 7) + 1$.

After that, $(1 \times 2 \times 3 \times 7 \times 43) + 1 = 1.806$ that is not a prime number. $\square$

# 6. Well ordering

# Caution !!!

This part still needs a lot of work.

If you pass this point, you should be warned that, in my opinion, the text that follows only provides a remote indication of the relationship between induction and well order.

# Well ordering

Intuitively, well ordering means
'the order is linear and there is no strictly decrescent sequences'.

Formally, we cannot state the definition in this way, because in doing so we were talking on sequences, that is, we were defining 'well ordering' using 'natural number', and, as a last resource, the DP-axioms.
But we want compare the logical strength of 'well ordering' and 'mathematical induction'.

How to scape from this circularity?

# Well ordering

First, observe that (usual) induction talks on a unary operation, $s$.

Whereas well ordering talks on a binary relation, $R$.

We will left some very important discussion on transitive closure and fixed points out and unify the language.

# PMI($\leq$)

We denote by $\leq$ the usual ordering on the set of natural numbers.

The Principle of Mathematical Induction on $\leq$, PMI($\leq$), states that:

(1) any subset $X$ of the set of natural numbers

(2) that contains a natural number $x$

(3) whenever it contains every natural number $y$ strictly less than $x$

(4) must contain all natural numbers.

# PMI($\leq$)

In logical symbols, PMI($\leq$) can be written as:

$$\underbrace{\forall X}_{(1)} \{\underbrace{\forall x[\forall y(y \leq x \land y \neq x \to y \in X)}_{(3)} \to \underbrace{x \in X}_{(2)}] \to \underbrace{\forall z(z \in X)}_{(4)}\}.$$

(1) any subset $X$ of the set of natural numbers
(2) that contains a natural number $x$
(3) whenever it contains every natural number $y$ strictly less than $x$
(4) must contain all natural numbers.

# WOP

The Principle of Well Ordering, WOP, states that

(1) any subset $X$ of the set of natural numbers

(2) which is nonempty

(3) has a least element according to $\leq$.

# WOP

In logical terms, PBO can be symbolized as:

$$\underbrace{\forall X}_{(1)} \{\underbrace{\exists x(x \in X)}_{(2)} \rightarrow \underbrace{\exists y[y \in X \wedge \forall z(z \in X \rightarrow y \leq z)]}_{(3)}\}.$$

(1) any subset $X$ of the set of natural numbers
(2) which is nonempty
(3) has a least element according to $\leq$.

# PMI($\leq$) $\times$ WOP

PMI($\leq$) and WOP are not logically equivalent . . .

but are arithmetically equivalent.

We present a proof of this equivalence that is 90% based on logic and 10% in arithmetic.

# PMI $\implies$ WOP

Since $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$:

$$\forall X\{\forall x[\forall y(y \leq x \wedge y \neq x \to y \in X) \to x \in X] \to \forall z(z \in X)\}$$

gives us

$$\forall X\{\neg\forall z(z \in X) \to \neg\forall x[\forall y(y \leq x \wedge y \neq x \to y \in X) \to x \in X]\}.$$

Since $\neg\forall v\varphi \equiv \exists v\neg\varphi$, this gives us:

$$\forall X\{\exists z\neg(z \in X) \to \exists x\neg[\forall y(y \leq x \wedge y \neq x \to y \in X) \to x \in X]\}.$$

# PMI $\Longrightarrow$ WOP

Since $\neg(\varphi \rightarrow \psi) \equiv \varphi \wedge \neg\psi$, this gives us:

$$\forall X\{\exists z\neg(z \in X) \rightarrow \exists x[\forall y(y \leq x \wedge y \neq x \rightarrow y \in X) \wedge \neg(x \in X)]\}.$$

Since $\varphi \wedge \psi \equiv \psi \wedge \varphi$, this gives us:

$$\forall X\{\exists z\neg(z \in X) \rightarrow \exists x[\neg(x \in X) \wedge \forall y(y \leq x \wedge y \neq x \rightarrow y \in X)]\}.$$

