Elements of Set Theory

Chapter 4: Natural Numbers

February 4 & 6, 2014

Lecturer: Fan Yang

Every mathematical object can be viewed as a set, or every such object is a set.

In this course, we study the basics of the big project: "embedding mathematics in set theory". In this chapter, we construct Natural Numbers:

$$0, 1, 2, 3, \ldots$$

What exactly are natural numbers??

...An awkward philosophical question... But we do know what we mean by

TWO apples:  

TWO pears:  

TWO-element sets: $\{a, b\}$, $\{\emptyset, \{\emptyset\}\}$, ...

We define natural numbers as suitable sets. Natural numbers are abstract concepts that do not at first glance appear to be sets. Nevertheless, we can construct specific sets that will serve perfectly well as natural numbers.

We take the standard approach (due to von Neumann) and define:

$$\begin{aligned} 0 &:= \emptyset, \\ 1 &:= \{0\} = \{\emptyset\}, \\ 2 &:= \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \\ 3 &:= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\ &\vdots \end{aligned}$$

The idea is to make each natural number be the set of all smaller natural numbers.

Note: For example, the set 2 has two elements. This set has been selected from the class of all two-element sets to represent the size of the sets in that class.

The above definition is one alternative of many (as with ordered pairs). This construction involves some unexpected properties, such as

$$0 \in 1 \in 2 \in 3 \in \ldots$$

and

$$0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \ldots$$

But these properties can be regarded as accidental side effects of the definition. They do no harm, and actually will be convenient at times.

Let us now turn to give a precise definition of the set of all natural numbers.

Definition 4.1

For any set a, its successor a^+ is defined as

$$a^+ = a \cup \{a\}.$$

By the above definition:

$$0 = \emptyset$$
$$1 = \{0\} = \{\emptyset\} = \emptyset \cup \{\emptyset\} = \emptyset^+ = 0^+$$
$$2 = \{0,1\} = \{0,\{0\}\} = \{0\} \cup \{\{0\}\} = 1 \cup \{1\} = 1^+ = \emptyset^{++}$$
$$3 = \{0,1,2\} = \{0,1,\{0,1\}\} = \{0,1\} \cup \{\{0,1\}\} = 2 \cup \{2\} = 2^+ = \emptyset^{+++}$$
$$\vdots$$

Definition 4.2

A set A is said to be inductive iff $\emptyset \in A$ and it is closed under successor, i.e.,

$$\forall a \in A(a^+ \in A).$$

Infinity Axiom

There exists an inductive set, i.e.,

$$\exists A(\emptyset \in A \wedge \forall a \in A(a^+ \in A)).$$

For example, given a set $a \neq \emptyset$, $A = \{\emptyset, a, \emptyset^+, a^+, \emptyset^{++}, a^{++}, \ldots\}$ is an inductive set.

Definition 4.3

A natural number is a set that belongs to every inductive set.
The set of all natural numbers is denoted by ω.

Clearly, $\omega = \{x \mid \forall y(y \text{ is inductive } \rightarrow x \in y)\} = \bigcap\{A \mid A \text{ is inductive}\}$.

Theorem 4B

The set ω is inductive, and is a subset of every inductive set. In other words, ω is the smallest inductive set.

Proof. By definition, ω is a subset of every inductive set. Next, we show that ω is inductive.

- Since $\emptyset$ is an element of every inductive set, $\emptyset \in \omega$.
- For any a, $a \in \omega \implies a$ belongs to every inductive set A
  $\implies a^+$ belongs to every inductive set A
  $\implies a^+ \in \omega$. □

From the above theorem, it follows that $\omega = \{\emptyset, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, \ldots\}$.

Induction Principle for ω

Any inductive subset of ω coincides with ω.

Mathematical Induction To prove that a property $P(x)$ holds for all natural numbers n, i.e., $T = \omega$ for the set

$$T = \{n \in \omega \mid P(n)\},$$

it suffices to prove that T is inductive, i.e., to prove the following:

- base case 0 has property P, i.e., $0 \in T$.
- inductive step If $P(n)$ (i.e., $n \in T$), then $P(n^+)$ (i.e., $n^+ \in T$).

Let us prove the following theorem by induction.

Theorem 4C

Every non-zero natural number is the successor of some natural number.

