Natural Numbers*

Ana Sokolova

Department of Computer Sciences, University of Salzburg

anas@cs.uni-salzburg.at

January 8, 2021

1 The Structure of Natural Numbers

We start with discussing the structure of the natural numbers. Understanding this is important for proving properties of the kind

$$\forall[n \in \mathbb{N}\colon\ P(n)] \quad \text{i.e.} \quad \forall n \in \mathbb{N}.\, P(n)$$

by a method that is intrinsic to natural numbers, called *induction*. We will also learn about induction in this unit.
You can read most of this material also in the book [LR].

The structure that is relevant for us here is $(\mathbb{N}, 0, s)$ where $\mathbb{N}$ is the set of natural numbers, $0 \in \mathbb{N}$, and $s\colon \mathbb{N} \to \mathbb{N}$. The function s models the notion of a successor and is defined by $s(n) = n + 1$. This enables us to count (linearly order): 0 is the starting natural number. For every natural number n, there is a next natural number s(n).

However, even if we do not know $\mathbb{N}$ at all (and do not know what $n + 1$ should be) we can construct the set $\mathbb{N}$ as the unique set (up to isomorphism[1]) with structure $(\mathbb{N}, 0, s\colon \mathbb{N} \to \mathbb{N})$ that satisfies the following Peano axioms:

(PA1) Different natural numbers have different successors, i.e.,

$$\forall n, m \in \mathbb{N}.\, n \neq m \Rightarrow s(n) \neq s(m)$$

or equivalently (positively stated)

$$\forall n, m \in \mathbb{N}.\, s(n) = s(m) \Rightarrow n = m.$$

Clearly, this is the statement that s is injective.

(PA2) 0 is not a successor, i.e,

$$\forall n[n \in \mathbb{N}\colon\ \neg(s(n) = 0)]$$

* Notes from the lectures Formale Systeme on naive set theory. Many thanks to Luis Thiele for helping me with producing the notes.

[1] The notion of isomorphism of structures is a very important one and you can read its definition in the lecture notes on Algebraic Structures.

(PA3) All natural numbers except 0 are successors, i.e.,

$$\forall n[n \in \mathbb{N} \wedge \neg(n = 0) \colon \exists m[m \in \mathbb{N} \colon\ n = s(m)]]$$

(PA4) For every (unary) predicate P on $\mathbb{N}$, the following formula is true:

$$P(0) \wedge \forall i[i \in \mathbb{N} \colon\ P(i) \Rightarrow P(i+1)] \quad \Rightarrow \quad \forall n[n \in \mathbb{N} \colon\ P(n)]$$

The fourth Peano Axiom (PA4) is the axiom/principle of mathematical induction. One can easily prove that if a structure $(A, o, f \colon A \to A)$ with $o \in A$ satisfies the axioms (PA1) - (PA4) when substituting o for 0 and f for s, then (A, a, f) must be isomorphic to $(\mathbb{N}, 0, s)$, i.e., there is a bijection $i \colon A \to \mathbb{N}$ such that $i(o) = 0$ and for all $a \in A$, $i(f(a)) = s(i(a))$, which means that the structures are really the same up-to remaining of the elements of A according to i (or equivalently, remaining the elements of $\mathbb{N}$ according to i^{-1}).

One can restate the fourth Peano Axiom, the axiom of mathematical induction, equivalently as follows

(PA4') Let $K \subseteq \mathbb{N}$ have the property that
(a) $0 \in K$
(b) $\forall n \in \mathbb{N}.\, n \in K \Rightarrow (n+1) \in K$
Then $K = \mathbb{N}$.

Lemma 1. *The axioms (PA4) and (PA4') are equivalent.*

Proof. Assume (PA4) holds. Let $K \subseteq \mathbb{N}$ have the properties (a) and (b) from (PA4'). Define a predicate P on $\mathbb{N}$ by $P(n) \stackrel{val}{=} n \in K$. Then (a) gives us $P(0)$. Further on, (b) gives us $\forall n \in \mathbb{N}.\, P(n) \Rightarrow P(n+1)$. Hence $P(0) \wedge \forall i[i \in \mathbb{N} \colon\ P(i) \Rightarrow P(i+1)]$, by bound variables and $\wedge$-intro. Now from (PA4) by $\Rightarrow$-elimination we get

$$\forall n[n \in \mathbb{N}.\, P(n)]$$

which is further equivalent to $\forall n[n \in \mathbb{N} \colon\ n \in K]$ and means $\mathbb{N} \subseteq K$. Together with $K \subseteq \mathbb{N}$, which holds by assumption, we get $K = \mathbb{N}$.

