$\mathbb{N}$ from $\mathbb{Z}$

Christian Sattler & David Wärn

Terminology

$\mathbb{N}$ is any type freely generated by:

- an element $0 : \mathbb{N}$,
- a self-map $S : \mathbb{N} \to \mathbb{N}$.

Terminology

$\mathbb{N}$ is any type freely generated by:

- an element $0 : \mathbb{N}$,
- a self-map $S : \mathbb{N} \to \mathbb{N}$.

$\mathbb{Z}$ is any type freely generated by:

- an element $0 : \mathbb{Z}$,
- a self-*equivalence* $S : \mathbb{Z} \to \mathbb{Z}$.

$\mathbb{Z}$-induction

Given

- $P : \mathbb{Z} \to \mathsf{U}$,
- $0_P : P(0)$,
- $S_P : (x : \mathbb{Z}) \to P(x) \simeq P(S(x))$,

obtain

- $p : (x : \mathbb{Z}) \to P(x)$,
- $p(0) = 0_P$,
- $p(S(x)) = S_P(p(x))$.

Our result

Our setting is type theory with:

- $\mathbf{1}$, Σ, $=$
- Π with funext
- $\mathbf{2}$ with large elimination (or descent)

Our result

Our setting is type theory with:

- $\mathbf{1}$, Σ, $=$
- Π with funext
- $\mathbf{2}$ with large elimination (or descent)

Theorem (Sattler and W.)

Given $\mathbb{Z}$, can construct $\mathbb{N}$.

We have two proofs. We present one of them in this talk.

Motivation

Where does $\mathbb{Z}$ come from?

Motivation

Where does $\mathbb{Z}$ come from?

Theorem

If S^1 has large elimination, then ΩS^1 is freely generated by:

- $\mathsf{refl} : \Omega S^1$
- $- \cdot \mathsf{loop} : \Omega S^1 \simeq \Omega S^1$

Motivation

Where does $\mathbb{Z}$ come from?

Theorem

If S^1 has large elimination, then ΩS^1 is freely generated by:

- $\mathsf{refl} : \Omega S^1$
- $- \cdot \mathsf{loop} : \Omega S^1 \simeq \Omega S^1$

Thus $\Omega S^1 = \mathbb{Z}$.

Previous work

Rijke–Shulman 17: construct $\mathbb{N}$ from $\mathbb{Z}$ given impredicative Prop *and* a universe

Previous work

Rijke–Shulman 17: construct $\mathbb{N}$ from $\mathbb{Z}$ given impredicative Prop *and* a universe

Rose 20: constructs $\mathbb{N}$ from $\mathbb{Z}$ given a univalent universe

Previous work

Rijke–Shulman 17: construct $\mathbb{N}$ from $\mathbb{Z}$ given impredicative Prop *and* a universe

Rose 20: constructs $\mathbb{N}$ from $\mathbb{Z}$ given a univalent universe

Rasekh 21: constructs $\mathbb{N}$ from $\mathbb{Z}$ given impredicative Prop

Previous work

Rijke–Shulman 17: construct $\mathbb{N}$ from $\mathbb{Z}$ given impredicative Prop *and* a universe

Rose 20: constructs $\mathbb{N}$ from $\mathbb{Z}$ given a univalent universe

Rasekh 21: constructs $\mathbb{N}$ from $\mathbb{Z}$ given impredicative Prop

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Given $\mathbb{N}$, can construct $\mathbb{Z}$ as follows:

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Given $\mathbb{N}$, can construct $\mathbb{Z}$ as follows:

- have $\mathbf{1} + \mathbb{N} \simeq \mathbb{N}$,

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Given $\mathbb{N}$, can construct $\mathbb{Z}$ as follows:

- have $\mathbf{1} + \mathbb{N} \simeq \mathbb{N}$,
- so $\mathbb{N} + \mathbf{1} + \mathbb{N} \simeq \mathbb{N} + (\mathbf{1} + \mathbb{N}) \simeq (\mathbb{N} + \mathbf{1}) + \mathbb{N} \simeq \mathbb{N} + \mathbf{1} + \mathbb{N}$,

