Peano Arithmetics in MLTT

Seminar: Foundations of Mathematics

Philipp Schepper

December 4, 2018

Saarland University – Department of Computer Science

Overview

Motivation

Peano Numbers in Modern, Lightweight Twitter Textmessages (MLTT)

Source: `https://twitter.com/every_peano`

Motivation

- We have already seen several definitions (von Neumann, Church, Scott, . . .)
- Try to embed them in type theory?

$\Rightarrow$ Maybe not possible or the best/easiest/most elegant/. . . way!

- MLTT introduces primitive constructions

$\Rightarrow$ We want to find a “good” foundation of mathematics!

Motivation

- We have already seen several definitions (von Neumann, Church, Scott, . . .)
- Try to embed them in type theory?

$\Rightarrow$ Maybe not possible or the best/easiest/most elegant/. . . way!

- MLTT introduces primitive constructions

$\Rightarrow$ We want to find a “good” foundation of mathematics!

Motivation

- We have already seen several definitions (von Neumann, Church, Scott, ...)
- Try to embed them in type theory?

$\Rightarrow$ Maybe not possible or the best/easiest/most elegant/...way!

- MLTT introduces primitive constructions

$\Rightarrow$ We want to find a "good" foundation of mathematics!

Motivation

- We have already seen several definitions (von Neumann, Church, Scott, ...)
- Try to embed them in type theory?

$\Rightarrow$ Maybe not possible or the best/easiest/most elegant/...way!

- MLTT introduces primitive constructions

$\Rightarrow$ We want to find a “good” foundation of mathematics!

Motivation

- We have already seen several definitions (von Neumann, Church, Scott, . . .)
- Try to embed them in type theory?

$\Rightarrow$ Maybe not possible or the best/easiest/most elegant/. . . way!

- MLTT introduces primitive constructions

$\Rightarrow$ We want to find a "good" foundation of mathematics!

Definition of Natural Numbers

Define $\mathbb{N}$ as inductive type:

$$\frac{}{0 : \mathbb{N}}\ (\text{nat0}) \qquad \frac{n : \mathbb{N}}{Sn : \mathbb{N}}\ (\text{natS})$$

Comes with elimination rule $R_{\mathbb{N}}$:

$R_{\mathbb{N}} : (\forall P : \mathbb{N} \to U)P0 \to ((\forall n : \mathbb{N})P(Sn)) \to (\forall n : \mathbb{N})Pn$

$$\frac{H : P\ 0 \qquad f : (\forall m : \mathbb{N})P(Sm)}{R_{\mathbb{N}}\ P\ H\ f : (\forall n : \mathbb{N})P\ n}\ P : \mathbb{N} \to U$$

Comes with computation rules:

$R_{\mathbb{N}}\ P\ H\ f\ 0 \succ H$

$R_{\mathbb{N}}\ P\ H\ f\ (Sn) \succ f\ n$

Definition of Natural Numbers

Define $\mathbb{N}$ as inductive type:

$$\frac{}{0 : \mathbb{N}}\ (\text{nat0}) \qquad\qquad \frac{n : \mathbb{N}}{Sn : \mathbb{N}}\ (\text{natS})$$

Comes with elimination rule $R_{\mathbb{N}}$:

$R_{\mathbb{N}} : (\forall P : \mathbb{N} \to U)P0 \to ((\forall n : \mathbb{N})P(Sn)) \to (\forall n : \mathbb{N})Pn$

$$\frac{H : P\ 0 \qquad f : (\forall m : \mathbb{N})P(Sm)}{R_{\mathbb{N}}\ P\ H\ f : (\forall n : \mathbb{N})P\ n}\ P : \mathbb{N} \to U$$

Comes with computation rules:

$R_{\mathbb{N}}\ P\ H\ f\ 0 \succ H$

$R_{\mathbb{N}}\ P\ H\ f\ (Sn) \succ f\ n$

Definition of Natural Numbers

Define $\mathbb{N}$ as inductive type:

$$\frac{}{0 : \mathbb{N}}\ (\text{nat0}) \qquad\qquad \frac{n : \mathbb{N}}{Sn : \mathbb{N}}\ (\text{natS})$$

Comes with elimination rule $R_\mathbb{N}$:

$R_\mathbb{N} : (\forall P : \mathbb{N} \to U)P0 \to ((\forall n : \mathbb{N})P(Sn)) \to (\forall n : \mathbb{N})Pn$

$$\frac{H : P\ 0 \qquad f : (\forall m : \mathbb{N})P(Sm)}{R_\mathbb{N}\ P\ H\ f : (\forall n : \mathbb{N})P\ n}\ P : \mathbb{N} \to U$$

Comes with computation rules:

$R_\mathbb{N}\ P\ H\ f\ 0 \succ H$

$R_\mathbb{N}\ P\ H\ f\ (Sn) \succ f\ n$

Recap: Equality

- Last week we have seen several definitions of equality.
- From now on, we use inductive equality:

$$\frac{}{Q\ a : a = a}\,(A : U), (a : A)$$

- And the corresponding eliminator $R_=$:
$R_= : (\forall A : U)(\forall P : A \to U)(\forall a : A)(P\ a) \to (\forall b : A)a = b \to P\ b$

$$\frac{H_1 : P\ a \qquad H_2 : a = b}{R_=\ A\ P\ a\ H_1\ b\ H_2 : P\ b}\,(A : U), (P : A \to U), (a, b : A)$$

Recap: Equality

- Last week we have seen several definitions of equality.
- From now on, we use inductive equality:

$$\frac{}{Q\ a : a = a}\,(A : U), (a : A)$$

- And the corresponding eliminator $R_=$:
  $R_= : (\forall A : U)(\forall P : A \to U)(\forall a : A)(P\ a) \to (\forall b : A) a = b \to P\ b$

$$\frac{H_1 : P\ a \qquad H_2 : a = b}{R_=\ A\ P\ a\ H_1\ b\ H_2 : P\ b}\,(A : U), (P : A \to U), (a, b : A)$$