# PMI $\Longrightarrow$ WOP

Since $\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi$, this gives us:

$$\forall X\{\exists z \neg(z \in X) \rightarrow \exists x[\neg(x \in X) \wedge \forall y(\neg(y \in X) \rightarrow \neg(y \leq x \wedge y \neq x))]\}.$$

Since $\neg(\varphi \wedge \psi) \equiv (\neg\varphi) \vee (\neg\psi)$, this gives us:

$$\forall X\{\exists z \neg(z \in X) \rightarrow \exists x[(\neg x \in X) \wedge \forall y((\neg y \in X) \rightarrow (\neg y \leq x \vee \neg y \neq x))]\}.$$

# PMI $\Longrightarrow$ WOP

Since $y \neq x \equiv \neg y = x$ and $\neg\neg\varphi \equiv \varphi$, this gives us:

$\forall X\{\exists z \neg(z \in X) \rightarrow \exists x[(\neg x \in X) \wedge \forall y((\neg y \in X) \rightarrow (\neg y \leq x \vee y = x))]\}$.

Now, by arithmetic we have $\neg y \leq x \equiv x < y$.

So, this gives us:

$\forall X\{\exists z \neg(z \in X) \rightarrow \exists x[(\neg x \in X) \wedge \forall y((\neg y \in X) \rightarrow (x < y \vee y = x))]\}$.

This last, because $x \leq y \equiv x < y \vee y = x$, gives us:

$\forall X\{\exists z \neg(z \in X) \rightarrow \exists x[(\neg x \in X) \wedge \forall y((\neg y \in X) \rightarrow (x \leq y))]\}$.

# PMI $\Longrightarrow$ WOP

Now, to prove PMI($\leq$) $\Rightarrow$ PBO, suppose PMI($\leq$), take a subset $X$ of the natural numbers and apply the equivalence above to $\overline{X}$, the complement of $X$, to obtain:

$$\exists z \neg (z \in \overline{X}) \to \exists x[(\neg x \in \overline{X}) \wedge \forall y((\neg y \in \overline{X}) \to (x \leq y))].$$

But, since by logic and set theory, $\neg v \in \overline{V} \equiv v \in V$, we have:

$$\exists (z \in X) \to \exists x[x \in X \wedge \forall y(y \in X \to x \leq y)].$$

Since $X$ is arbitrary, by a renaming of variables, we are done.

# PMI $\Longrightarrow$ WOP

Analogously, to prove PBO $\Rightarrow$ PMI($\leq$).

So, there is no point in considering the equivalence between PMI and WOP under the DP-axioms.

# Well foundeness

If we are considering Ind-structures which are not DP-structures, we can not impose linear ordering.

Neither $\mathcal{N}_n$ nor $\mathcal{N}_{n,k}$ possesses a linear ordering compatible with $s$.

We need a more liberal concept ...

Let $R$ be a binary relation on $N$.
We say that $R$ is well-founded on $N$ if

$$\forall X \subseteq N \{ \forall x \in N [x \in X \to \exists y \in N (xRy \wedge y \in X) \to X = \emptyset)].$$

## Well foundness

Second, Ind-structures and well founded sets are mathematical objects of different types.

- Mathematical induction uses a unary operation $s$.
- Well founding uses a binary relation $R$.

We need a more liberal notion of Ind-structure . . .

Let $R$ be a binary relation on $N$.
We say that $R$ admits induction on $N$ if

$$\forall X \subseteq N\{\forall x \in N[\forall y \in N(yRx \rightarrow y \in X) \rightarrow x \in X] \rightarrow \forall z(z \in X)\}.$$

# Well foundeness

To finish I will stop to present the details, and state the results I intend to cover in a next opportunity . . .

If we consider $\exists y \in N(xRy \wedge y \in X)$ as a binary operation on relations and sets, we do not need to consider the full negation in the metalanguage, and we have:

1. $R$ admits induction on $N \Longrightarrow R$ is well founded on $N$;
2. $R$ is well founded on $N \not\Longrightarrow R$ admits induction on $N$;
3. If we have negation on the metalanguage, $R$ admits induction on $N \Longleftrightarrow R$ is well founded on $N$.