Natural Numbers and Induction

Ming Hsiung
mingshone@163.com

School of Philosophy and Social Development
South China Normal University

Set Theory, Spring 2022

Outline

Outline

Recall

- $\varnothing$
- $\{\varnothing\}$
- $\{\varnothing, \{\varnothing\}\}$
- $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$
- ......

Example

$$S(x) =_{\text{df}} x \cup \{x\}$$

- 0
- $1 = S(0) = \{0\}$
- $2 = S(1) = \{0, 1\}$
- $3 = S(2) = \{0, 1, 2\}$
- ......

Example

$$S(x) =_{\text{df}} x \cup \{x\}$$

- 0
- $1 = S(0) = \{0\}$
- $2 = S(1) = \{0, 1\}$
- $3 = S(2) = \{0, 1, 2\}$
- ......

Example

$$S(x) =_{\text{df}} x \cup \{x\}$$

- 0
- $1 = S(0) = \{0\}$
- $2 = S(1) = \{0, 1\}$
- $3 = S(2) = \{0, 1, 2\}$
- ......

Example

$$S(x) =_{\text{df}} x \cup \{x\}$$

- 0
- $1 = S(0) = \{0\}$
- $2 = S(1) = \{0, 1\}$
- $3 = S(2) = \{0, 1, 2\}$
- ......

Example

$$S(x) =_{\text{df}} x \cup \{x\}$$

- 0
- $1 = S(0) = \{0\}$
- $2 = S(1) = \{0, 1\}$
- $3 = S(2) = \{0, 1, 2\}$
- ……

The Axiom of Infinity

- Is there any infinite set?
- Answer: the Axiom of Infinity is indpendent of the other axioms of ZFC.
- **The Axiom of Infinity**: There is a set I such that $0 \in I$ and if $x \in I$, then $S(x) \in I$.
- Definition: a set I is called **inductive**, if $0 \in I$ and if $x \in I$, then $S(x) \in I$.

The Axiom of Infinity

- Is there any infinite set?
- Answer: the Axiom of Infinity is indpendent of the other axioms of ZFC.
- **The Axiom of Infinity**: There is a set I such that $0 \in I$ and if $x \in I$, then $S(x) \in I$.
- Definition: a set I is called **inductive**, if $0 \in I$ and if $x \in I$, then $S(x) \in I$.

The Axiom of Infinity

- Is there any infinite set?
- Answer: the Axiom of Infinity is indpendent of the other axioms of ZFC.
- **The Axiom of Infinity**: There is a set I such that $0 \in I$ and if $x \in I$, then $S(x) \in I$.
- Definition: a set I is called **inductive**, if $0 \in I$ and if $x \in I$, then $S(x) \in I$.

The Axiom of Infinity

- Is there any infinite set?
- Answer: the Axiom of Infinity is indpendent of the other axioms of ZFC.
- **The Axiom of Infinity**: There is a set I such that $0 \in I$ and if $x \in I$, then $S(x) \in I$.
- Definition: a set I is called **inductive**, if $0 \in I$ and if $x \in I$, then $S(x) \in I$.

The set $\mathbb{N}$

- Definition: $\mathbb{N} =_{\text{df}} \{x | x \text{ belongs to every inductive set}\}$. The elements of $\mathbb{N}$ are called the natural numbers.
- Formally, $\mathbb{N} =_{\text{df}} \ldots$.
- Fact: $\mathbb{N}$ itself is an inductive set, and it is a subset of every inductive set.

The set $\mathbb{N}$

- Definition: $\mathbb{N} =_{\text{df}} \{x | x \text{ belongs to every inductive set}\}$. The elements of $\mathbb{N}$ are called the natural numbers.
- Formally, $\mathbb{N} =_{\text{df}} \ldots$.
- Fact: $\mathbb{N}$ itself is an inductive set, and it is a subset of every inductive set.

The set $\mathbb{N}$

- Definition: $\mathbb{N} =_{\mathrm{df}} \{x | x \text{ belongs to every inductive set}\}$. The elements of $\mathbb{N}$ are called the natural numbers.
- Formally, $\mathbb{N} =_{\mathrm{df}} \ldots$.
- Fact: $\mathbb{N}$ itself is an inductive set, and it is a subset of every inductive set.

Outline

Induction Principle

- **The Induction Principle:** Let $P(x)$ be a property (possibly with parameters). Assume that
  (a) $P(0)$ holds.
  (b) For all $n \in \mathbb{N}$, $P(n)$ implies $P(S(n))$.

  Then $P(n)$ holds for any $n \in \mathbb{N}$.

Example

- Definition: The relation $<$ on $\mathbb{N}$ is defined by: $m < n$ iff $m \in n$.
- Definition: $m \leq n =_{\text{df}} m \in n \vee m = n$.
- Fact: For any $n \in \mathbb{N}$, $0 \leq n$.