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Given $\mathbb{N}$, can construct $\mathbb{Z}$ as follows:

- have $\mathbf{1} + \mathbb{N} \simeq \mathbb{N}$,
- so $\mathbb{N} + \mathbf{1} + \mathbb{N} \simeq \mathbb{N} + (\mathbf{1} + \mathbb{N}) \simeq (\mathbb{N} + \mathbf{1}) + \mathbb{N} \simeq \mathbb{N} + \mathbf{1} + \mathbb{N}$,
- together with $* : \mathbf{1}$ this gives $\mathbb{Z} \to \mathbb{N} + \mathbf{1} + \mathbb{N}$.

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Given $\mathbb{N}$, can construct $\mathbb{Z}$ as follows:

- have $\mathbf{1} + \mathbb{N} \simeq \mathbb{N}$,
- so $\mathbb{N} + \mathbf{1} + \mathbb{N} \simeq \mathbb{N} + (\mathbf{1} + \mathbb{N}) \simeq (\mathbb{N} + \mathbf{1}) + \mathbb{N} \simeq \mathbb{N} + \mathbf{1} + \mathbb{N}$,
- together with $* : \mathbf{1}$ this gives $\mathbb{Z} \to \mathbb{N} + \mathbf{1} + \mathbb{N}$.

Idea

How are $\mathbb{N}$ and $\mathbb{Z}$ related?

Given $\mathbb{N}$, can construct $\mathbb{Z}$ as follows:

- have $\mathbf{1} + \mathbb{N} \simeq \mathbb{N}$,
- so $\mathbb{N} + \mathbf{1} + \mathbb{N} \simeq \mathbb{N} + (\mathbf{1} + \mathbb{N}) \simeq (\mathbb{N} + \mathbf{1}) + \mathbb{N} \simeq \mathbb{N} + \mathbf{1} + \mathbb{N}$,
- together with $* : \mathbf{1}$ this gives $\mathbb{Z} \to \mathbb{N} + \mathbf{1} + \mathbb{N}$.

This characterizes *negative*, *zero*, and *positive* integers.

Idea

Same works given *any* types A and B with $A + B \simeq B$ and $* : A$.

Idea

Same works given *any* types A and B with $A + B \simeq B$ and $* : A$.

Lemma

$\mathbb{Z} + \mathbb{Z} \simeq \mathbb{Z}$.

Proof.

Via doubling and halving (direct integer induction). $\square$

Idea

Same works given *any* types A and B with $A + B \simeq B$ and $* : A$.

Lemma

$\mathbb{Z} + \mathbb{Z} \simeq \mathbb{Z}$.

Proof.

Via doubling and halving (direct integer induction). □

This induces:

- $\mathbb{Z} \to \mathbb{Z} + \mathbb{Z} + \mathbb{Z}$,
- hence sign : $\mathbb{Z} \to \mathbf{1} + \mathbf{1} + \mathbf{1}$,
- hence a decomposition $\mathbb{Z} \simeq \mathbb{Z}^- + \mathbb{Z}^0 + \mathbb{Z}^+$
  with $S(x) \in \mathbb{Z}^+$ iff $x \in \mathbb{Z}^0 + \mathbb{Z}^+$.

Idea

Aim: define $\mathbb{N}$ as Σ-type over $M \equiv_{\mathsf{def}} \mathbb{Z}^0 + \mathbb{Z}^+$.

Idea

Aim: define $\mathbb{N}$ as Σ-type over $M \equiv_{\mathsf{def}} \mathbb{Z}^0 + \mathbb{Z}^+$.

Both

- definition of $\mathbb{N}$
- derivation of $\mathbb{N}$-induction

use the idea of *partially defined inductive functions*.

Ordering

Can define subtraction $(-) : \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$ by integer induction.

Ordering

Can define subtraction $(-) : \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$ by integer induction.

Take $x \leq y$ to mean $x - y \in \mathbb{Z}^- + \mathbb{Z}^0$.