Recap: Equality

- Last week we have seen several definitions of equality.
- From now on, we use inductive equality:

$$\frac{}{Q\ a : a = a}\ (A : U), (a : A)$$

- And the corresponding eliminator $R_=$:
  $R_= : (\forall A : U)(\forall P : A \to U)(\forall a : A)(P\ a) \to (\forall b : A)a = b \to P\ b$

$$\frac{H_1 : P\ a \qquad H_2 : a = b}{R_=\ A\ P\ a\ H_1\ b\ H_2 : P\ b}\ (A : U), (P : A \to U), (a, b : A)$$

Peano S 0

The first Peano Axioms

The natural numbers are well defined

Zero is a natural number:

$0 : \mathbb{N}$

The successor of each natural number is a natural number:

$(\forall n)(n : \mathbb{N}) \to (Sn : \mathbb{N})$

True by the definition of $\mathbb{N}$

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

The first Peano Axioms

The natural numbers are well defined

Zero is a natural number:

$0 : \mathbb{N}$

The successor of each natural number is a natural number:

$(\forall n)(n : \mathbb{N}) \to (Sn : \mathbb{N})$

True by the definition of $\mathbb{N}$

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

The first Peano Axioms

The natural numbers are well defined

Zero is a natural number:

$0 : \mathbb{N}$

The successor of each natural number is a natural number:

$(\forall n)(n : \mathbb{N}) \to (Sn : \mathbb{N})$

True by the definition of $\mathbb{N}$

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

Proof of Disjointness

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda \_.U)\bot(\lambda \_.\top)m)\ (Sn)\ I\ 0\ H$$

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

$$\bot$$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)\ (Sn)\ I\ 0\ H$$

Proof of Disjointness

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

$$\frac{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)0}{\bot}$$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)\ (Sn)\ I\ 0\ H$$

Proof of Disjointness

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

$$\dfrac{\dfrac{(\lambda m.R_{\mathbb{N}}(\lambda \_.U)\bot(\lambda \_.\top)m)Sn \qquad Sn = 0}{(\lambda m.R_{\mathbb{N}}(\lambda \_.U)\bot(\lambda \_.\top)m)0}\; R_{=}}{\bot}$$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda \_.U)\bot(\lambda \_.\top)m)\ (Sn)\ I\ 0\ H$$

Proof of Disjointness

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

$$\dfrac{\dfrac{\top}{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)Sn} \qquad Sn = 0}{\dfrac{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)0}{\bot}}\; R_{=}$$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)\ (Sn)\ I\ 0\ H$$

Proof of Disjointness

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\top}\,I}{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)Sn} \qquad \dfrac{}{Sn = 0}\,H}{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)0}\,R_{=}}{\bot}$$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)\ (Sn)\ I\ 0\ H$$

Proof of Disjointness

Disjointness

Zero is not the successor of any number:

$(\forall n : \mathbb{N}) Sn \neq 0$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\top}\,I}{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)Sn} \qquad \dfrac{}{Sn = 0}\,H}{(\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)0}\,R_{=}}{\bot}$$

The resulting proof term:

$$\lambda n\ H.R_{=}\ \mathbb{N}\ (\lambda m.R_{\mathbb{N}}(\lambda\_.U)\bot(\lambda\_.\top)m)\ (Sn)\ I\ 0\ H$$

Injectivity

Injectivity

Two numbers are equal if their successors are equal:

$$(\forall n, m : \mathbb{N}) Sn = Sm \to n = m$$

The predecessor

$\pi := R_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda m.m)n$

$\pi 0 \succ R_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda m.m)0) \succ 0$

$\pi(Sn) \succ R_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda m.m)(Sn) \succ n$

Injectivity

Injectivity

Two numbers are equal if their successors are equal:

$(\forall n, m : \mathbb{N}) Sn = Sm \to n = m$

The predecessor

$\pi := R_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda m.m)n$

$\pi 0 \succ R_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda m.m)0) \succ 0$

$\pi(Sn) \succ R_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda m.m)(Sn) \succ n$

Proof of Injectivity

$$n = m$$

Proof of Injectivity

$$\frac{\pi(Sn) = m \qquad \pi(Sn) = n}{n = m} \, R_=$$

Proof of Injectivity

$$\dfrac{\dfrac{\pi(Sn) = \pi(Sm) \qquad \pi(Sm) = m}{\pi(Sn) = m}\,R_{=} \qquad \pi(Sn) = \mathrm{n}}{n = m}\,R_{=}$$

Proof of Injectivity

$$\cfrac{\cfrac{\cfrac{\pi(Sn) = \pi(Sn) \qquad Sn = Sm}{\pi(Sn) = \pi(Sm)}\, R_= \qquad \pi(Sm) = m}{\pi(Sn) = m}\, R_= \qquad \pi(Sn) = n}{n = m}\, R_=$$

Proof of Injectivity

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\pi(Sn)=\pi(Sn)}\,Q \qquad \dfrac{}{Sn=Sm}\,H}{\pi(Sn)=\pi(Sm)}\,R_{=} \qquad \pi(Sm)=m}{\pi(Sn)=m}\,R_{=} \qquad \pi(Sn)=n}{n=m}\,R_{=}$$

Proof of Injectivity

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\pi(Sn) = \pi(Sn)}\,Q \qquad \dfrac{}{Sn = Sm}\,H}{\pi(Sn) = \pi(Sm)}\,R_= \qquad \pi(Sm) = m}{\pi(Sn) = m}\,R_= \qquad \pi(Sn) = n}{n = m}\,R_=
$$

