Constructing $\mathbb{N}$ by S^1 induction

Robert Rose

Indiana University

rrose1@iu.edu

August 13, 2019

The problem

In Martin-Löf type theory and homotopy type theory, an "axiom of infinity" is given explicitly as a type of natural numbers with a combined principle for proof by induction and definition by recursion.

A couple of years ago, Rijke and Shulman conjectured that in HoTT, we have an axiom of infinity in the form of the higher inductive type S^1. Can ΩS^1 be used to construct the natural numbers inside of type theory?

I learned about this problem in the lead up to the 2017 AMS Mathematical Research Community on Homotopy Type Theory. In the intervening time, Mike's feedback has been vital.

Main result

Let $S1TT$ denote a Martin-Löf type theory whose type formers comprise Σ, Π, $=$, $\bot$, $\top$, $Bool$, $U_0, U_1, \ldots$ and $S1$.

Theorem

A natural number system is derivable in $S1TT$.

Specialization of S^1 induction

Given the following data:

- a family of types P over S^1
- a family of types b^* over the fiber $P(b)$
- a family of equivalences: for $x \colon P(b)$, $l^*(x) \colon b^*(x) \simeq b^*(tpt(P, l, x))$

the S^1 induction principle supplies a family of types Q which varies over both $a \colon S^1$ and $P(a)$, with proofs that

- $Q(b) = b^*$
- $Q(b, l, x) = l^*(x)$ for all $x \colon P(b)$

S^1 induction

When specialized to the case where P is the type of paths with a free endpoint, we get from

- $P_b \colon \Omega S^1 \to U_i$
- a family of equivalences $P_b(x) \simeq P_b(l \cdot x)$ for $x \colon \Omega S^1$

a family of types $P \colon \Sigma_{a \colon S^1}(a = b) \to U_i$ satisfying the expected equations.

Moreover, since the domain of P is contractible, we get a section of P_b just by showing that $P_b(\mathit{refl})$ is inhabited.

S^1 induction

Finally, from the data

- $P_b \colon \Omega S^1 \to U_i$
- a family of equivalences $P_b(x) \simeq P_b(l \cdot x)$ for $x \colon \Omega S^1$
- $P_b(\mathit{refl})$

we get a function $P \colon \Pi_{x \colon \Omega S^1} P(x)$ satisfying the expected equations.

If we take $s := l \cdot -$ and $z := \mathit{refl}$, this looks something like the induction principle for $\mathbb{N}$. But of course the fact that we require a family of equivalences instead of a family of functions means it is too weak to simply restrict somehow.

Nonetheless, we can heuristically view this principle as a means of defining "predicates" over ΩS^1, and so as a means of proving various properties of elements of ΩS^1.

Examples

What sorts of properties of ΩS^1 have we been able to prove this way?

- that l commutes with all loops in ΩS^1 : $x \mapsto l \cdot x = x \cdot l$
- that ΩS^1 is abelian : $x, y \mapsto y \cdot x = x \cdot y$
- fixing n, we can show that ΩS^1 has division by l^n with remainder: e.g., for $n = 2$, $x \mapsto \Sigma_{y : \Omega S^1}(x = y \cdot y) + (x = l \cdot y \cdot y)$
- fixing n, dividing a loop x^n by l^n yields x : e.g., for $n = 2$, $x \mapsto div_2(x \cdot x) = x$

Example: Divison by 2

The path algebra can be a hassle.

```
(q : l * x == y * y)
-> ((l [1,0,2] ! *unitl
               * ! (*invl [2,0,1] x)
               * *assoc
               * (! l [1,0,2] q)
               * ! *assoc
               * ((! (! l [1,0,2] *unitr)
                  * ! (! l [1,0,2] y [1,0,2] *invr)
                  * ! (! l [1,0,2] *assoc)
                  * ! (! l [1,0,2] com [2,0,1] ! l)
                  * (! l [1,0,2] *assoc)
                  * ! *assoc
                  * (*invl l [2,0,1] (y * ! l))
                  * *unitl)                            [2,0,1] y)
               * *assoc
               * ! *unitl
               * ! (*invr [2,0,1] y * ! l * y)
               * *assoc
               * l [1,0,2] ! *assoc)
* (l [1,0,2] ! *assoc)
```

Example: Divison by 2

```
* (l [1,0,2] (! *unitl
              * ! (*invl [2,0,1] l * ! l * y)
              * *assoc
              * (! l [1,0,2] (((l [1,0,2] ! (! *unitl
                                            * ! (*invr [2,0,1] y)
                                            * *assoc))
                               * com
                               * (! *unitl
                                  * ! (*invr [2,0,1] y)
                                  * *assoc)              [2,0,1] l)
                               * *assoc))
             * ! *assoc
             * (*invl [2,0,1] (! l * y) * l)
             * *unitl)                                      [2,0,1] ! l * y)
* (l [1,0,2] *assoc)
* ! *assoc)
* (! *assoc
   * (*invr [2,0,1] y)
   * *unitl)           [2,0,2] ! *assoc
                               * (*invr [2,0,1] y)
                               * *unitl

==
q
```

Non-examples

What are some properties which don't seem (directly) provable this way?

