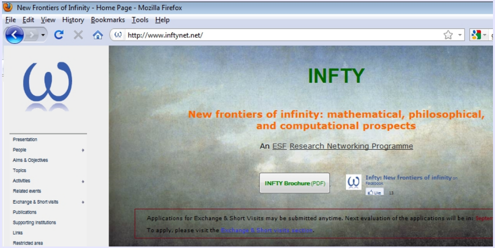
Basic set-theoretic techniques in logic
Part III, Transfinite recursion and induction

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI 2011, Ljubljana, Slovenia

Both the workshop *Modern Set Theory: Foundations & Applications* and the foundational course *Ordinals and Cardinals: Basic set-theoretic techniques in logic* are generously funded by the European Science Foundation in the research networking programme INFTY.



http://www.math.uni-hamburg.de/home/loewe/INFTY@ESSLLI2011/

Today...

$$\aleph_0 < \aleph_1 < \aleph_2 < \dots$$

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$$

1. Mirna's question: how do you construct an uncountable ordinal?
2. The Continuum Hypothesis
3. Induction and Recursion on $\mathbb{N}$
4. Transfinite Induction and Recursion
5. A few applications

Reminder (1).

Two equivalence relations:

- $|X| = |Y|$: X and Y are equinumerous; i.e., there is a bijection between X and Y.
- $(X, R) \simeq (Y, S)$: (X, R) and (Y, S) are isomorphic as ordered structures; i.e., there is an order-preserving bijection between X and Y.

The cardinalities are the equivalence classes of the equivalence relation of being equinumerous; the ordinals are the equivalence classes of being order-isomorphic.

Note that if $(X, R) \simeq (Y, S)$, then $|X| = |Y|$. The converse doesn't hold: $|\omega + 1| = |\omega|$, but $\omega + 1 \not\simeq \omega$. We called an ordinal κ a cardinal if for all $\alpha < \kappa$, we have $|\alpha| < |\kappa|$.

Reminder (2).

A structure (X, R) was called a wellorder if (X, R) is a linear order and every nonempty subset of X has an R-least element.

Proposition. The following are equivalent for a linear order (X, R):

1. (X, R) is a well-order, and
2. there is no infinite R-descending sequence, i.e., a sequence $\{x_i; i \in \mathbb{N}\}$ such that for every i, we have $x_{i+1} R x_i$.

Proof. "1⇒2". If $X_0 := \{x_i; i \in \mathbb{N}\}$ is an R-descending sequence, then X_0 is a nonempty subset of X without R-least element.

"2⇒1". Let $Z \subseteq X$ be a nonempty subset without R-least element. Since it is nonempty, there is a $z_0 \in Z$. Since it has no R-least element, for each $z \in Z$, the set $B_z := \{x \in Z; xRz\}$ is nonempty.

For each z, pick an element $b(z) \in B_z$. Now define by recursion $z_{n+1} := b(z_n)$. The defined sequence $\{z_n; n \in \mathbb{N}\}$ is R-descending by construction. q.e.d.

Mirna's question: how do you construct an uncountable ordinal?

Hartogs' Theorem. If X is a set, then we can construct a well-order (Y, R) such that $|Y| \not\leq |X|$.

We'll prove the special case of $X = \mathbb{N}$ and thus prove that there is an uncountable ordinal:

Consider

$$H := \{(X, R)\ ;\ X \subseteq \mathbb{N} \text{ and } (X, R) \text{ is a wellorder}\}.$$

We can order H by

$(X, R) \prec (Y, S)$
iff (X, R) is isomorphic to a proper initial segment of (Y, S).

How do you construct an uncountable ordinal? (2)

$$H := \{(X, R)\ ;\ X \subseteq \mathbb{N} \text{ and } (X, R) \text{ is a wellorder}\}.$$

$(X, R) \prec (Y, R)$ iff (X, R) is isomorphic to a proper initial segment of (Y, S).

1. $(H, \prec)$ is a linear order.
2. $(H, \prec)$ is a wellorder.
3. H is closed under initial segments: if $(X, R) \in H$ and $(Y, R{\upharpoonright}Y)$ is an initial segment of (X, R), then $(Y, R{\upharpoonright}Y) \in H$. So in particular, if α is the order type of some element of H, then the order type of $(H, \prec)$ must be at least α.
4. If α is the order type of some element of H, then $\alpha + 1$ is.

Claim. H cannot be countable.

In fact, we have *constructed* a wellorder of order type ω_1.