The resulting proof term:

$$
\begin{aligned}
\lambda n\ m\ H.R_=(\lambda k.k = m)(\pi(Sn))& \\
&(R_=(\lambda k.\pi(Sn) = k)(\pi(Sm)) \\
&\quad (R_=(\lambda k.\pi(Sn) = \pi k)(Sn)Q(Sm)H) \\
&m(\text{predS } m)) \\
&n(\text{predS } n)
\end{aligned}
$$

Induction I

- In ZF induction follows by definition of the natural numbers
- Recursion (computation) must be proven by a theorem!
- Comes for free in type theory: recursion = induction
- Induction extends case distinction by assumption:

Induction I

- In ZF induction follows by definition of the natural numbers
- Recursion (computation) must be proven by a theorem!
- Comes for free in type theory: recursion = induction
- Induction extends case distinction by assumption:

Induction I

- In ZF induction follows by definition of the natural numbers
- Recursion (computation) must be proven by a theorem!
- Comes for free in type theory: recursion = induction
- Induction extends case distinction by assumption:

Induction I

- In ZF induction follows by definition of the natural numbers
- Recursion (computation) must be proven by a theorem!
- Comes for free in type theory: recursion = induction
- Induction extends case distinction by assumption:

Remember the elimination rule $R_{\mathbb{N}}$:
$R_{\mathbb{N}} : (\forall P : \mathbb{N} \to U) P0 \to ((\forall n : \mathbb{N}) P(Sn)) \to (\forall n : \mathbb{N}) Pn$

$$\frac{H : P\ 0 \qquad f : (\forall m : \mathbb{N}) P(Sm)}{R_{\mathbb{N}}\ P\ \ H\ f : (\forall n : \mathbb{N}) P\ n}\ P : \mathbb{N} \to U$$

Induction I

- In ZF induction follows by definition of the natural numbers
- Recursion (computation) must be proven by a theorem!
- Comes for free in type theory: recursion = induction
- Induction extends case distinction by assumption:

Extended to induction rule $I_{\mathbb{N}}$:
$I_{\mathbb{N}} : (\forall P : \mathbb{N} \to U) P0 \to ((\forall n : \mathbb{N}) P\ n \to P(Sn)) \to (\forall n : \mathbb{N}) Pn$

$$\frac{H : P\ 0 \qquad f : (\forall m : \mathbb{N}) P\ m \to P(Sm)}{I_{\mathbb{N}}\ P\ \ H\ f : (\forall n : \mathbb{N}) P\ n}\ P : \mathbb{N} \to U$$

Induction II

Induction for $\mathbb{N}$

$(\forall P : \mathbb{N} \to U) P\ 0 \to ((\forall n : \mathbb{N}) P\ n \to P(Sn)) \to (\forall n : \mathbb{N}) P\ n$

Proof

Exactly $I_{\mathbb{N}}$

Case distinction is redundant

We can define case distinction by induction.

Proof: Exercise.

Induction II

Induction for $\mathbb{N}$

$(\forall P : \mathbb{N} \to U) P\ 0 \to ((\forall n : \mathbb{N}) P\ n \to P(Sn)) \to (\forall n : \mathbb{N}) P\ n$

Proof

Exactly $I_{\mathbb{N}}$

Case distinction is redundant

We can define case distinction by induction.

Proof: Exercise.

Induction II

Induction for $\mathbb{N}$

$(\forall P : \mathbb{N} \to U) P\ 0 \to ((\forall n : \mathbb{N}) P\ n \to P(Sn)) \to (\forall n : \mathbb{N}) P\ n$

Proof

Exactly $I_{\mathbb{N}}$

Case distinction is redundant

We can define case distinction by induction.

Proof: Exercise.

Less or Equal

Less or Equal – Definition

- We have seen an intuitive ordering of the numbers in ZF-set theory (i.e. $\in$).
- Does such a relation come for free in type theory?

Less or Equal – Definition

- We have seen an intuitive ordering of the numbers in ZF-set theory (i.e. $\in$).
- Does such a relation come for free in type theory?

Less or Equal – Definition

- We have seen an intuitive ordering of the numbers in ZF-set theory (i.e. $\in$).
- Does such a relation come for free in type theory? No!

Less or Equal – Definition

- We have seen an intuitive ordering of the numbers in ZF-set theory (i.e. $\in$).
- Does such a relation come for free in type theory? No!

Define $\leq$ as an inductive predicate ($\approx$ type):

$$\frac{}{n \leq n}\ (\text{le1}) \text{ with } n : \mathbb{N}$$

$$\frac{m : \mathbb{N} \qquad n \leq m}{n \leq Sm}\ (\text{le2}) \text{ with } n : \mathbb{N}$$

Less or Equal – Definition

- We have seen an intuitive ordering of the numbers in ZF-set theory (i.e. $\in$).
- Does such a relation come for free in type theory? No!

Define $\leq$ as an inductive predicate ($\approx$ type):

$$\frac{}{n \leq n}\ (\text{le1}) \text{ with } n : \mathbb{N}$$

$$\frac{m : \mathbb{N} \qquad n \leq m}{n \leq Sm}\ (\text{le2}) \text{ with } n : \mathbb{N}$$

This definition is not unique, but complete and sound!

Less or Equal – Induction

We have already seen “normal” induction and the inductive equality. Apply these concepts to more complicated types (i.e. predicates).