For the opposite, assume (PA4') holds for any subset $K \subseteq \mathbb{N}$. Let P be an arbitrary unary predicate on $\mathbb{N}$. Consider the subset $\mathbb{P} \subseteq \mathbb{N}$ defined as the extension of the predicate P, i.e.,

$$\mathbb{P} = \{n \in \mathbb{N} \mid P(n)\}$$

Applying (PA4') to $\mathbb{P}$ (taking $K = \mathbb{P}$) will yield (PA4): First assume $P(0) \wedge \forall i[i \in \mathbb{N} \colon\ P(i) \Rightarrow P(i+1)]$. Then $P(0)$ holds, i.e., $0 \in \mathbb{P}$ and hence $\mathbb{P}$ satisfies (a) of (PA4'). Then also $\forall i[i \in \mathbb{N} \colon\ P(i) \Rightarrow P(i+1)]$, i.e., $\forall i[i \in \mathbb{N} \colon\ i \in \mathbb{P} \Rightarrow (i+1) \in \mathbb{P}]$ and hence $\mathbb{P}$ satisfies (b) from (PA4'). From (PA4') $\mathbb{P} = \mathbb{N}$ which shows in particular $\mathbb{N} \subseteq \mathbb{P}$, i.e., $\forall n[n \in \mathbb{N} \colon\ n \in \mathbb{P}]$, i.e.,

$$\forall n[n \in \mathbb{N} \colon\ P(n)].$$

The axiom (PA4) follows now by implication intro. □

Let us intuitively convince ourselves that (PA4) holds on the natural numbers $\mathbb{N}$, as we know them. Assume that indeed $P(0) \wedge \forall i[i \in \mathbb{N} \colon\ P(i) \Rightarrow P(i+i)]$. Then we know

(1) $P(0)$ {by assumption with $\wedge$-elimination}
(2) $P(0) \Rightarrow P(1)$ {by assumption with $\wedge$-elimination and $\forall$-elimination on $i = 0$}
(3) $P(1)$ {by $\Rightarrow$-elimination on (1) and (2)}
(4) $P(1) \Rightarrow P(2)$ {by assumption with $\wedge$-elimination and $\forall$-elimination on $i = 1$}
(5) $P(2)$ {by $\Rightarrow$-elimination on (3) and (4)}
...

This way we can write a proof of $P(n)$ for arbitrary given $n \in \mathbb{N}$.

2 Induction Proofs

The induction axiom gives us a proof method for properties of the kind

$$\forall[n \in \mathbb{N}\colon\ P(n)].$$

This is a very important proof method with numerous applications.

Let us explain the proof method now. We want to show the property $\forall n[n \in \mathbb{N}\colon\ P(n)]$. To do so, by induction on i it suffices to show

$$P(0) \text{ and } \forall[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)]$$

Proving $P(0)$ is known as the induction basis, abbreviated by (IB). Proving $\forall[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)]$ consists of: (IH) Fixing a natural number $i \in \mathbb{N}$ and assuming that $P(i)$ holds; and (IS) Proving that then $P(i+1)$ holds for i being the fixed number from (IH). Here, (IH) is an abbreviation for induction hypothesis, and (IS) for induction step.

Hence, a proof by induction on i of $\forall n[n \in \mathbb{N}\colon\ P(n)]$ consists of:

(IB) A proof of $P(0)$;
(IH) Stating the right induction hypothesis: Let $i \in \mathbb{N}$ be such that $P(i)$ holds; and
(IS) A proof of $P(i+1)$ using the induction hypothesis.

Why is this sufficient? We will explain this with a flag proof, like we did in the lectures. Assume we prove

...

(m) $P(0)$

...

(l) $\forall i[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)]$

{ $\wedge$-intro (m), (l) }

(l') $P(0) \wedge \forall i[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)]$

{ (PA4), the induction axiom }

(l'') $P(0) \wedge \forall i[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)] \Rightarrow \forall n[n \in \mathbb{N}\colon\ P(n)]$

{ $\Rightarrow$-elim. on (l') and (l'') }

(l+1) $\forall n[n \in \mathbb{N}\colon\ P(n)]$

Now, for proving $\forall i[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)]$ at line (l), notice that, by domain weakening

$$\forall i[i \in \mathbb{N}\colon\ P(i) \Rightarrow P(i+1)] \stackrel{val}{=} \forall i[i \in \mathbb{N} \wedge P(i)\colon\ P(i+1)]$$

So, we do the proof as follows

(m+1) **var** i; $i \in \mathbb{N} \wedge P(i)$

...

(l-1) $P(i+1)$

{ $\forall$-intro on $(m+1)$, $(l-1)$ }

(l) $\forall i[i \in \mathbb{N} \wedge P(i)\colon\ P(i+1)]$

Line (m+1) is the inductive hypothesis (IH). The proof obligation above line (l-1) (the hole from line (m+2) to (l-2)) should be filled by the inductive step (IS). The proof obligation above line (m) (the hole from line (1) to (m-1)) should be filled by the induction basis (IB).

