CONSTRUCTION OF NUMBER SYSTEMS

N. MOHAN KUMAR

1. Peano's Axioms and Natural Numbers

We start with the axioms of Peano.

Peano's Axioms. *$\mathbb{N}$ is a set with the following properties.*

1. *$\mathbb{N}$ has a distinguished element which we call '1'.*
2. *There exists a distinguished set map $\sigma : \mathbb{N} \to \mathbb{N}$.*
3. *σ is one-to-one (injective).*
4. *There does not exist an element $n \in \mathbb{N}$ such that $\sigma(n) = 1$. (So, in particular σ is not surjective).*
5. *(Principle of Induction) Let $S \subset \mathbb{N}$ such that a) $1 \in S$ and b) if $n \in S$, then $\sigma(n) \in S$. Then $S = \mathbb{N}$.*

We call such a set $\mathbb{N}$ to be the set of natural numbers and elements of this set to be natural numbers.

Lemma 1.1. *If $n \in \mathbb{N}$ and $n \neq 1$, then there exists a unique $m \in \mathbb{N}$ such that $\sigma(m) = n$.*

Proof. Consider the subset S of $\mathbb{N}$ defined as,

$$S = \{n \in \mathbb{N} \mid n = 1 \,\text{or}\, n = \sigma(m), \text{ for some}\, m \in \mathbb{N}\}.$$

By definition, $1 \in S$. If $n \in S$, clearly $\sigma(n) \in S$, again by definition of S. Thus by the Principle of Induction, we see that $S = \mathbb{N}$. Further injectivity of σ implies uniqueness as claimed in the lemma. This proves the lemma. □

We define the operation of addition (denoted by $+$) by the following two recursive rules.

1. For all $n \in \mathbb{N}$, $n + 1 = \sigma(n)$.
2. For any $n, m \in \mathbb{N}$, $n + \sigma(m) = \sigma(n + m)$.

Notice that by lemma 1.1, any natural number is either 1 or of the form $\sigma(m)$ for some unique $m \in \mathbb{N}$ and thus the defintion of addition above does define it for any two natural numbers n, m.

Similarly we define multiplication on $\mathbb{N}$ (denoted by $\cdot$, or sometimes by just writing letters adjacent to each other, as usual) by the following two recursive rules.

(1) For all $n \in \mathbb{N}$, $n \cdot 1 = n$.
(2) For any $n, m \in \mathbb{N}$, $n \cdot \sigma(m) = n \cdot m + n$.

Agian, lemma 1.1 assures that this defines multiplication of any two natural numbers. This procedure seems a bit informal and logically suspect. You are of course right. To be completely precise, we have to prove the Universal Property of Natural Numbers, first. This may look very abstract and so, if you wish, you may just trust the above formulas. But, we prove it for those more skeptical and those who are not afraid of abstractions.

1.1. **Universal Property of Natural Numbers.**

Theorem 1.1 (Universal Property of Natural Numbers)**.** *Let S be any set, $f : S \to S$ be any function and let $s \in S$ be a fixed element. Then there exists a unique function $\phi : \mathbb{N} \to S$ such that $\phi(1) = s$ and $\phi \circ \sigma = f \circ \phi$.*

Proof. The follwing proof is rather long, so we will discuss at least some part of thinking, which is not part of the proof itself. So, this will be in blue, while the proof itself will be in black.

The theorem asserts the existence and uniqueness of a function ϕ with some properties. We will not worry about the uniqueness, which is easy and concentrate on the existence. Since, at present, we just have some knowledge of set theory and we have assumed Peano's axioms, but little else and none of these tell us how to construct a function. By the first property we know that $\phi(1) = s$. If we call $\sigma(1) = 2, \sigma(2) = 3$ etc., which are just names we have given, the second property says $\phi(2) = \phi(\sigma(2)) = f(\phi(1)) = f(s)$, $\phi(3) = f(f(s))$ etc. But, we have no logical way of interpreting 'etc.'. So, we seem to be at an impasse. Thus, we are forced to rethink our path. Since we know a bit about sets and how to define them, can we interpret ϕ in terms of a set? We have seen that a function gives the graph, which is a set and we can retrieve the function from the graph. So, let me recall this.

