Math 310 Class Notes 5: The Recursion Theorem for $\mathbb{N}$

In this set of notes we will tighten a loose end that has been left dangling. Namely, in Class Notes 3 we used the word "assign" when we defined the notion of + for $\mathbb{N}$ (see Definition 2 of the notes). The word "assign" actually means we have a *function* that does the assignment. To be precise, we have the following theorem.

Theorem 1. (The recursion theorem) *Let c be a fixed natural number and let $f : \mathbb{N} \to \mathbb{N}$ be a function. Then there is a unique function $g : \mathbb{N} \to \mathbb{N}$ such that $g(1) = c$ and $g(x') = f(g(x))$ for all $x \in \mathbb{N}$.*

Before proving this theorem, let us see a few applications.

Application 1. Consider the function $f : \mathbb{N} \to \mathbb{N}$ given by

$$f : x \mapsto x'.$$

Fix a number $m \in \mathbb{N}$. Then by the recursion theorem there is a function g such that $g(1) = m'$ and $g(x') = f(g(x))$ for all $x \in \mathbb{N}$. Let us now define

$$m + n := g(n)$$

for all $n \in \mathbb{N}$.

Theorem 2. *Fix $m \in \mathbb{N}$. We have $m + n' = (m + n)'$ for all $n \in \mathbb{N}$.*

Proof. $m + n' = g(n') = f(g(n)) = f(m + n) = (m + n)'$. □

Slightly harder to verify is the following.

Theorem 3. *Fix $m \in \mathbb{N}$. We have $m' + n = (m + n)'$ for all $n \in \mathbb{N}$.*

Proof. $m + n = g(n)$ for all $n \in \mathbb{N}$, where $g(1) = m'$ and $g(n') = f(g(n))$. Likewise, $m' + n = h(n)$ for all $n \in \mathbb{N}$, where $h(1) = (m')'$ and $h(n') = f(h(n))$.

Let S be the set of all $n \in \mathbb{N}$ such that $m' + n = (m + n)'$.

We first show $1 \in S$. Now $m' + 1 = h(1) = (m')'$ while $m + 1 = g(1) = m'$, so that $m' + 1 = (m')' = (m + 1)'$. Thus $1 \in S$.

Next suppose $n \in S$. We establish that $n' \in S$. That $n \in S$ means

$$m' + n = (m + n)',$$

which is the induction hypothesis. Therefore, by the preceding theorem and the induction hypothesis we have

$$m' + n' = (m' + n)' = ((m + n)')' = (m + n')'.$$

Therefore, $n' \in \mathbb{N}$ and so $S = \mathbb{N}$. That is $m' + n = (m + n)'$ for all $n \in \mathbb{N}$. □

This theorem is what we have seen in class. The advantage of this approach via the recursion formula is that we can take care of $m + n$ for all m and n at one stroke.

Application 2. Fix $m \in \mathbb{N}$. Consider the function $f : \mathbb{N} \to \mathbb{N}$ given by

$$f : x \mapsto x + m.$$

Then by the recursion theorem there is a function $g : \mathbb{N} \to \mathbb{N}$ such that $g(1) = m$ and $g(x') = f(g(x))$. We define

$$m \cdot n := g(n)$$

for all $n \in \mathbb{N}$.

Exercise. Prove that $m \cdot n' = m \cdot n + m$ and $m' \cdot n = m \cdot n + n$ for all $n \in \mathbb{N}$.

Application 3. Fix $a \in \mathbb{N}$. Consider the function $f : \mathbb{N} \to \mathbb{N}$ given by

$$f : x \mapsto ax.$$

Then by the recursion theorem there is a function $g : \mathbb{N} \to \mathbb{N}$ such that $g(1) = a$ and $g(x') = f(g(x))$. We define

$$a^n := g(n).$$

Exerxise. By the mathematical induction, prove that $a^{m+n} = a^m \cdot a^n$ and $(a^m)^n = a^{mn}$.

Now let us look at the proof of the recursion theorem.