The continuum hypothesis

- $\aleph_1$ is the least cardinal greater than $\aleph_0$.
- $\mathfrak{c}$ is the cardinality of the real line $\mathbb{R}$.
- It is not obvious at all that there is **any** relation between $\aleph_1$ and $\mathfrak{c}$, as we do not know whether there is a cardinal that is equinumerous to $\mathbb{R}$ (see the Thursday lecture).
- If we assume that $\mathfrak{c}$ is a **cardinal** and not just a cardinality, then we know that $\mathfrak{c} \geq \aleph_1$ since cardinals are linearly ordered.
- Cantor conjectured (in 1877) that in fact $\mathfrak{c} = \aleph_1$. This statement is called **the Continuum Hypothesis** (CH).
- CH was the first problem on the famous Hilbert list (1900).
- In 1938, Kurt Gödel proved that there is a model of set theory in which CH holds.
- In 1963, Paul Cohen proved that you cannot prove CH. In fact, for any $n \geq 1$, the statement $\mathfrak{c} = \aleph_n$ is consistent. With a few exceptions (e.g., $\aleph_\omega$), $\mathfrak{c}$ can be any $\aleph_\alpha$.

Induction on the natural numbers (1).

The induction principle (IP).

Suppose $X \subseteq \mathbb{N}$. If

- $0 \in X$, and
- $n \in X$ implies $n + 1 \in X$,

then $X = \mathbb{N}$.

Example. The proof of "There are countably many polynomials with integer coefficients":

$$P = P_1 \cup P_2 \cup P_3 \cup \ldots$$

If we can show that each P_i is countable, then P is countable as a countable union of countable sets.

Define

$$X := \{n \ ; \ P_{n+1} \text{ is countable}\}$$

Induction on the natural numbers (2).

$$X := \{n \ ; \ P_{n+1} \text{ is countable}\}$$

$0 \in X$. An element of P_1 is of the form $ax + b$ for $a, b \in \mathbb{Z}$, so $|P_1| = \mathbb{Z} \times \mathbb{Z}$. Thus P_1 is countable, and $0 \in X$.

if $n \in X$, then $n + 1 \in X$. Suppose $n \in X$, that means that P_{n+1} is countable. Take an element of P_{n+2}. That is of the form

$$a_{n+2}x^{n+2} + a_{n+1}x^{n+1} + a_n x^n + \ldots + a_0 = a_{n+2}x^{n+2} + p$$

for some $p \in P_{n+1}$. So, $|P_{n+2}| = |\mathbb{Z} \times P_{n+1}|$, and thus (because P_{n+1} was countable), P_{n+2} is countable.

The induction principle now implies that $X = \mathbb{N}$, and this means that P_n is countable for all n.

The least number principle.

The least number principle (LNP).

Every nonempty subset of $\mathbb{N}$ has a least element.

This means: $(\mathbb{N}, <)$ is a wellorder.

(Meta-)Theorem. If LNP holds, then IP holds.

Proof. Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \mathbb{N}$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n+1 \in X$.

Consider $Y := \mathbb{N} \backslash X$. Since $X \neq \mathbb{N}$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n+1$ for some $n \in \mathbb{N}$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n+1 \in X$, but that's a contradiction to our assumption. q.e.d.

Recursion on the natural numbers (1).

The recursion principle (RP).

Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function and $n_0 \in \mathbb{N}$. Then there is a unique function $F : \mathbb{N} \to \mathbb{N}$ such that

- $F(0) = n_0$, and
- $F(n+1) = f(F(n))$ for any $n \in \mathbb{N}$.

Two ways to define addition and multiplication on the natural numbers:

1. "cardinal-theoretic": $n + m$ is the unique natural number k such that any set that is the disjoint union of a set of n elements with a set of m elements has k elements.
2. "recursive": Fix n. Define a function addto_n by recursion ("Grassmann equalities"):

$$\mathrm{addto}_n(0) := n, \text{ and}$$
$$\mathrm{addto}_n(m+1) := \mathrm{addto}_n(m) + 1.$$

Define $n + m := \mathrm{addto}_n(m)$.

Recursion on the natural numbers (1).

The recursion principle (RP).

Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function and $n_0 \in \mathbb{N}$. Then there is a unique function $F : \mathbb{N} \to \mathbb{N}$ such that

- $F(0) = n_0$, and
- $F(n+1) = f(F(n))$ for any $n \in \mathbb{N}$.

Is RP obvious?

No, since the recursion equations are not an allowed form of definition: in the definition of the objection F, you are referring to F itself.