Example

- Definition: The relation $<$ on $\mathbb{N}$ is defined by: $m < n$ iff $m \in n$.
- Definition: $m \leq n =_{\text{df}} m \in n \vee m = n$.
- Fact: For any $n \in \mathbb{N}$, $0 \leq n$.

Example

- Definition: The relation $<$ on $\mathbb{N}$ is defined by: $m < n$ iff $m \in n$.
- Definition: $m \leq n =_{\text{df}} m \in n \vee m = n$.
- Fact: For any $n \in \mathbb{N}$, $0 \leq n$.

- Theorem: $<$ is a linear ordering on $\mathbb{N}$.

Induction Principle, Second Version

- **The Induction Principle, Second Version:** Let $P(x)$ be a property (possibly with parameters). Assume that for $n \in \mathbb{N}$,

$$\text{If } P(k) \text{ holds for all } k < n, \text{ then } P(n).$$

Then $P(n)$ holds for any $n \in \mathbb{N}$.

Well-foundedness

- Definition: A relation R on A is **well-founded**, if for every nonempty subset B of A, there exists a R-minimal element of B, i.e., an element $x \in B$ such that yRx fails for any $y \in B$.
- Fact: A relation R on A is well-founded, iff no elements x_0, x_1, ..., of A can form a decreasing chain, that is, $x_1 R x_0$, $x_2 R x_1$, ...

  Proof. $\Rightarrow$:

  $\Leftarrow$:

  Note: The $\Leftarrow$ side needs to employ the Axiom of Choice (AC). People usually use AC without realizing it!

Well-foundedness

- Definition: A relation R on A is **well-founded**, if for every nonempty subset B of A, there exists a R-minimal element of B, i.e., an element $x \in B$ such that yRx fails for any $y \in B$.
- Fact: A relation R on A is well-founded, iff no elements x_0, x_1, …, of A can form a decreasing chain, that is, $x_1 R x_0$, $x_2 R x_1$, ….

Proof. $\Rightarrow$:

$\Leftarrow$:

Note: The $\Leftarrow$ side needs to employ the Axiom of Choice (AC). People usually use AC without realizing it!

Well-foundedness

- Definition: A relation R on A is **well-founded**, if for every nonempty subset B of A, there exists a R-minimal element of B, i.e., an element $x \in B$ such that yRx fails for any $y \in B$.
- Fact: A relation R on A is well-founded, iff no elements x_0, x_1, …, of A can form a decreasing chain, that is, $x_1 R x_0$, $x_2 R x_1$, ….

  Proof. $\Rightarrow$:

  $\Leftarrow$:

  Note: The $\Leftarrow$ side needs to employ the Axiom of Choice (AC). People usually use AC without realizing it!

Well-foundedness

- Definition: A relation R on A is **well-founded**, if for every nonempty subset B of A, there exists a R-minimal element of B, i.e., an element $x \in B$ such that yRx fails for any $y \in B$.
- Fact: A relation R on A is well-founded, iff no elements x_0, x_1, ..., of A can form a decreasing chain, that is, $x_1 R x_0$, $x_2 R x_1$, ...

  Proof. $\Rightarrow$:

  $\Leftarrow$:

Note: The $\Leftarrow$ side needs to employ the Axiom of Choice (AC). People usually use AC without realizing it!

- Theorem: $<$ is a well-founded relation on $\mathbb{N}$.

Outline

Finite and Infinite Sequences

Informally,

- $a_0, a_1, \ldots, a_{n-1}$ is a sequence of length n.
- $a_0, a_1, \ldots, a_n, \ldots$ is an infinite sequence (of length ω).

Formally,

- A **finite sequence of elements of A** is a function from n to A for some n. n is called the length of this sequence. If $n = 0$, we get the **empty sequence**.
- An (countably) **infinite sequence of elements of A** is a function from $\mathbb{N}$ to A.

Finite and Infinite Sequences

Informally,

- $a_0, a_1, \ldots, a_{n-1}$ is a sequence of length n.
- $a_0, a_1, \ldots, a_n, \ldots$ is an infinite sequence (of length ω).

Formally,

- A **finite sequence of elements of A** is a function from n to A for some n. n is called the length of this sequence. If $n = 0$, we get the **empty sequence**.
- An (countably) **infinite sequence of elements of A** is a function from $\mathbb{N}$ to A.

Finite and Infinite Sequences

Informally,

- $a_0, a_1, \ldots, a_{n-1}$ is a sequence of length n.
- $a_0, a_1, \ldots, a_n, \ldots$ is an infinite sequence (of length ω).

Formally,

- A **finite sequence of elements of A** is a function from n to A for some n. n is called the length of this sequence. If $n = 0$, we get the **empty sequence**.
- An (countably) **infinite sequence of elements of A** is a function from $\mathbb{N}$ to A.

Finite and Infinite Sequences

Informally,

- $a_0, a_1, \ldots, a_{n-1}$ is a sequence of length n.
- $a_0, a_1, \ldots, a_n, \ldots$ is an infinite sequence (of length ω).