Proof. Let

$$T = \{n \in \omega \mid n = 0 \vee \exists m \in \omega(n = m^+)\}.$$

Clearly, $0 \in T$. Moreover, $n \in T \implies n \in \omega \implies n^+ \in \omega \implies n^+ \in T$.
Hence by induction principle, $T = \omega$. □

Transitive Sets

Definition 4.4

A set A is said to be a transitive set iff

$$x \in a \in A \Longrightarrow x \in A.$$

The above condition is equivalent to

$$a \in A \Longrightarrow a \subseteq A$$

or

$$\bigcup A \subseteq A.$$

For example:

- The set $\{\emptyset, \{\{\emptyset\}\}\}$ is not a transitive set, since
$$\{\emptyset\} \in \{\{\emptyset\}\} \in \{\emptyset, \{\{\emptyset\}\}\},$$
but $\{\emptyset\} \notin \{\emptyset, \{\{\emptyset\}\}\}$.
- The set $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$ is transitive, since
$$\emptyset \in \{\emptyset\} \in \{\emptyset, \{\emptyset\}\} \quad \text{(i.e., } 0 \in 1 \in 2\text{)}$$
and $\emptyset \in \{\emptyset, \{\emptyset\}\}$ (i.e., $0 \in 2$).
- The set $\{0, 2\}$ is not transitive, since $1 \in 2 \in \{0, 2\}$, but $1 \notin \{0, 2\}$.
- $\emptyset$ is a transitive set.

Theorem 4E

For any transitive set a, $\bigcup a^+ = a$.

Proof.
$$\begin{aligned} \bigcup a^+ &= \bigcup (a \cup \{a\}) \\ &= (\bigcup a) \cup (\bigcup \{a\}) \\ &= (\bigcup a) \cup a \\ &= a \;\; (\text{since } \bigcup a \subseteq a). \end{aligned}$$
□

Theorem 4F

Every natural number is a transitive set.

Proof. (by induction) Trivially, $0 = \emptyset$ is transitive. If n is a transitive set, then by Theorem 4E,

$$\bigcup n^+ = n \subseteq n \cup \{n\} = n^+,$$

thus by definition, n^+ is transitive. Hence by Induction Principle, every natural number is a transitive set. □

Theorem 4.5

The successor function $s : \omega \to \omega$*, defined as* $n \mapsto n^+$*, is one-to-one.*

Proof. For any $m, n \in \omega$, by Theorem 4E and 4F, we have that

$$s(m) = s(n) \Longrightarrow m^+ = n^+ \Longrightarrow \bigcup m^+ = \bigcup n^+ \Longrightarrow m = n.$$

□

Theorem 4G

The set ω *is a transitive set.*

Note: By this theorem, $n \in \omega \Longrightarrow n \subseteq \omega$, i.e, every natural number is itself a set of natural numbers. For example, as we have seen, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, etc.

Proof. (by induction) We want to show that $\forall n \in \omega (n \subseteq \omega)$. It suffices to show that the set $T = \{n \in \omega \mid n \subseteq \omega\}$ is inductive.
As $0 = \emptyset \subseteq \omega$, we have $0 \in T$. If $n \in T$, then

$$n \subseteq \omega \quad \text{and} \quad \{n\} \subseteq \omega$$

thus $n^+ = n \cup \{n\} \subseteq \omega$, thereby $n^+ \in T$. Hence T is inductive. □

Ordering on ω

$$
\begin{aligned}
&0 = \emptyset,\\
&1 = 0^+ = 0 \cup \{0\} = \{0\} = \{\emptyset\}\\
&2 = 1^+ = 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\}\\
&3 = 2^+ = 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\\
&\vdots
\end{aligned}
$$

Definition 4.6

For any $m, n \in \omega$, we say that m is less than n (i.e., $m < n$) iff $m \in n$. We write $m \underline{\in} n$ or $m \leq n$ iff $m \in n$ or $m = n$.

Clearly,
- $m \in m^+ = m \cup \{m\}$
- $m \in n^+ \iff m \in n \cup \{n\} \iff m \in n$ or $m = n$.

Fact 4.7

Every natural number n is equal to the set of all natural numbers m smaller than n, i.e., $n = \{m \in \omega \mid m \in n\}$.