Induction Lemma for $\leq$

$I_{\leq}$ is of type
$(\forall(n:\mathbb{N})(P:\mathbb{N}\to U))\ P\ n \to ((\forall m:\mathbb{N})n\leq m \to P\ m \to P(Sm)) \to (\forall k:\mathbb{N})n\leq k \to P\ k$

$$\frac{H_1 : P\ n \qquad f:(\forall m:\mathbb{N})n\leq m\to P\ m\to P(Sm) \qquad H_2 : n\leq m}{I_{\leq}\ n\ P\ H_1\ f\ m\ H_2 : P\ m}\ (n,m:\mathbb{N})$$

Less or Equal – Induction

We have already seen "normal" induction and the inductive equality.
Apply these concepts to more complicated types (i.e. predicates).

Induction Lemma for $\leq$

$I_{\leq}$ is of type
$(\forall(n:\mathbb{N})(P:\mathbb{N}\to U))\ P\ n \to ((\forall m:\mathbb{N})n\leq m \to P\ m \to P(Sm)) \to (\forall k:\mathbb{N})n\leq k \to P\ k$

$$\frac{H_1 : P\ n \qquad f : (\forall m:\mathbb{N})n\leq m \to P\ m \to P(Sm) \qquad H_2 : n \leq m}{I_{\leq}\ n\ P\ H_1\ f\ m\ H_2 : P\ m}\,(n, m : \mathbb{N})$$

Less or Equal – Induction

We have already seen "normal" induction and the inductive equality.
Apply these concepts to more complicated types (i.e. predicates).

Induction Lemma for $\leq$

$I_{\leq}$ is of type
$(\forall(n:\mathbb{N})(P:\mathbb{N}\to U))\ P\ n \to ((\forall m:\mathbb{N})n\leq m \to P\ m \to P(Sm)) \to (\forall k:\mathbb{N})n\leq k \to P\ k$

$$\frac{H_1 : P\ n \qquad f : (\forall m:\mathbb{N})n\leq m \to P\ m \to P(Sm) \qquad H_2 : n \leq m}{I_{\leq}\ n\ P\ H_1\ f\ m\ H_2 : P\ m}\ (n, m:\mathbb{N})$$

Peano S(S 0)

More Peano Axioms

Reflexivity

$(\forall n : \mathbb{N}) n \leq n$

Proof: Exactly the first constructor of $\leq$.

Transitivity

$(\forall n, m, k : \mathbb{N}) n \leq m \to m \leq k \to n \leq k$

Proof: Exercise.

Antisymmetry

$(\forall n, m : \mathbb{N}) n \leq m \to m \leq n \to n = m$

More Peano Axioms

Reflexivity

$(\forall n : \mathbb{N}) n \leq n$

Proof: Exactly the first constructor of $\leq$.

Transitivity

$(\forall n, m, k : \mathbb{N}) n \leq m \to m \leq k \to n \leq k$

Proof: Exercise.

Antisymmetry

$(\forall n, m : \mathbb{N}) n \leq m \to m \leq n \to n = m$

More Peano Axioms

Reflexivity

$(\forall n : \mathbb{N}) n \leq n$

Proof: Exactly the first constructor of $\leq$.

Transitivity

$(\forall n, m, k : \mathbb{N}) n \leq m \to m \leq k \to n \leq k$

Proof: Exercise.

Antisymmetry

$(\forall n, m : \mathbb{N}) n \leq m \to m \leq n \to n = m$

Proof of Antisymmetry

We use the following unproven lemma:

Lemma

$(\forall n : \mathbb{N}) Sn \leq 0 \rightarrow \bot$

Proof by induction on n and case distinction of m:

- $n = 0, m = 0$: Show: $0 \leq 0 \rightarrow 0 \leq 0 \rightarrow 0 \leq 0$ ✓
- $n = 0, m = Sm'$: Show $0 \leq Sm' \rightarrow Sm' \leq 0 \rightarrow 0 = Sm'$
  ✓ by lemma and exfalso
- $n = Sn', m = 0$: Show $Sn' \leq 0 \rightarrow 0 \leq Sn' \rightarrow Sn' = 0$
  ✓ by lemma and exfalso
- $n = Sn', m = Sm'$: $IH : (\forall m : \mathbb{N}) n' \leq m \rightarrow m \leq n' \rightarrow n' = m$.
  Show: $Sn' \leq Sm' \rightarrow Sm' \leq Sn' \rightarrow Sn' = Sm'$.
  ✓ by injectivity and IH.

Proof of Antisymmetry

We use the following unproven lemma:

Lemma

$(\forall n : \mathbb{N}) Sn \leq 0 \to \bot$

Proof by induction on n and case distinction of m:

- $n = 0, m = 0$: Show: $0 \leq 0 \to 0 \leq 0 \to 0 \leq 0$ ✓
- $n = 0, m = Sm'$: Show $0 \leq Sm' \to Sm' \leq 0 \to 0 = Sm'$
  ✓ by lemma and exfalso
- $n = Sn', m = 0$: Show $Sn' \leq 0 \to 0 \leq Sn' \to Sn' = 0$
  ✓ by lemma and exfalso
- $n = Sn', m = Sm'$: $IH : (\forall m : \mathbb{N}) n' \leq m \to m \leq n' \to n' = m$.
  Show: $Sn' \leq Sm' \to Sm' \leq Sn' \to Sn' = Sm'$.
  ✓ by injectivity and IH.

Proof of Antisymmetry

We use the following unproven lemma:

Lemma

$(\forall n : \mathbb{N}) Sn \leq 0 \to \bot$

Proof by induction on n and case distinction of m:

- $n = 0, m = 0$: Show: $0 \leq 0 \to 0 \leq 0 \to 0 \leq 0$ ✓
- $n = 0, m = Sm'$: Show $0 \leq Sm' \to Sm' \leq 0 \to 0 = Sm'$
  ✓ by lemma and exfalso
- $n = Sn', m = 0$: Show $Sn' \leq 0 \to 0 \leq Sn' \to Sn' = 0$
  ✓ by lemma and exfalso
- $n = Sn', m = Sm'$: $IH : (\forall m : \mathbb{N}) n' \leq m \to m \leq n' \to n' = m$.
  Show: $Sn' \leq Sm' \to Sm' \leq Sn' \to Sn' = Sm'$.
  ✓ by injectivity and IH.