Ordering

Can define subtraction $(-) : \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$ by integer induction.

Take $x \leq y$ to mean $x - y \in \mathbb{Z}^- + \mathbb{Z}^0$.

Have:

- if $x \leq y$ then $x \leq S(y)$
- if $S(x) \leq y$ then $x \leq y$
- $S(x) \leq S(y)$ iff $x \leq y$
- $x \leq 0$ iff $x \in \mathbb{Z}^0$
- $x \leq x$

Inductive functions

Let $A : M \to \mathsf{U}$ with:

- $0_A : (x : \mathbb{Z}^0) \to A(x)$
- $S_A : (x : M) \to A(x) \to A(S(x))$

Inductive functions

Let $A : M \to \mathrm{U}$ with:

- $0_A : (x : \mathbb{Z}^0) \to A(x)$
- $S_A : (x : M) \to A(x) \to A(S(x))$

Define $B : M \to \mathrm{U}$ as

$$B(u) \equiv_{\mathsf{def}} (x : M) \to x \leq u \to A(x).$$

Inductive functions

Let $A : M \to \mathrm{U}$ with:

- $0_A : (x : \mathbb{Z}^0) \to A(x)$
- $S_A : (x : M) \to A(x) \to A(S(x))$

Define $B : M \to \mathrm{U}$ as

$$B(u) \equiv_{\mathsf{def}} (x : M) \to x \leq u \to A(x).$$

Have canonical maps:

- $\mathsf{res}_u : B(S(u)) \to B(u)$
- $\mathsf{ext}_u : B(u) \to B(S(u))$

Inductive functions

Let $A : M \to \mathrm{U}$ with:

- $0_A : (x : \mathbb{Z}^0) \to A(x)$
- $S_A : (x : M) \to A(x) \to A(S(x))$

Define $B : M \to \mathrm{U}$ as

$$B(u) \equiv_{\mathsf{def}} (x : M) \to x \leq u \to A(x).$$

Have canonical maps:

- $\mathsf{res}_u : B(S(u)) \to B(u)$
- $\mathsf{ext}_u : B(u) \to B(S(u))$

Say $f : B(u)$ is *inductive* if $\mathsf{res}_u(\mathsf{ext}_u(f)) = f$.
Write $I(u)$ for type of inductive functions.

Rolling rule

For $t : X \to X$, let $\text{fix}(f) \equiv_{\text{def}} (x : X) \times (f(x) = x)$.

Rolling rule

For $t : X \to X$, let $\mathrm{fix}(f) \equiv_{\mathsf{def}} (x : X) \times (f(x) = x)$.

Lemma

$\mathrm{fix}(f \circ g) \simeq \mathrm{fix}(g \circ f)$ *for* $f : X \to Y$, $g : Y \to X$.

Rolling rule

For $t : X \to X$, let $\mathrm{fix}(f) \equiv_{\mathrm{def}} (x : X) \times (f(x) = x)$.

Lemma

$\mathrm{fix}(f \circ g) \simeq \mathrm{fix}(g \circ f)$ *for* $f : X \to Y$, $g : Y \to X$.

Proof.

Both types are equivalent to
$(x : X) \times (y : Y) \times (f(x) = y) \times (g(y) = x)$. □

Inductive functions (cont.)

$$
\begin{aligned}
I(0) &\simeq \mathsf{fix}(\mathsf{res}_0 \circ \mathsf{ext}_0) \\
&\simeq \mathsf{fix}(- \mapsto 0_A) \\
&\simeq \mathbf{1}
\end{aligned}
$$

Inductive functions (cont.)

$$\begin{aligned} I(0) &\simeq \mathsf{fix}(\mathsf{res}_0 \circ \mathsf{ext}_0) \\ &\simeq \mathsf{fix}(- \mapsto 0_A) \\ &\simeq \mathbf{1} \end{aligned}$$

$$\begin{aligned} I(S(u)) &\simeq \mathsf{fix}(\mathsf{res}_{S(u)} \circ \mathsf{ext}_{S(u)}) \\ &\simeq \mathsf{fix}(\mathsf{ext}_u \circ \mathsf{res}_u) \\ &\simeq \mathsf{fix}(res_u \circ \mathsf{ext}_u) \\ &\simeq I(u) \end{aligned}$$