- that for a fixed loop x in ΩS^1, being equal to x is decidable: $y \mapsto y = x + (y = x \to \bot)$
- that ΩS^1 is a set (if you find otherwise, please let me know)

For decidable equality, the obstacle seems to be that the disequality is not informative enough. The intuitionistic negation $y = x \to \bot$ is insufficient to decide whether or not $l \cdot y = x$. Instead of $y = x \to \bot$, we'd like a measure of how different they are.

Intuition

Consider two elements of ΩS^1, l^{-2} and l^3. We can construct a finite sequence of elements l^{-2} and l^3 generated by the equivalence $l \cdot -$:

$$l^{-2}, l^{-1}, \mathit{refl}, l, l^2, l^3$$

In the process of producing this partial orbit, we might also generate a relation:

$$l^{-2} \longrightarrow l^{-1} \longrightarrow \mathit{refl} \longrightarrow l \longrightarrow l^2 \longrightarrow l^3$$

We can try to formalize a theory of such segments as a type family over $\Omega S^1 \times \Omega S^1$; the fibers of this type family would consist of structures interpreting the theory.

Intuition

Hence, we might constrain such a type family to get segments starting at *refl*:

$$\begin{gathered} \mathit{refl} \\ \mathit{refl}, l \\ \mathit{refl}, l, l^2 \\ \ldots \end{gathered}$$

And those non-trivial segments ending at *refl*:

$$\begin{aligned} l^{-1}, \mathit{refl} \\ l^{-1}, l^{-2}, \mathit{refl} \\ \ldots \end{aligned}$$

We'd like to show that every loop corresponds to a exactly one such segment.

Segments

To each type B, base point $b\colon B$, $x_{min}\colon \Omega B$, $x_{max}\colon \Omega B$ and equivalence $s : B \simeq B$, we associate a complicated Σ type each term of which contains the following data:

- a family of types $D\colon \Omega B \to U_0$
- $d_{min}\colon D(x_{min})$
- $d_{max}\colon D(x_{max})$
- a “binary” relation $R\colon \Pi_{(x_1\colon \Omega B, d_1\colon D(x_1), x_2\colon \Omega B, d_2\colon D(x_2))} hProp$
- a lot of more data ensuring that R projected to ΩS^1 is a finite segment from x_{min} to x_{max}

More data

Segments also include proofs that (eliding further scare quotes)

- R is irreflexive: $R(x_1, d_1, x_1, d_1') \to \bot$
- R is transitive: $R(x_1, d_1, x_2, d_2) \to R(x_2, d_2', x_3, d_3) \to R(x_1, d_1, x_3, d_3)$
- R is trichotomous: $R(x_1, d_1, x_2, d_2) + (x_1 = x_2) + R(x_2, d_2, x_1, d_1)$
- d_{min} is minimal: $x \neq x_{min} \to R(x_{min}, d_{min}, x, d)$
- d_{max} is maximal: $x \neq x_{max} \to R(x, d, x_{max}, d_{max})$
- R is generated by s: $R(x_1, d_1, s(x_1), d_2)$
- R is discrete wrt s: $R(x_1, d_1, x_2, d_2) \to R(x_2, d_2, s(x_1), d_3) \to \bot$
- R is up-closed and down-closed wrt s: $\Sigma_{d\,:\,D(x)} R(x, d, x_{max}, d_{max}) \simeq \Sigma_{d\,:\,D(s(x))} R(x_{min}, d_{min}, x, d)$
- D is asymmetric wrt *refl*: $x \neq \mathit{refl} \to D(x) \to D(x^{-1}) \to \bot$.