Proof of Antisymmetry

We use the following unproven lemma:

Lemma

$(\forall n : \mathbb{N}) Sn \leq 0 \rightarrow \bot$

Proof by induction on n and case distinction of m:

- $n = 0, m = 0$: Show: $0 \leq 0 \rightarrow 0 \leq 0 \rightarrow 0 \leq 0$ ✓
- $n = 0, m = Sm'$: Show $0 \leq Sm' \rightarrow Sm' \leq 0 \rightarrow 0 = Sm'$
  ✓ by lemma and exfalso
- $n = Sn', m = 0$: Show $Sn' \leq 0 \rightarrow 0 \leq Sn' \rightarrow Sn' = 0$
  ✓ by lemma and exfalso
- $n = Sn', m = Sm'$: $IH : (\forall m : \mathbb{N}) n' \leq m \rightarrow m \leq n' \rightarrow n' = m$.
  Show: $Sn' \leq Sm' \rightarrow Sm' \leq Sn' \rightarrow Sn' = Sm'$.
  ✓ by injectivity and IH.

Proof of Antisymmetry

We use the following unproven lemma:

Lemma

$(\forall n : \mathbb{N}) Sn \leq 0 \to \bot$

Proof by induction on n and case distinction of m:

- $n = 0, m = 0$: Show: $0 \leq 0 \to 0 \leq 0 \to 0 \leq 0$ ✓
- $n = 0, m = Sm'$: Show $0 \leq Sm' \to Sm' \leq 0 \to 0 = Sm'$
  ✓ by lemma and exfalso
- $n = Sn', m = 0$: Show $Sn' \leq 0 \to 0 \leq Sn' \to Sn' = 0$
  ✓ by lemma and exfalso
- $n = Sn', m = Sm'$: $IH : (\forall m : \mathbb{N}) n' \leq m \to m \leq n' \to n' = m$.
  Show: $Sn' \leq Sm' \to Sm' \leq Sn' \to Sn' = Sm'$.
  ✓ by injectivity and IH.

More Peano Axioms

Linearity

$(\forall n, m : \mathbb{N}) n \leq m \vee m \leq n$

Proof: By induction on n, case distinction on m, analysing the IH, and using $0 \leq n$ and $n \leq m \to Sn \leq Sm$ (left as exercise).

Definition of strictly less ($<$)

$n < m := Sn \leq m \quad (\forall n, m : \mathbb{N})$

Now we can define a variant of the classical induction:

Complete Induction

$(\forall P : \mathbb{N} \to U)((\forall n : \mathbb{N})((\forall m : \mathbb{N}) m < n \to P\ m) \to P\ n) \to (\forall n : \mathbb{N}) P\ n$

Proof

By induction on n. Details left as exercise.

More Peano Axioms

Linearity

$(\forall n, m : \mathbb{N}) n \leq m \vee m \leq n$

Proof: By induction on n, case distinction on m, analysing the IH, and using $0 \leq n$ and $n \leq m \to Sn \leq Sm$ (left as exercise).

Definition of strictly less ($<$)

$n < m := Sn \leq m \quad (\forall n, m : \mathbb{N})$

Now we can define a variant of the classical induction:

Complete Induction

$(\forall P : \mathbb{N} \to U)((\forall n : \mathbb{N})((\forall m : \mathbb{N}) m < n \to P\ m) \to P\ n) \to (\forall n : \mathbb{N}) P\ n$

Proof

By induction on n. Details left as exercise.

More Peano Axioms

Linearity

$(\forall n, m : \mathbb{N}) n \leq m \vee m \leq n$

Proof: By induction on n, case distinction on m, analysing the IH, and using $0 \leq n$ and $n \leq m \to Sn \leq Sm$ (left as exercise).

Definition of strictly less ($<$)

$n < m := Sn \leq m \quad (\forall n, m : \mathbb{N})$

Now we can define a variant of the classical induction:

Complete Induction

$(\forall P : \mathbb{N} \to U)((\forall n : \mathbb{N})((\forall m : \mathbb{N}) m < n \to P\ m) \to P\ n) \to$
$(\forall n : \mathbb{N}) P\ n$

Proof

By induction on n. Details left as exercise.

Wellfoundedness

- First attempt: Use classical approach:
  $(\forall \emptyset \neq P \subseteq \mathbb{N})(\exists n \in P)(\forall m \in P) n \leq m$
- How to instantiate the $\exists$?
  Only possible for decidable sets ($\hat{=}$ propositions).
- Need different approach!

Definition of inductive predicate WF

$$\frac{(\forall m : \mathbb{N}) m < n \rightarrow WF\ m}{WF\ n} \text{ (WFI) with } n : \mathbb{N}$$

Wellfoundedness

Every descending chain $n_1 > n_2 > \ldots$ is finite: $(\forall n : \mathbb{N}) WF\ n$

Wellfoundedness

- First attempt: Use classical approach:
  $(\forall \emptyset \neq P \subseteq \mathbb{N})(\exists n \in P)(\forall m \in P) n \leq m$
- How to instantiate the $\exists$?
  Only possible for decidable sets ($\triangleq$ propositions).
- Need different approach!

Definition of inductive predicate WF

$$\frac{(\forall m : \mathbb{N}) m < n \rightarrow WF\ m}{WF\ n} \text{ (WFI) with } n : \mathbb{N}$$

Wellfoundedness

Every descending chain $n_1 > n_2 > \dots$ is finite: $(\forall n : \mathbb{N}) WF\ n$

Wellfoundedness

- First attempt: Use classical approach:

  $(\forall \emptyset \neq P \subseteq \mathbb{N})(\exists n \in P)(\forall m \in P) n \leq m$
- How to instantiate the $\exists$?