Defining $\mathbb{N}$

Instantiate A as follows:

$$
\begin{aligned}
A(-) &\equiv_{\mathsf{def}} M \\
0_A(-) &\equiv_{\mathsf{def}} 0 \\
S_A(x) &\equiv_{\mathsf{def}} S(x)
\end{aligned}
$$

Defining $\mathbb{N}$

Instantiate A as follows:

$$\begin{aligned} A(-) &\equiv_{\mathsf{def}} M \\ 0_A(-) &\equiv_{\mathsf{def}} 0 \\ S_A(x) &\equiv_{\mathsf{def}} S(x) \end{aligned}$$

Then define naturals:

$$\begin{aligned} N(m) &\equiv_{\mathsf{def}} (f : I(m)) \times (f(m) = m) \\ \mathbb{N} &\equiv_{\mathsf{def}} (m : M) \times N(m) \end{aligned}$$

Defining $\mathbb{N}$

Instantiate A as follows:

$$\begin{aligned} A(-) &\equiv_{\text{def}} M \\ 0_A(-) &\equiv_{\text{def}} 0 \\ S_A(x) &\equiv_{\text{def}} S(x) \end{aligned}$$

Then define naturals:

$$\begin{aligned} N(m) &\equiv_{\text{def}} (f : I(m)) \times (f(m) = m) \\ \mathbb{N} &\equiv_{\text{def}} (m : M) \times N(m) \end{aligned}$$

Have:

- unique element $(0, 0_N)$ of $(m : \mathbb{Z}^0) \times N(m)$
- $S_N : (m : M) \to N(m) \simeq N(S(m))$

Deriving $\mathbb{N}$-induction

Given:

- $P : (m : M) \to N(m) \to \mathsf{U}$
- $0_P : P(0, 0_N)$
- $S_P : (m : M)\,(n : N(m)) \to P(m, n) \to P(S(m), S_N(n))$

Deriving $\mathbb{N}$-induction

Given:

- $P : (m : M) \to N(m) \to \mathsf{U}$
- $0_P : P(0, 0_N)$
- $S_P : (m : M)\,(n : N(m)) \to P(m, n) \to P(S(m), S_N(n))$

Instantiate A as follows:

$$\begin{aligned} A(-) &\equiv_{\text{def}} (n : N(m)) \to P(m, n) \\ 0_A &\equiv_{\text{def}} \ldots \\ S_A &\equiv_{\text{def}} \ldots \end{aligned}$$

Deriving $\mathbb{N}$-induction

Given:

- $P : (m : M) \to N(m) \to \mathsf{U}$
- $0_P : P(0, 0_N)$
- $S_P : (m : M)\,(n : N(m)) \to P(m, n) \to P(S(m), S_N(n))$

Instantiate A as follows:

$$A(-) \equiv_{\mathsf{def}} (n : N(m)) \to P(m, n)$$
$$0_A \equiv_{\mathsf{def}} \dots$$
$$S_A \equiv_{\mathsf{def}} \dots$$

Prove $(m : M) \to I(m)$ by $\mathbb{Z}$-induction.

Deriving $\mathbb{N}$-induction

Given:

- $P : (m : M) \to N(m) \to \mathsf{U}$
- $0_P : P(0, 0_N)$
- $S_P : (m : M)\,(n : N(m)) \to P(m, n) \to P(S(m), S_N(n))$

Instantiate A as follows:

$$\begin{aligned} A(-) &\equiv_{\text{def}} (n : N(m)) \to P(m, n) \\ 0_A &\equiv_{\text{def}} \ldots \\ S_A &\equiv_{\text{def}} \ldots \end{aligned}$$

Prove $(m : M) \to I(m)$ by $\mathbb{Z}$-induction.

Deduce $(m : M)\,(n : N(m)) \to P(m, n)$ compatible with 0_P and S_P.