Proof. Put $X = \{m \in \omega \mid m \in n\}$. Obviously, $m \in X \Longrightarrow m \in n$. Conversely, since ω is a transitive set, if $m \in n (\in \omega)$, then $m \in \omega$, thus $m \in X$. □

We will show that $\in$ is a linear ordering on ω, that is, $\in$ is transitive and satisfies trichotomy: exactly one of the following three alternatives holds:

$$m \in n, \quad m = n, \quad n \in m.$$

Fact 4.8

The ordering $\in$ on ω is transitive, i.e., for any $m, n, k \in \omega$,

$$m \in n \ \wedge \ n \in k \Longrightarrow m \in k.$$

Proof. Since $k \in \omega$ is a transitive set. □

Lemma 4L

Let $m, n \in \omega$. (a) $m \in n$ iff $m^+ \in n^+$
(b) $n \notin n$.

Proof. (a) If $m^+ \in n^+ = n \cup \{n\}$, then $m^+ \in n$ or $m^+ = n$. Since $m \in m^+ = m \cup \{m\}$, by transitivity of $\in$, we obtain $m \in n$.

For the converse direction, we show that

$$T = \{n \in \omega \mid \forall m \in n(m^+ \in n^+)\}$$

is inductive.

Vacuously, $0 \in T$. Assume $n \in T$. For any $m \in n^+$, we show that $m^+ \in n^{++}$.
Since $m \in n^+ = n \cup \{n\}$, we have that $m \in n$ or $m = n$. If $m = n$, then $m^+ = n^+ \in n^{++}$. If $m \in n$, then since $n \in T$, we have $m^+ \in n^+ \in n^{++}$, which by the transitivity of $\in$ implies $m^+ \in n^{++}$.

(b) It suffices to show that $T = \{n \in \omega \mid n \notin n\}$ is inductive.
Since $\emptyset \notin \emptyset$, we have $0 \in T$. By (a),

$$n \in T \Longrightarrow n \notin n \Longrightarrow n^+ \notin n^+ \Longrightarrow n^+ \in T.$$

□

Theorem 4.9

The ordering $\in$ on ω is a linear ordering.

Proof. We have shown that $\in$ is transitive. It remains to show that $\in$ satisfies trichotomy, i.e., exactly one of the following three alternatives holds:

$$(i)\ m \in n, \text{ or } (ii)\ m = n, \text{ or } (iii)\ n \in m. \qquad (*)$$

If (i) and (iii) are both true, then by transitivity, $m \in m$, contradicting Lemma 4L. If (ii) and ((i) or (ii)) are true, then we also derive $m \in m$, which again leads to a contradiction. Thus at most one of the alternatives in $(*)$ holds.

Next, we show that at least one of the alternatives in $(*)$ holds. It suffices to show that

$$T = \{n \in \omega \mid \forall m \in \omega (m \in n \vee m = n \vee n \in m)\}$$

is inductive.

Base case: We show that $0 = m$ or $0 \in m$ for all $m \in \omega$ by induction.
(a) Obviously, $0 = 0$. (b) If $0 = m$ or $0 \in m$, then $0 \in m^+$, since $m \in m^+$ and $\in$ is transitive.

Inductive step: Assume $n \in T$. We show that $n^+ \in T$, i.e., one of the three alternatives in $(*)$ holds for n^+. By assumption, for any $m \in \omega$, one of the three alternatives in $(*)$ holds for n. If (i) or (ii) is the case, since $n \in n^+$, we derive $m \in n^+$. If (iii) is the case, by Lemma 4L, $n^+ \in m^+ = m \cup \{m\}$, thus $n^+ \in m$ or $n^+ = m$. Hence $n^+ \in T$. □

Corollary 4M

For any $m, n \in \omega$,

$$m \in n \quad \textit{iff} \quad m \subset n.$$

Proof. Since n is a transitive set, if $m \in n$, then $m \subseteq n$, and the inclusion is proper as $m \notin m$ by Lemma 4L(b).

Conversely, if $m \subset n$, then $m \neq n$. If $n \in m$, then $n \in n$, contradicting Lemma 4L(b). Therefore by trichotomy, $m \in n$ is the case. □

Theorem 4.10 (Well Ordering of ω)

Any nonempty subset A of ω contains a least element, i.e., there is $n \in A$ such that $n \underline{\in} k$ for all $k \in A$.

Proof. Suppose $A \subseteq \omega$ does not have a least element. We will show that $A = \emptyset$. To this end, consider the set

$$B = \{m \in \omega \mid \forall n \in m (n \notin A)\}.$$

It is sufficient to show that $B = \omega$, or B is an inductive set.

Vacuously, $0 \in B$. Assume $k \in B$. We show that $k^+ \in B$. Given any $n \in k^+ = k \cup \{k\}$, we want to show that $n \notin A$.

Case 1: $n \in k$. Then since $k \in B$, $n \notin A$.