  Only possible for decidable sets ($\hat{=}$ propositions).
- Need different approach!

Definition of inductive predicate WF

$$\frac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n} \text{ (WFI) with } n : \mathbb{N}$$

Wellfoundedness

Every descending chain $n_1 > n_2 > \ldots$ is finite: $(\forall n : \mathbb{N}) WF\ n$

Wellfoundedness

- First attempt: Use classical approach:
  $(\forall \emptyset \neq P \subseteq \mathbb{N})(\exists n \in P)(\forall m \in P) n \leq m$
- How to instantiate the $\exists$?
  Only possible for decidable sets ($\hat{=}$ propositions).
- Need different approach!

Definition of inductive predicate WF

$$\frac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n} \text{ (WFI) with } n : \mathbb{N}$$

Wellfoundedness

Every descending chain $n_1 > n_2 > \ldots$ is finite: $(\forall n : \mathbb{N}) WF\ n$

Wellfoundedness

- First attempt: Use classical approach:

  $(\forall \emptyset \neq P \subseteq \mathbb{N})(\exists n \in P)(\forall m \in P) n \leq m$
- How to instantiate the $\exists$?

  Only possible for decidable sets ($\hat{=}$ propositions).
- Need different approach!

Definition of inductive predicate WF

$$\frac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}\ \text{(WFI) with } n : \mathbb{N}$$

Wellfoundedness

Every descending chain $n_1 > n_2 > \ldots$ is finite: $(\forall n : \mathbb{N}) WF\ n$

Wellfoundedness

- First attempt: Use classical approach:

  $(\forall \emptyset \neq P \subseteq \mathbb{N})(\exists n \in P)(\forall m \in P) n \leq m$
- How to instantiate the $\exists$?

  Only possible for decidable sets ($\hat{=}$ propositions).
- Need different approach!

Definition of inductive predicate WF

$$\frac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}\ \text{(WFI) with } n : \mathbb{N}$$

Wellfoundedness

Every descending chain $n_1 > n_2 > \ldots$ is finite: $(\forall n : \mathbb{N}) WF\ n$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \equiv Sm \leq Sn \overset{\text{injectivity}}{\Longrightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m < n'}$: $n \equiv Sn' \Rightarrow$ Show $WF\ m$.

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \vdash Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH, it remains to show $m < n \succ Sm \leq Sn'$.
    ✓ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  $\checkmark$ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: $\checkmark$ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH, it remains to show $m < n \succ Sm \leq Sn'$
    $\checkmark$ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH', it remains to show $m < n \succ Sm \leq Sn'$
    ✓ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH, it remains to show $m < n \succ Sm \leq Sn'$.
    ✓ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH, it remains to show $m < n \succ Sm \leq Sn'$.
    ✓ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH, it remains to show $m < n \succ Sm \leq Sn'$.
    ✓ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness I

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Induction on n:

- $\mathbf{n = 0}$: Show $(\forall m : \mathbb{N}) m < 0 \to WF\ m$
  ✓ by $(\forall m : \mathbb{N}) Sm \leq 0 \to \bot$ and exfalso
- $\mathbf{n \to Sn}$: Given $IHn : WF\ n$. Show $(\forall m : \mathbb{N}) m < Sn \to WF\ m$.
  Let $m < Sn \succ Sm \leq Sn \overset{\text{injectivity}}{\Rightarrow} H : m \leq n$
  Now do a case distinction on H:
  - $\mathbf{m = n}$: ✓ IH is a solution
  - $\mathbf{m \leq n'}$: $n \mapsto Sn' \Rightarrow$ Show $WF\ m$.
    Using IH, it remains to show $m < n \succ Sm \leq Sn'$.
    ✓ since $(\forall n, m : \mathbb{N}) n \leq m \to Sn \leq Sm$

Proof of Wellfoundedness II

Want to show for all $n : \mathbb{N}$: $\dfrac{(\forall m : \mathbb{N}) m < n \to WF\ m}{WF\ n}$

Simplified proofterm:

$$
\begin{aligned}
&\lambda n. I_{\mathbb{N}}(\lambda k. WF\ k)\\
&\quad (WFI\ 0\ (\lambda m, H.\ \text{match (notEqualZero } m\ H) \text{ with end}))\\
&\quad (\lambda k, IHn. WFI(Sk)\\
&\qquad (\lambda m, H.\text{match (removeS } m\ k\ H) \text{ with}\\
&\qquad |le1\ \_ \mapsto \lambda IHk, \_. IHk\\
&\qquad |le2\ \_\ m'\ H1 \mapsto\\
&\qquad\quad \lambda IHk, \_.\\
&\qquad\quad (\text{match } IHk \text{ with } WFI\ \_\ x \mapsto x \text{ end}) m (leS\ m\ m'\ H1)\\
&\qquad \text{end } IHn\ H))n
\end{aligned}
$$

match $\widehat{=}$ syntactic sugar for use of eliminator

Working with Natural Numbers

Addition I

Definition of +

$(\forall n, m : \mathbb{N})\, \text{add}\ \ m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.Sk)n$

Example

$3 + 2 \succ^* \text{add}\ \ 3\ (S(S0)) \succ S(\text{add}\ \ 3\ (S0)) \succ S(S(\text{add}\ \ 3\ 0)) \succ S(S(3))$
$\succ^* S(S(S(S(S0)))) \succ^* 5$

Associativity

$(\forall n, m, k : \mathbb{N})\ (n + m) + k = n + (m + k)$

Follows by induction on k.