Specialized Segments

Take $B := S^1$ and the equivalence s to be left composition with l. Define

- $Seg_{\geq 0}$ to be a segment with $x_{min} = refl$
- $Seg_{>0}$ to be a segment with $x_{min} = refl$
  with additional datum $R(x_{min}, d_{min}, x_{max}, d_{max})$
- $Seg_{\leq 0}$ to be a segment with $x_{max} = refl$
- $Seg_{<0}$ to be a segment with $x_{max} = refl$
  with additional datum $R(x_{min}, d_{min}, x_{max}, d_{max})$
- Seg_{+0} to be a segment with $x_{min} = refl$
  with additional datum $R(x_{min}, d_{min}, x_{max}, d_{max}) \to \bot$
- Seg_{-0} to be a segment with $x_{max} = refl$
  with additional datum $R(x_{min}, d_{min}, x_{max}, d_{max}) \to \bot$

Negative or non-negative

Hence, we define the following second-order predicate of ΩS^1:

$$\begin{aligned} &P_b \colon \Omega S^1 \to U_1 \\ &P_b(x) := Seg_{<0}(x) + Seg_{\geq 0}(x) \end{aligned}$$

To apply S^1 induction so as to generalize P_b and prove that it holds of every element of ΩS^1, we need to show that $P_b(x) \simeq P_b(l \cdot x)$.

$P_b(x) \simeq P_b(I \cdot x)$

We obtain the desired family of equivalences from these components:

$$\begin{aligned}
&Seg_{<0}(x) + Seg_{\geq 0}(x) \simeq \\
&Seg_{\leq 0}(I \cdot x) + Seg_{>0}(I \cdot x) \simeq \\
&(Seg_{<0}(I \cdot x) + Seg_{-0}(I \cdot x)) + Seg_{>0}(I \cdot x) \simeq \\
&Seg_{<0}(I \cdot x) + (Seg_{+0}(I \cdot x) + Seg_{>0}(I \cdot x)) \simeq \\
&Seg_{<0}(I \cdot x) + Seg_{\geq 0}(I \cdot x) \simeq
\end{aligned}$$

Defining the equivalence $Seg_{\geq 0}(x) \simeq Seg_{>0}(I \cdot x)$ (and its negative reflection) is lengthy and contains some subtleties. In particular, one has to be careful about how to define the “increase max” and “decrease max” functions for non-negative segments so that they compose to the identities. (And likewise for “increase min” and “decrease min”.)

$P_b(x) \simeq P_b(l \cdot x)$

Note that we have not characterized finite segments purely in terms of order theoretic properties and the iteration of the equivalence. The asymmetry assumption allows us to exclude any model where l^{-2} is the max, *refl* is the min and every loop but l^{-1} is in the segment.

Moreover, some algebraic facts come into play crucially:

- $l \neq refl$
- $l^2 \neq refl$
- $l^3 \neq refl$
- l is odd
- l is in the center
- there are no elements of order 2

$P_b(\mathit{refl})$

We define a non-negative segment with *refl* for min and max as follows:

- $D(x) := (x = \mathit{refl})$
- $R(x1, d2, x2, d2) := \bot$
- trichotomy is obtained by composing paths from $D(x_1)$ and $D(x_2)$
- generation invokes the fact that $l \neq \mathit{refl}$

The rest of the properties more or less vacuously hold.

sign

Theorem

There exists a section $sign \colon \Pi_{x \colon \Omega S^1} Seg_{<0}(x) + Seg_{\geq 0}(x)$ *which computes as expected.*

Corollary

ΩS^1 *has decidable equality.*

Corollary

For all $x \colon \Omega S^1$*, the underlying type family of* $sign(x)$ *is a family of decidable propositions.*

$\mathbb{N}$

With *sign*, we can now define

$$\begin{aligned}&\mathbb{N} \colon U_0\\&\mathbb{N} := \Sigma_{(x \colon \Omega S^1)} \mathit{fst}(\mathit{sign}(x)) = \mathit{true}\end{aligned}$$

The usual first order properties of $\mathbb{N}$ are provable directly by reasoning about segments, and we are also able to define a total ordering $\leq$ on $\mathbb{N}$.

It remains to derive the induction principle for $\mathbb{N}$.

Approximations

Given

- $Q : N \to U_i$
- $z^* : Q(z)$
- $s^* : \Pi_{(n:N)} Q(n) \to Q(suc(n))$

an approximation is defined as an element of a type family over $x \colon \Omega S^1$:

- a function $a \colon \Pi_{(m \colon nat(x), n \colon \mathbb{N})}(n \leq (x, m)) \to Q(n)$
- a function $rz \colon \Pi_{(m \colon nat(x), r \colon z \leq (x,m))} a(m, z, r) = z^*$.
- a function $rs \colon \Pi_{(m \colon nat(x), r_1 \colon suc(n) \leq (x,m), r_2 \colon n \leq (x,m))} a(m, suc(n), r_1) = s^*(n, a(m, n, r_2))$.

Approximations

Note that whenever x is not a natural number, the type of approximations over x is contractible with center the triple of empty functions.

Hence, we again apply S^1 induction to obtain a section $a : \Pi_{x:\,\Omega S^1} approx(x)$, from which we may extract a section $ind\mathbb{N} : \Pi_{(n:\,\mathbb{N})} Q(n)$.