Case 2: $n = k$. If $n = k \in A$, then as k is not a least element of A, we must have that $n_0 \in k$ for some $n_0 \in A$. But this contradicts the fact that $k \in B$. Therefore $n \notin A$.

Hence in both cases, we derive $n \notin A$. It follows that $k^+ \in B$. □

Induction Principle for ω

Any inductive subset of ω coincides with ω.

To prove that a subset $T \subseteq \omega$ equals ω, it suffices to prove:

base case $0 \in T$.

inductive step If $n \in T$, then $n^+ \in T$.

Strong Induction Principle for ω

Let A be a subset of ω. Suppose that for every $n \in \omega$,

$$\textit{if } m \in A \textit{ holds for all } m \in n, \textit{ then } n \in A. \qquad (*)$$

Then $A = \omega$.

Proof. Suppose towards a contradiction that $A \neq \omega$. Then $\omega \setminus A \neq \emptyset$, and by the well ordering, $\omega \setminus A$ contains a least element n. Thus for all $m \in n$, we have that $m \notin \omega \setminus A$ (i.e., $m \in A$) holds. But then by $(*)$, we have $n \in A$, which leads to a contradiction. □

Recursion Theorem

Suppose we are writing a computer program, in which a function $h : \omega \to A$ needs to be defined. We can either directly write down the defining expression of h, or give a recursive definition.

To define $h : \omega \to A$ recursively, we specify

(i) the value of $h(0)$,
(ii) and a function $F : A \to A$ such that $h(n^+) = F(h(n))$ for all $n \in \omega$.
When the program is being executed, the computer computes successively

$$\begin{aligned} &h(0), \\ &h(1) = F(h(0)), \\ &h(2) = F(h(1)), \\ &\vdots \end{aligned}$$

The above program tells us how to compute h *if it exists*. But we need to prove that there exists a set h that is a function meeting the above conditions.

Recursion Theorem on ω

Let A be a set, $a \in A$, and $F : A \to A$. Then there exists a unique function $h : \omega \to A$ such that $h(0) = a$, and for every $n \in \omega$,

$$h(n^+) = F(h(n)).$$

Example 4.1: Suppose we want to define a function $\mathrm{Add}_5 : \omega \to \omega$ such that $\mathrm{Add}_5(n)$ is the result of adding 5 to n. We specify the function $\mathrm{Add}_5(n)$ by requiring

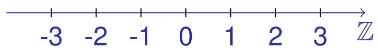
$$\begin{aligned} \mathrm{Add}_5(0) &= 5, \\ \mathrm{Add}_5(n^+) &= \mathrm{Add}_5(n)^+ \quad \text{for } n \in \omega. \end{aligned}$$

The Recursion Theorem guarantees that a unique such function exists.

Note: To apply the Recursion Theorem, we may let $a = 5$, $F : \omega \to \omega$ be defined as $F(b) = b^+$ for all $b \in \omega$. This way

$$\mathrm{Add}_5(n^+) = F(\mathrm{Add}_5(n)) = \mathrm{Add}_5(n)^+.$$

Example 4.2: Let $\mathbb{Z}$ be the set of all integers, and $F(x) = x^2 + 1$, $x \in \mathbb{Z}$.



There is no function $h : \mathbb{Z} \to \mathbb{Z}$ such that for every $m \in \mathbb{Z}$,

$$h(m+1) = F(h(m)) = h(m)^2 + 1. \qquad (*)$$

Proof. $(*)$ implies that $h(m) \geq 1$ for all $m \in \mathbb{Z}$. It follows that

$$h(m)^2 \geq h(m) \Longrightarrow h(m)^2 + 1 > h(m) \Longrightarrow h(m+1) > h(m) \geq 1.$$

Hence $h(0) > h(-1) > h(-2) > \cdots \geq 1$, which means that the interval $[1, h(0)]$ contains infinitely many integers, being impossible. □

Note: Recursion on ω relies on there being a starting point 0, whereas $\mathbb{Z}$ has no analogous starting point.

Proof. (of Recursion Theorem) We only prove the existence of such function, and the uniqueness part is left as an exercise.

Let h be the union of all *approximating functions* of h. Formally, let

$$h = \bigcup\{v : X \to A \mid X \subseteq \omega,\ v \text{ is acceptable}\},$$

where a function v is said to be *acceptable* iff $\mathrm{dom}\, v \subseteq \omega$, $\mathrm{ran}\, v \subseteq A$ and the following two conditions hold:

(i) If $0 \in \mathrm{dom}\, v$, then $v(0) = a$.