Addition I

Definition of $+$

$(\forall n, m : \mathbb{N})\,\text{add}\;\; m\;\; n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.Sk)n$

Example

$3 + 2 \succ^* \text{add}\;\; 3\;\; (S(S0)) \succ S(\text{add}\;\; 3\;\; (S0)) \succ S(S(\text{add}\;\; 3\;\; 0)) \succ S(S(3))$
$\succ^* S(S(S(S(S0)))) \succ^* 5$

Associativity

$(\forall n, m, k : \mathbb{N})\;\; (n + m) + k = n + (m + k)$

Follows by induction on k.

Addition I

Definition of +

$(\forall n, m : \mathbb{N})\,\mathsf{add}\ \ m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.Sk)n$

Example

$3 + 2 \succ^* \mathsf{add}\ \ 3\ (S(S0)) \succ S(\mathsf{add}\ \ 3\ (S0)) \succ S(S(\mathsf{add}\ \ 3\ 0)) \succ S(S(3))$
$\succ^* S(S(S(S(S0)))) \succ^* 5$

Associativity

$(\forall n, m, k : \mathbb{N})\ (n + m) + k = n + (m + k)$

Follows by induction on k.

Addition II

Peano Axioms for Addition

$(\forall n : \mathbb{N}) n + 0 = n$

$(\forall n, m : \mathbb{N}) n + Sm = S(n + m)$

While the above follows by computation and equality, the following needs induction:

Lemma for Addition

$(\forall n : \mathbb{N}) 0 + n = n$

$(\forall n, m : \mathbb{N}) Sn + m = S(n + m)$

Using these axioms and lemmas we can show:

Commutativity

$(\forall n, m : \mathbb{N}) n + m = m + n$

Proof: Exercise by proving the lemmas first.

Addition II

Peano Axioms for Addition

$(\forall n : \mathbb{N}) n + 0 = n$

$(\forall n, m : \mathbb{N}) n + Sm = S(n + m)$

While the above follows by computation and equality, the following needs induction:

Lemma for Addition

$(\forall n : \mathbb{N}) 0 + n = n$

$(\forall n, m : \mathbb{N}) Sn + m = S(n + m)$

Using these axioms and lemmas we can show:

Commutativity

$(\forall n, m : \mathbb{N}) n + m = m + n$

Proof: Exercise by proving the lemmas first.

Addition II

Peano Axioms for Addition

$(\forall n : \mathbb{N}) n + 0 = n$

$(\forall n, m : \mathbb{N}) n + Sm = S(n + m)$

While the above follows by computation and equality, the following needs induction:

Lemma for Addition

$(\forall n : \mathbb{N}) 0 + n = n$

$(\forall n, m : \mathbb{N}) Sn + m = S(n + m)$

Using these axioms and lemmas we can show:

Commutativity

$(\forall n, m : \mathbb{N}) n + m = m + n$

Proof: Exercise by proving the lemmas first.

Multiplication

As in all other encodings: We use addition to define multiplication:

Definition of $*$

$(\forall m, n : \mathbb{N})\text{mult } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda\_k.k + m)n$

This definition satisfies the usual properties:

Peano Axioms for Multiplication

$(\forall m : \mathbb{N})m * 0 = 0$

$(\forall n, m : \mathbb{N})m * Sn = (m * n) + m$

Other lemmas can also be shown (most of them by induction).

Multiplication

As in all other encodings: We use addition to define multiplication:

Definition of $*$

$(\forall m, n : \mathbb{N})\text{mult } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda\_k.k + m)n$

This definition satisfies the usual properties:

Peano Axioms for Multiplication

$(\forall m : \mathbb{N})m * 0 = 0$

$(\forall n, m : \mathbb{N})m * Sn = (m * n) + m$

Other lemmas can also be shown (most of them by induction).

Multiplication

As in all other encodings: We use addition to define multiplication:

Definition of $*$

$(\forall m, n : \mathbb{N})\text{mult } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})0(\lambda\_k.k + m)n$

This definition satisfies the usual properties:

Peano Axioms for Multiplication

$(\forall m : \mathbb{N})m * 0 = 0$
$(\forall n, m : \mathbb{N})m * Sn = (m * n) + m$

Other lemmas can also be shown (most of them by induction).

Subtraction I

This definition of numbers works out very well and is easy to use.
Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0))$$
$$\succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$
$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0))$$
$$\succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0))$

$\succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$

$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0))$

$\succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda \_.\mathbb{N})m(\lambda \_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0))$$
$$\succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$
$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0))$$
$$\succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction I

This definition of numbers works out very well and is easy to use.

Why not extend the system to subtraction?

$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda \_.\mathbb{N})m(\lambda \_k.\pi\ k)n$

Example

$$\begin{aligned} 1 - 2 &\succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \\ &\succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0 \\ 2 - 2 &\succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \\ &\succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0 \end{aligned}$$

Subtraction I

This definition of numbers works out very well and is easy to use.
Why not extend the system to subtraction?
$\Rightarrow$ We have to deal with negative numbers!

$\Rightarrow$ Use truncating minus ignoring negative numbers!

Definition of truncating $-$

$(\forall m, n : \mathbb{N})\text{minus } m\ n := I_{\mathbb{N}}(\lambda\_.\mathbb{N})m(\lambda\_k.\pi\ k)n$

Example

$$1 - 2 \succ^* \text{minus } 1\ (S(S0)) \succ \pi(\text{minus } 1\ (S0)) \succ \pi(\pi(\text{minus } 1\ 0)) \succ^* \pi(\pi(S0)) \succ \pi(0) \succ 0$$

$$2 - 2 \succ^* \text{minus } 2\ (S(S0)) \succ \pi(\text{minus } 2\ (S0)) \succ \pi(\pi(\text{minus } 2\ 0)) \succ^* \pi(\pi(S(S0))) \succ^* 0$$

Subtraction II

Proof of $\bot$

Same as before holds for $0 - 1$ and $1 - 1$: $\Rightarrow 0 - 1 = 0 = 1 - 1$.