Remark 1. In the book [LR] and in general in flag proofs one omits the lines (l') and (l''), as one does not write the induction axiom as part of the proof, just refers to it, and one does the $\wedge$-intro implicitly. The explanation for line (l+1) is then "{induction on (m), (l)}".

We next show an example of an inductive proof, first with all the details of a flag-proof (following the structure that we just discussed and filling-in the holes) and then we write it in a more usual, and more concise way afterwards.

Example 1. Proof of $\forall n \left[n \in \mathbb{N}\colon\ \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \right]$. Note: $P(n) \stackrel{val}{=} \left(\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \right)$.

(1) $\sum_{i=0}^{0} i = 0$

(2) $\frac{0(0+1)}{2} = 0$

{ from (1), (2) and transitivity of "=" }

(3) $\sum_{i=0}^{0} i = \frac{0(0+1)}{2}$

{ direct from (3) }

(4) For $n = 0$, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

{ directly equiv. to (4) }

(m) = (5) $P(0)$

(m+1) = (6) **var** n; $n \in \mathbb{N} \wedge \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ (IH)

{ Def. $\sum$ }

(7) $\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1)$

{ (7) and (IH) = (m+1) }

(8) $\sum_{i=0}^{n+1} i = \frac{n(n+1)}{2} + (n+1)$

{ Mathematical derivation }

(l-1) = (9) $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$

(l) $\forall n \left[n \in \mathbb{N} \colon \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2} \right]$

{ induction on (m), (l) }

(l+1) $\forall n \left[n \in \mathbb{N} \colon \sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2} \right]$

The same example concisely, with a standard proof by induction:

Proof. We prove $\forall n \in \mathbb{N}.\ \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$, by induction on n.

(IB) We must show the property holds for $n = 0$ i.e.

$$\sum_{i=0}^{0} i = \frac{0(0+1)}{2}.$$

We evaluate both sides and see

$$\sum_{i=0}^{0} i = 0 \quad , \quad \frac{0(0+1)}{2} = 0$$

so clearly (by transitivity of "=") the inductive basis holds.

(IH) Let $n \in \mathbb{N}$ (be arbitrary) and assume $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

(IS) We must show that $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$, i.e., the property holds for $n+1$ using (IH). We have

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) \overset{\text{(IH)}}{=} \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}.$$

So we have shown the inductive step, and this completes the proof. □

3 Inductive Definitions

The axiom of induction also allows inductive definitions like in the next example. Here, "allows" means that it guarantees that inductive definitions lead to well-defined functions.

Example 2. The sequence of real numbers $(a_i \mid i \in \mathbb{N})$ is defined inductively by

$$\begin{aligned} a_0 &= 2 \\ a_{i+1} &= 2a_i - 1 \end{aligned}$$

Note that such a sequence is actually a function $a\colon \mathbb{N} \to \mathbb{R}$ where we write a_i for $a(i)$.

We can prove by induction that such a function/sequence is well-defined, i.e. that it assigns a unique real number to any natural number i.

Clearly, $a_0 = 2$ assigns a real number to a_0, and this is unique as 0 is no successor. Hence $P(0)$ holds (IB proven). Assume $P(i)$ holds, i.e., assume a_i is well-defined for $i \in \mathbb{N}$. (This is our IH!) Then $a_{i+1} = 2a_i - 1$ assigns a real number to $i+1$ and this is unique as the successor function is injective.

What we discussed here it usually taken for clear, and not writen explicitly.

Now, for inductively defined objects, like in this sequence above, we can prove properties by induction. For example, we can prove

Lemma 2. $a_n = 2^n + 1$ *holds for the inductively defined sequence* $(a_i | i \in \mathbb{N})$ *where*

$$a_0 = 2 \quad , \quad a_{i+1} = 2a_i - 1.$$

The formula $a_n = 2^n + 1$ is called a "closed formula" as a_n depends explicitly on n, i.e., there is no longer inductive definition here.

Proof. (By induction on n) Note that we are proving the property $\forall n \in \mathbb{N}.\, P(n)$ for the predicate $P(n) \stackrel{val}{=} (a_n = 2^n + 1)$.

(IB) We need to prove

$$a_0 = 2^0 + 1.$$

We have $a_0 \stackrel{\text{def}}{=} 2$; $2^0 + 1 = 1 + 1 = 2$ So indeed, $a_0 = 2^0 + 1$.

(IH) Let $n \in \mathbb{N}$ be such that

$$a_n = 2^n + 1.$$

(IS) We need to show that $a_{n+1} = 2^{n+1} + 1$. We have

$$\begin{aligned} a_{n+1} \stackrel{\text{def}}{=} 2a_n - 1 &\stackrel{\text{(IH)}}{=} 2(2^n + 1) - 1 \\ &= 2 \cdot 2^n + 2 - 1 \\ &= 2^{n+1} + 1 \end{aligned}$$

□