Proof. We'll prove RP from IP.

What do we have to prove? We need to give a concrete definition of F, i.e., a formula $\varphi(n, m)$ that holds if and only if $F(n) = m$.

Recursion on the natural numbers (2).

Preliminary work:

If $g : \{0, ..., m\} \to \mathbb{N}$ is a function such that

- $g(0) = n_0$, and
- $g(n+1) = f(g(n))$ for any $n < m$,

we call it a germ of length m.

1. The function $g_0 : \{0\} \to \mathbb{N}$ defined by $g_0(0) := n_0$ is a germ of length 0.
2. If g is a germ of length m and $k < m$, then $g \restriction \{0, ..., k\}$ is a germ of length k.
3. If g is a germ of length m, then the function g^* defined by

$$g^*(k) := \begin{cases} g(k) & \text{if } k \leq m, \\ f(g(m)) & \text{if } k = m+1. \end{cases}$$

   is a germ of length $m+1$.
4. For every $n \in \mathbb{N}$, there is a germ of length n.
5. If g, h are germs of length n, then $g = h$.

Recursion on the natural numbers (3).

(RP) Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function and $n_0 \in \mathbb{N}$. Then there is a unique function $F : \mathbb{N} \to \mathbb{N}$ such that

- $F(0) = n_0$, and
- $F(n+1) = f(F(n))$ for any $n \in \mathbb{N}$.

What do we have to prove? We need to give a concrete definition of F, i.e., a formula $\varphi(n, m)$ that holds if and only if $F(n) = m$.

We have proved that for every $n \in \mathbb{N}$, there is a unique germ of length n, let's call it g_n. Here is our definition of F:

$$\varphi(n, m) \iff m = f(g_n(n)).$$

Counting beyond infinity.

We have defined the ordinals (essentially) as wellorders, i.e., sets that satisfy what we called the least number principle. For $\mathbb{N}$, we showed that LNP implies IP, so maybe we can prove a transfinite induction principle?

First attempt at a transfinite induction principle.

Suppose α is an ordinal and $X \subseteq \alpha$. If

- $0 \in X$, and
- $\beta \in X$ implies $\beta + 1 \in X$,

then $X = \alpha$.

Can this be true? Let $\alpha = \omega + 1 = \{0, 1, 2, 3, ..., 2011, ..., \omega\}$ and consider $X = \{0, 1, 2, 3, ..., 2011, ...\}$. Then X satisfies the two conditions in the induction principle, but $X \neq \omega + 1$.

So, our first attempt didn't work.

That's strange...

We proved that LNP implies IP (for $\mathbb{N}$) and all ordinals satisfy LNP, so why don't they also satisfy IP?

We need to analyse what goes wrong in our proof in the case of $\omega + 1$ and X:

Proof of "LNP implies IP".

Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \mathbb{N}$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n + 1 \in X$.

Consider $Y := \mathbb{N} \backslash X$. Since $X \neq \mathbb{N}$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \mathbb{N}$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

That's strange...

We proved that LNP implies IP (for $\mathbb{N}$) and all ordinals satisfy LNP, so why don't they also satisfy IP?

We need to analyse what goes wrong in our proof in the case of $\omega + 1$ and X:

Proof of "LNP implies IP".

Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \omega + 1$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n + 1 \in X$.

Consider $Y := \omega + 1 \backslash X$. Since $X \neq \omega + 1$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \omega + 1$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

That's strange...

We proved that LNP implies IP (for $\mathbb{N}$) and all ordinals satisfy LNP, so why don't they also satisfy IP?

We need to analyse what goes wrong in our proof in the case of $\omega + 1$ and X:

Proof of "LNP implies IP".

Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \omega + 1$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n + 1 \in X$.

Consider $Y := \omega + 1 \backslash X$. Since $X \neq \omega + 1$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \omega + 1$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

Successor ordinals and limit ordinals.

We say that an ordinal α is a successor ordinal if there is some β such that $\alpha = \beta + 1$. If that is not the case, then α is called a limit ordinal.

Examples.

$$1 = 0 + 1$$
$$17 = 16 + 1$$
$$2001 = 2010 + 1$$
$$\omega + 17 = (\omega + 16) + 1$$

But ω, $\omega + \omega$, $\omega + \omega + \omega$, and also ω_1, ω_2 etc. do not have this property, and thus are limit ordinals.

Transfinite induction (1).

Transfinite induction principle.

