2.13 Natural numbers

Canonical name	213NaturalNumbers
Date of creation	2013-11-14 18:12:08
Last modified on	2013-11-14 18:12:08
Owner	PMBookProject (1000683)
Last modified by	rspuzio (6075)
Numerical id	2
Author	PMBookProject (6075)
Entry type	Feature
Classification	msc 03B15

We use the encode-decode method to characterize the path space of the natural numbers, which are also a positive type. In this case, rather than fixing one endpoint, we characterize the two-sided path space all at once. Thus, the codes for identities are a type family

$$\mathsf{code} : \mathbb{N} \to \mathbb{N} \to \mathcal{U},$$

defined by double recursion over $\mathbb{N}$ as follows:

$$\begin{aligned}
\mathsf{code}(0,0) &\equiv \mathbf{1} \\
\mathsf{code}(\mathsf{succ}(m),0) &\equiv \mathbf{0} \\
\mathsf{code}(0,\mathsf{succ}(n)) &\equiv \mathbf{0} \\
\mathsf{code}(\mathsf{succ}(m),\mathsf{succ}(n)) &\equiv \mathsf{code}(m,n).
\end{aligned}$$

We also define by recursion a dependent function $r : \prod_{(n:\mathbb{N})} \mathsf{code}(n,n)$, with

$$\begin{aligned}
r(0) &\equiv \star \\
r(\mathsf{succ}(n)) &\equiv r(n).
\end{aligned}$$

Theorem 2.13.1. *For all $m,n : \mathbb{N}$ we have $(m = n) \simeq \mathsf{code}(m,n)$.*

Proof. We define

$$\mathsf{encode} : \prod_{m,n:\mathbb{N}} (m = n) \to \mathsf{code}(m,n)$$

by transporting, $\mathsf{encode}(m,n,p) \equiv \mathsf{transport}^{\mathsf{code}(m,-)}(p, r(m))$. And we define

$$\mathsf{decode} : \prod_{m,n:\mathbb{N}} \mathsf{code}(m,n) \to (m = n)$$

by double induction on m,n. When m and n are both 0, we need a function $\mathbf{1} \to (0 = 0)$, which we define to send everything to refl_0. When m is a successor and n is 0 or vice versa, the domain $\mathsf{code}(m,n)$ is $\mathbf{0}$, so the eliminator for $\mathbf{0}$ suffices. And when both are successors, we can define $\mathsf{decode}(\mathsf{succ}(m),\mathsf{succ}(n))$ to be the composite

$$\mathsf{code}(\mathsf{succ}(m),\mathsf{succ}(n)) \equiv \mathsf{code}(m,n) \xrightarrow{\mathsf{decode}(m,n)} (m = n) \xrightarrow{\mathsf{ap}_{\mathsf{succ}}} (\mathsf{succ}(m) = \mathsf{succ}(n)).$$

Next we show that $\mathsf{encode}(m,n)$ and $\mathsf{decode}(m,n)$ are quasi-inverses for all m,n.

On one hand, if we start with $p : m = n$, then by induction on p it suffices to show

$$\mathsf{decode}(n, n, \mathsf{encode}(n, n, \mathsf{refl}_n)) = \mathsf{refl}_n.$$

But $\mathsf{encode}(n, n, \mathsf{refl}_n) \equiv r(n)$, so it suffices to show that $\mathsf{decode}(n, n, r(n)) = \mathsf{refl}_n$. We can prove this by induction on n. If $n \equiv 0$, then $\mathsf{decode}(0, 0, r(0)) = \mathsf{refl}_0$ by definition of decode. And in the case of a successor, by the inductive hypothesis we have $\mathsf{decode}(n, n, r(n)) = \mathsf{refl}_n$, so it suffices to observe that $\mathsf{ap}_{\mathsf{succ}}(\mathsf{refl}_n) \equiv \mathsf{refl}_{\mathsf{succ}(n)}$.

On the other hand, if we start with $c : \mathsf{code}(m, n)$, then we proceed by double induction on m and n. If both are 0, then $\mathsf{decode}(0, 0, c) \equiv \mathsf{refl}_0$, while $\mathsf{encode}(0, 0, \mathsf{refl}_0) \equiv r(0) \equiv \star$. Thus, it suffices to recall from `http://planetmath.org/28theunittype`§2.8 that every inhabitant of $\mathbf{1}$ is equal to $\star$. If m is 0 but n is a successor, or vice versa, then $c : \mathbf{0}$, so we are done. And in the case of two successors, we have

$$\begin{aligned}
&\mathsf{encode}(\mathsf{succ}(m), \mathsf{succ}(n), \mathsf{decode}(\mathsf{succ}(m), \mathsf{succ}(n), c)) \\
&\qquad = \mathsf{encode}(\mathsf{succ}(m), \mathsf{succ}(n), \mathsf{ap}_{\mathsf{succ}}(\mathsf{decode}(m, n, c))) \\
&\qquad = \mathsf{transport}^{\mathsf{code}(\mathsf{succ}(m), -)}(\mathsf{ap}_{\mathsf{succ}}(\mathsf{decode}(m, n, c)), r(\mathsf{succ}(m))) \\
&\qquad = \mathsf{transport}^{\mathsf{code}(\mathsf{succ}(m), \mathsf{succ}(-))}(\mathsf{decode}(m, n, c), r(\mathsf{succ}(m))) \\
&\qquad = \mathsf{transport}^{\mathsf{code}(m, -)}(\mathsf{decode}(m, n, c), r(m)) \\
&\qquad = \mathsf{encode}(m, n, \mathsf{decode}(m, n, c)) \\
&\qquad = c
\end{aligned}$$

using the inductive hypothesis. $\square$

In particular, we have

$$\mathsf{encode}(\mathsf{succ}(m), 0) : (\mathsf{succ}(m) = 0) \to \mathbf{0} \tag{2.13.2}$$

which shows that "0 is not the successor of any natural number". We also have the composite

$$(\mathsf{succ}(m) = \mathsf{succ}(n)) \xrightarrow{\mathsf{encode}} \mathsf{code}(\mathsf{succ}(m), \mathsf{succ}(n)) \equiv \mathsf{code}(m, n) \xrightarrow{\mathsf{decode}} (m = n) \tag{2.13.3}$$

which shows that the function succ is injective.

We will study more general positive types in `http://planetmath.org/node/87578`Chapter 5,`http://planetmath.org/node/87579`Chapter 6. In `http://planetmath.org/node/87582`Chap

8, we will see that the same technique used here to characterize the identity types of coproducts and $\mathbb{N}$ can also be used to calculate homotopy groups of spheres.