Add 1 on both sides $\Rightarrow 0 - 1 + 1 = 1 - 1 + 1 \Rightarrow 0 = 1$

Subtraction II

Proof of $\bot$

Same as before holds for $0 - 1$ and $1 - 1$: $\Rightarrow 0 - 1 = 0 = 1 - 1$.
Add 1 on both sides $\Rightarrow 0 - 1 + 1 = 1 - 1 + 1 \Rightarrow 0 = 1$

$\lightning$ Because of the following:

No associativity and commutativity

The associativity and commutativity does not hold for expressions with minus and plus.

Associativity:
$1 + (1 - 2) \succ^* 1 + 0 \succ^* 1$
$(1 + 1) - 2 \succ^* 2 - 2 \succ^* 0$

Commutativity:
$(1 + 2) - 2 \succ^* 3 - 2 \succ^* 1$
$(1 - 2) + 2 \succ^* 0 + 2 \succ^* 2$

Subtraction II

Proof of $\bot$

Same as before holds for $0 - 1$ and $1 - 1$: $\Rightarrow 0 - 1 = 0 = 1 - 1$.
Add 1 on both sides $\Rightarrow 0 - 1 + 1 = 1 - 1 + 1 \Rightarrow 0 = 1$

$\lightning$ Because of the following:

No associativity and commutativity

The associativity and commutativity does not hold for expressions with minus and plus.

Associativity:

$1 + (1 - 2) \succ^* 1 + 0 \succ^* 1$

$(1 + 1) - 2 \succ^* 2 - 2 \succ^* 0$

Commutativity:

$(1 + 2) - 2 \succ^* 3 - 2 \succ^* 1$

$(1 - 2) + 2 \succ^* 0 + 2 \succ^* 2$

Subtraction III

No associativity and commutativity between $+$ and $-$. But nevertheless:

Truncating minus is sound

1. $(\forall m : \mathbb{N}) m - 0 = m$
2. $(\forall n, m : \mathbb{N})(m + n) - n = m$
3. $(\forall n : \mathbb{N}) n - n = 0$

And therefore $(\forall n, m : \mathbb{N})(m + n) - n = m + (n - n)$.

How to read: Truncating minus is not too much wrong.

There are ways to encode negative numbers defining them according to the definition on paper: e.g. $\mathbb{N} \times \mathbb{N}, \mathbb{N} + \mathbb{N}, \mathbb{B} \times \mathbb{N}$

Subtraction III

No associativity and commutativity between $+$ and $-$. But nevertheless:

Truncating minus is sound

1. $(\forall m : \mathbb{N}) m - 0 = m$
2. $(\forall n, m : \mathbb{N})(m + n) - n = m$
3. $(\forall n : \mathbb{N}) n - n = 0$

And therefore $(\forall n, m : \mathbb{N})(m + n) - n = m + (n - n)$.

How to read: Truncating minus is not too much wrong.

There are ways to encode negative numbers defining them according to the definition on paper: e.g. $\mathbb{N} \times \mathbb{N}, \mathbb{N} + \mathbb{N}, \mathbb{B} \times \mathbb{N}$

Conclusion

Conclusion – Comparison to ZF

The Good

- Recursion and induction is built-in
- Ideas can be directly extended to lists
- There are tools for working in type theory

The Bad

- Comparison is not built-in
- Size of proof terms grow fast
- Inherits all "problems" of type theory (e.g. no XM)

General Problems

- Correct/Complete subtraction requires a bit more work
- Yet another way for a foundation

Conclusion – Comparison to ZF

The Good

- Recursion and induction is built-in
- Ideas can be directly extended to lists
- There are tools for working in type theory

The Bad

- Comparison is not built-in
- Size of proof terms grow fast
- Inherits all "problems" of type theory (e.g. no XM)

General Problems

- Correct/Complete subtraction requires a bit more work
- Yet another way for a foundation

Conclusion – Comparison to ZF

The Good

- Recursion and induction is built-in
- Ideas can be directly extended to lists
- There are tools for working in type theory

The Bad

- Comparison is not built-in
- Size of proof terms grow fast
- Inherits all “problems” of type theory (e.g. no XM)

General Problems

- Correct/Complete subtraction requires a bit more work
- Yet another way for a foundation

Questions?

Exercises

1. Show that case distinction is not necessary.
2. Remember that we defined complete induction in the following way: $(\forall P : \mathbb{N} \to U)((\forall n : \mathbb{N})((\forall m : \mathbb{N})m < n \to P\ m) \to P\ n) \to (\forall n : \mathbb{N})P\ n$. Give a proof (term).
3. To show the linearity we used the following unproven lemma: $(\forall n, m : \mathbb{N}) : n \leq m \to Sn \leq Sm$.
   Now prove this lemma.
4. In the following we show that our definition of addition is commutative.
   - Show $(\forall n : \mathbb{N})0 + n = n$
   - Show $(\forall n, m : \mathbb{N})Sn + m = S(n + m)$
   - Now conclude that $(\forall n, m : \mathbb{N})n + m = m + n$).
5. Proof that $\leq$ is transitive.
   Hint: Doing an induction on a number is probably not the best idea!

References

Dominik Kirst. "Foundations of Mathematics: A Discussion of Sets and Types". Bachelor's Thesis. Saarland University, 2018.

Per Martin-Löf. *Intuitionistic Type Theory: Notes by Giovanni Sambin of a Series of Lectures Given in Padua, June 1980*. Prometheus Books, Napoli, June 1985.

Gert Smolka. *Introduction to Computational Logic - Lecture Notes*. Summer 2018.