Suppose α is an ordinal and $X \subseteq \alpha$. If

- $0 \in X$,
- $\beta \in X$ implies $\beta + 1 \in X$, and
- if $\lambda < \alpha$ is a limit ordinal and for all $\beta < \lambda$, we have $\beta \in X$, then $\lambda \in X$,

then $X = \alpha$.

Transfinite induction (2).

Proof of TIP. Suppose α is an ordinal, i.e., wellordered, but TIP doesn't hold. So, there is some $X \neq \alpha$ satisfying the conditions of TIP, i.e.,

- $0 \in X$,
- $\beta \in X$ implies $\beta + 1 \in X$, and
- if $\lambda < \alpha$ is a limit ordinal and for all $\beta < \lambda$, we have $\beta \in X$, then $\lambda \in X$.

Consider $Y := \alpha \backslash X$. Since $X \neq \alpha$, this is a nonempty set. By the fact that α is wellordered, it has a least element, let's call it y_0.

The element y_0 has to be either a successor or a limit ordinal. If it is a successor, then $y_0 = \beta + 1$ for some $\beta \in X$, but then $y_0 \in X$. If it is a limit, then all of its predecessors are in X, and thus $y_0 \in X$. This gives the desired contradiction. q.e.d.

Transfinite recursion.

Suppose that α is an ordinal. We call a function $s : \beta \to \mathrm{Ord}$ a segment if $\beta < \alpha$. Suppose that you have an ordinal α_0, a function $f : \mathrm{Ord} \to \mathrm{Ord}$ and a function g assigning an ordinal to every segment.

Then there is a unique function $F : \alpha \to \mathrm{Ord}$ such that

1. $F(0) = \alpha_0$,
2. $F(\beta + 1) = f(F(\beta))$, if $\beta + 1 \in \alpha$, and
3. $F(\lambda) = g(F \restriction \lambda)$ if $\lambda \in \alpha$ is a limit ordinal.

The proof is a homework exercise.

Global version of transfinite recursion.

Suppose that you have an ordinal α_0, a function $f : \mathrm{Ord} \to \mathrm{Ord}$ and a function g assigning an ordinal to every segment.

Then there is a unique set operation $F : \mathrm{Ord} \to \mathrm{Ord}$ such that

1. $F(0) = \alpha_0$,
2. $F(\beta + 1) = f(F(\beta))$, for every β, and
3. $F(\lambda) = g(F{\restriction}\lambda)$ if λ is a limit ordinal.

First application:

$$\begin{aligned} \aleph_0 &:= \omega, \\ \aleph_{\beta+1} &:= \text{the least ordinal } \gamma \text{ such that } |\aleph_\beta| < |\gamma|, \\ \aleph_\lambda &:= \text{the least ordinal } \gamma \text{ such that } |\aleph_\beta| < |\gamma| \text{ for all } \beta < \lambda. \end{aligned}$$

$$\begin{aligned} \beth_0 &:= \omega, \\ \beth_{\beta+1} &:= |2^{\beth_\beta}| \\ \beth_\lambda &:= \text{the least ordinal } \gamma \text{ such that } |\beth_\beta| < |\gamma| \text{ for all } \beta < \lambda. \end{aligned}$$

Ordinal arithmetic (1).

Two ways to define ordinal addition:

1. "order-theoretic": $\alpha + \beta$ is the unique ordinal corresponding to the wellorder of the disjoint union of α and β where all elements of α precede all elements of β.
2. "recursive": Fix α. Define a function addto_α by recursion:

$$\begin{aligned} \mathrm{addto}_\alpha(0) &:= \alpha, \\ \mathrm{addto}_\alpha(\beta+1) &:= \mathrm{addto}_\alpha(\beta) + 1, \\ \mathrm{addto}_\alpha(\lambda) &:= \text{the least } \gamma \text{ bigger than all } \mathrm{addto}_\alpha(\beta) \text{ for } \beta < \lambda. \end{aligned}$$

   Define $\alpha + \beta := \mathrm{addto}_\alpha(\beta)$.

And based on this, ordinal multiplication:

$$\begin{aligned} \mathrm{mult}_\alpha(0) &:= 0, \\ \mathrm{mult}_\alpha(\beta+1) &:= \mathrm{mult}_\alpha(\beta) + \alpha, \\ \mathrm{mult}_\alpha(\lambda) &:= \text{the least } \gamma \text{ bigger than all } \mathrm{mult}_\alpha(\beta) \text{ for } \beta < \lambda. \end{aligned}$$

$\alpha \cdot \beta := \mathrm{mult}_\alpha(\beta)$.