(ii) If $n^+ \in \mathrm{dom}\, v$, then $n \in \mathrm{dom}\, v$ and $v(n^+) = F(v(n))$.

Claim: h is the required function, that is, (1) h is a function, (2) h is acceptable, (3) $\mathrm{dom}\, h = \omega$.

(1) It suffices to show that the set

$$S = \{n \in \omega \mid (n, y) \in h \text{ for at most one } y\}.$$

equals ω. To this end, we prove that S is inductive.

Base case: We show that $(0, y) \in h$ for at most one y. Given $(0, y_1), (0, y_2) \in h$, there exist acceptable v_1, v_2 such that

$$(0, y_1) \in v_1 \text{ and } (0, y_2) \in v_2,$$

i.e., $v_1(0) = y_1$ and $v_2(0) = y_2$. But by (i), $y_1 = a = y_2$.

Inductive step: Assume $m \in S$. We show $m^+ \in S$. If $(m^+, y_1), (m^+, y_2) \in h$, then there exist acceptable v_1, v_2 such that $m^+ \in \mathrm{dom}\, v_1$ and $m^+ \in \mathrm{dom}\, v_2$. Hence, $m \in \mathrm{dom}\, v_1 \subseteq \mathrm{dom}\, h$ and $m \in \mathrm{dom}\, v_2 \subseteq \mathrm{dom}\, h$, as well as

$$y_1 = v_1(m^+) = F(v_1(m)) \quad \text{and} \quad y_2 = v_2(m^+) = F(v_2(m)).$$

Since $m \in S$, we have that $v_1(m) = v_2(m)$, thereby $y_1 = y_2$. ⊣

(2) We have shown that h is a function, and clearly $\mathrm{dom}\, h \subseteq \omega$, $\mathrm{ran}\, h \subseteq A$. It remains to check that h satisfies (i) and (ii).

(i) If $0 \in \mathrm{dom}\, h$, then there exists an acceptable v such that $0 \in \mathrm{dom}\, v$. Since v is acceptable, $a = v(0) = h(0)$.

(ii) If $n^+ \in \mathrm{dom}\, h$, we show that $n \in \mathrm{dom}\, h$ and $h(n^+) = F(h(n))$. By assumption, there exists an acceptable v such that $n^+ \in \mathrm{dom}\, v$. Since v is acceptable, $n \in \mathrm{dom}\, v \subseteq \mathrm{dom}\, h$ and

$$F(h(n)) = F(v(n)) = v(n^+) = h(n^+).$$

⊣

(3) It suffices to show that $\mathrm{dom}\, h$ is inductive.

Base case: Clearly, the function $\{(0, a)\}$ is acceptable, thus $0 \in \mathrm{dom}\, h$.

Inductive step: Assuming $m \in \mathrm{dom}\, h$, we show that $m^+ \in \mathrm{dom}\, h$. By assumption, there exists an acceptable v such that $m \in \mathrm{dom}\, v$. If $m^+ \in \mathrm{dom}\, v \subseteq \mathrm{dom}\, h$, then we are done. Now, assume $m^+ \notin \mathrm{dom}\, v$. Let

$$u = v \cup \{(m^+, F(v(m)))\}.$$

Clearly, u is a function and $m^+ \in \mathrm{dom}\, u$. It suffices to show that u is acceptable (for then $m^+ \in \mathrm{dom}\, u \subseteq \mathrm{dom}\, h$). Obviously, $\mathrm{dom}\, u \subseteq \omega$, $\mathrm{ran}\, u \subseteq A$ and $u(0) = v(0) = a$. It remains to check (ii) for u.

Assuming $n^+ \in \mathrm{dom}\, u$, we show $n \in \mathrm{dom}\, u$ and $u(n^+) = F(u(n))$. If $n^+ \neq m^+$, then $n^+ \in \mathrm{dom}\, v$, which implies that $n \in \mathrm{dom}\, v \subseteq \mathrm{dom}\, u$ and

$$u(n^+) = v(n^+) = F(v(n)) = F(u(n)).$$

Otherwise, if $n^+ = m^+$, since successor function is one-to-one, $n = m \in \mathrm{dom}\, v \subseteq \mathrm{dom}\, u$. By the definition of u,

$$u(n^+) = u(m^+) = F(v(m)) = F(u(m)) = F(u(n)).$$

⊣

□