Formally,

- A **finite sequence of elements of A** is a function from n to A for some n. n is called the length of this sequence. If $n = 0$, we get the **empty sequence**.
- An (countably) **infinite sequence of elements of A** is a function from $\mathbb{N}$ to A.

Example

- $1, 1, 2, 6, 24, \ldots, 1 \cdot 2 \cdot \ldots \cdot n, \ldots$.
- Explicit Definition: f is a function such that $f(n) = n!$(stipulate: $0! = 1$).
- Implicit Definition: f is a function such that $f(0) = 1$ and $f(S(n)) = f(n) \cdot S(n)$. [1]

[1] This is an example for illustrating the idea of recursion, as we still have not a well-defined notion of multiplication for natural numbers.

Example

- $1, 1, 2, 6, 24, \ldots, 1 \cdot 2 \cdot \ldots \cdot n, \ldots$.
- Explicit Definition: f is a function such that $f(n) = n!$(stipulate: $0! = 1$).
- Implicit Definition: f is a function such that $f(0) = 1$ and $f(S(n)) = f(n) \cdot S(n)$. [1]

[1] This is an example for illustrating the idea of recursion, as we still have not a well-defined notion of multiplication for natural numbers.

Example

- $1, 1, 2, 6, 24, \ldots, 1 \cdot 2 \cdot \ldots \cdot n, \ldots$.
- Explicit Definition: f is a function such that $f(n) = n!$(stipulate: $0! = 1$).
- Implicit Definition: f is a function such that $f(0) = 1$ and $f(S(n)) = f(n) \cdot S(n)$. [1]

[1] This is an example for illustrating the idea of recursion, as we still have not a well-defined notion of multiplication for natural numbers.

Recursion on Natural Numbers

Theorem (The Recursion Theorem)

For any set A*, any* $a \in A$*, and any function* $g : A \times \mathbb{N} \to A$*, there exists a unique function* $f : \mathbb{N} \to A$ *such that*

(a) $f(0) = a$;

(b) $f(S(n)) = g(f(n), n)$ *for all* $n \in \mathbb{N}$.

- Application 1: For every $m \in \mathbb{N}$, there exists a unique function $f_m : \mathbb{N} \to \mathbb{N}$ such that
  (a) $f_m(0) = m$;
  (b) $f_m(S(n)) = S(f_m(n))$ for all $n \in \mathbb{N}$.

Proof.

- Definition.

$$m + n =_{\text{df}} f_m(n).$$

- Thus:
  (a) $m + 0 = m$;
  (b) $m + S(n) = S(m + n)$ for all $m, n \in \mathbb{N}$.

- Prove: $m + 1 = S(m)$

  From now on, we can use $m + 1$ instead of $S(m)$.

Theorem (The Recursion Theorem with parameters)

For any $a : P \to A$ *and any function* $g : P \times A \times \mathbb{N} \to A$*, there exists a unique function* $f : P \times \mathbb{N} \to A$ *such that*

(a) $f(p, 0) = a(p)$;

(b) $f(p, S(n)) = g(p, f(n), n)$ *for all* $n \in \mathbb{N}$ *and* $p \in P$.

- Application 2: There exists a unique function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that
  (a) $f(m, 0) = 0$;
  (b) $f(m, S(n)) = f(m, n) + m$ for all $m, n \in \mathbb{N}$.

Proof.

- Definition.

$$m \cdot n =_{\text{df}} f(m, n).$$

- Thus:
  (a) $m \cdot 0 = m$;
  (b) $m \cdot S(n) = m \cdot n + m$ for all $m, n \in \mathbb{N}$.

- Application 3: There exists a unique function $f : \mathbb{N} \to \mathbb{N}$ such that
  (a) $f(0) = 1$;
  (b) $f(S(n)) = f(n) \cdot n$ for all $n \in \mathbb{N}$.

Proof.

- Definition.

$$n! =_{\text{df}} f(n).$$

- Thus:
  (a) $0! = 1$;
  (b) $(n+1)! = n! \cdot n$ for all $n \in \mathbb{N}$.

Theorem (The Recursion Theorem)

For any set A, any $a \in A$, and any function $g : A \times N \to A$, there exists a unique function $f : \mathbb{N} \to A$ such that

(a) $f(0) = a$;

(b) $f(S(n)) = g(f(n), n)$ *for all* $n \in \mathbb{N}$.

Proof.

Homework

- How to define exponentiation of natural numbers? Justify your definition.
- How to define (by recursion) Fibonacci function $f : \mathbb{N} \to \mathbb{N}$, which meets the condition:

$$\begin{cases} f(0) = 1 \\ f(1) = 1 \\ f(n+2) = f(n+1) + f(n), n \geq 0 \end{cases}$$

Hint: Refer to Hrbaeck & Jech (3 ed.), pp. 50.

Thanks for your attention!

Q & A