Proof. **Existence of** g.

By definition, a function $g : \mathbb{N} \to \mathbb{N}$ is a special sort of subset of $\mathbb{N} \times \mathbb{N}$. Recall that $g(1) = c$ means $(1, c) \in g$ and $g(x') = f(g(x))$ means that if we let $y = g(x)$, i.e., let $(x, y) \in g$, then $(x', f(y)) \in g$ as this just says

$$g(x') = f(g(x)) = f(y).$$

Motivated by this, let us begin to construct the function g by considering the set S, where

$$\mathcal{S} := \{A \subset \mathbb{N} \times \mathbb{N} : (1, c) \in A \text{ and } (x, y) \in A \text{ implies } (x', f(y)) \in A\}.$$

S is not empty since $\mathbb{N} \times \mathbb{N} \in S$. Consider the set

$$g := \cap_{A \in \mathcal{S}} A,$$

which consists of elements common to all $A \in \mathcal{S}$.

Now $(1, c) \in g$ since it is in all $A \in \mathcal{S}$. Moreover, if $(x, y) \in g$ then $(x, y) \in A$ for all $A \in \mathcal{S}$. But then $(x', f(y)) \in A$ for all $A \in \mathcal{S}$ so that

$(x', f(y)) \in g$. We conclude therefore that g is in fact an element of $\mathcal{S}$; it is the smallest element of $\mathcal{S}$.

We now prove that g is a function from $\mathbb{N}$ to $\mathbb{N}$.

First we show that the domain of g is $\mathbb{N}$. Let T be the subset of $n \in \mathbb{N}$ such that there is a $z \in \mathbb{N}$ for which $(n, z) \in g$. Now $1 \in T$ since $(1, c) \in g$. Suppose $n \in T$. Then $(n, z) \in g$ for some $z \in \mathbb{N}$. This gives $(n', f(z)) \in g$. Hence $n' \in T$. It follows by mathematical induction that $T = \mathbb{N}$. That is, the domain of g is $\mathbb{N}$.

Secondly, we show that each domain element of g is mapped to a unique target element. To this end, consider the set

$$U := \{x \in \mathbb{N} : (x, y), (x, z) \in g \text{ imply } y = z\}.$$

We show $1 \in U$. Suppose this is not the case. That is, suppose we have $(1, z)$, in addition $(1, c) \in g$, where $z \neq c$. Then the set $g \setminus \{(1, z)\}$ would be a member of $\mathcal{S}$ (WHY?). But this contradicts the fact that g is already the smallest element of $\mathcal{S}$. Thus, $1 \in U$.

We show that if $x \in U$ then $x' \in U$. Suppose this is not the case. Then there is an $m \in U$ so that $m' \notin U$. Since $m \in U$, there is a unique $n \in \mathbb{N}$ with $(m, n) \in g$. As a consequence $(m', f(n)) \in g$. Since $m' \notin U$, there is an $(m', z) \in g$, in addition to $(m', f(n)) \in g$, where $z \neq f(n)$. But then $g \setminus \{(m', z)\}$ is an element of $\mathcal{S}$ that is even smaller than g (WHY?), which is absurd.

The mathematical induction then says that $U = \mathbb{N}$. In conclusion, g is a function.

Uniqueness of g.

Suppose we have two functions g_1 and g_2 satisfying $g_1(1) = c = g_2(1)$ and $g_1(x') = f(g_1(x))$ and $g_2(x') = f(g_2(x))$ for all $x \in \mathbb{N}$. Let us consider the set

$$V := \{n \in \mathbb{N} : g_1(n) = g_2(n)\}.$$

$1 \in V$ because $g_1(1) = g_2(1) = c$. If $n \in V$, then $g_1(n) = g_2(n)$, so that

$$g_1(n') = f(g_1(n)) = f(g_2(n)) = g_2(n'),$$

which implies $n' \in V$. Hence $V = \mathbb{N}$ by the mathematical induction. That is, $g_1 = g_2$. $\square$