Lemma 1.2. *Let A, B be sets. Then a subset $\Gamma \subset A \times B$ is the graph of a function from A to B if and only if $p : \Gamma \to A$, the first projection, is a bijection.*

Proof. If Γ is the graph of a function $\phi : A \to B$, then $\Gamma = \{(a, \phi(a)) | a \in A\}$. Then for any $a \in A$, $p^{-1}(a) = \{(a, \phi(a))\}$ and thus p is injective and surjective. So, p is a bijection.

Now, assume that $p : \Gamma \to A$ is a bijection. Then we can define ϕ as $\phi(a) = q(p^{-1}(a))$, where $q : \Gamma \to B$ is the second projection and $p^{-1} : A \to \Gamma$ is the inverse of p, which makes sense since p is a bijection. I will leave you to check that then Γ is the graph of this function ϕ. □

So, in our situation, we need to find a subset $\Gamma \subset \mathbb{N} \times S$ such that $p : \Gamma \to \mathbb{N}$ is a bijection. What other properties should it have, if this is going to be the graph of ϕ asserted in the theorem? Since $\phi(1) = s$, we must have $(1, s) \in \Gamma$. Next let us interpret the second condition. Since Γ is expected to be the graph of the yet unconstructed function ϕ, for any $n \in \mathbb{N}$, we must have elements of the form $(n, \phi(n)) \in \Gamma$. So, if $(n, t) \in \Gamma$, then t is expected to be $\phi(n)$. Then, the second condition says the $\phi(\sigma(n)) = f(\phi(n))$ and hence $(\sigma(n), f(t)) \in \Gamma$. This says, if we define $\theta : \mathbb{N} \times S \to \mathbb{N} \times S$ as $\theta((n, t)) = (\sigma(n), f(t))$, then $\theta(\Gamma) \subset \Gamma$. So, these three conditions will ensure what we need. So, we start the proof.

First, we prove the existence of ϕ, uniqueness will be easy. We will construct the graph of ϕ, which in turn will define ϕ. So, we plan to construct a suitable subset Γ of $\mathbb{N} \times S$. First, we have a function $\theta : \mathbb{N} \times S \to \mathbb{N} \times S$, given by $\theta((n, t)) = (\sigma(n), f(t))$ for $n \in \mathbb{N}, t \in S$. We will have the required function if we can construct such a subset Γ satisfying the following three properties.

(1) $p : \Gamma \to \mathbb{N}$, the first projection, is a bijection.
(2) $(1, s) \in \Gamma$.
(3) $\theta(\Gamma) \subset \Gamma$.

If we look for such a subset, clearly nothing immediately strikes one as a possible candidate. So, we are still stuck. Since Γ has to satisfy the three conditions above, may be we can find some set satisfying some of the conditions easily? Here we strike gold, since the set $\mathbb{N} \times S$ itself satisfy the second and third conditions. So, may be we should study all sets satisfying the last two conditions and then look for Γ among them? At least our search has narrowed down.

Let $\mathcal{C}$ be the set of all subsets of $\mathbb{N} \times S$ satisfying the last two conditions above. Then $\mathbb{N} \times S \in \mathcal{C}$ and hence this collection is non-empty.

How do we distinguish our Γ from these sets? If $X \in \mathcal{C}$, then we have $(1, s) \in X$ and $\theta(X) \subset X$. Since $\theta((1, s)) = (2, f(s))$, $\theta(2, f(s)) = (3, f(f(s)))$ etc. and these are precisely the elements expected to be in Γ, it seems that $\Gamma \subset X$. So, the Γ we are looking for seems to be the 'smallest' element in $\mathcal{C}$. So, it makes sense to look at the set Γ which is the intersection of all the sets in $\mathcal{C}$.

Let Γ be the intersection of all elelements in $\mathcal{C}$, which makes sense since this collection is non-empty. First let us check that $\Gamma \in \mathcal{C}$. This is easy, since $(1, s) \in X$ for all $X \in \mathcal{C}$ and Γ beng the intersection of such sets, $(1, s) \in \Gamma$. Similarly, for any $X \in \mathcal{C}$, $\theta(\Gamma) \subset \theta(X) \subset X$ and thus $\theta(\Gamma) \subset X$ for all $X \in \mathcal{C}$. So, by definition of Γ, $\theta(\Gamma) \subset \Gamma$. So, Γ satisfies the last two conditions and hence $\Gamma \in \mathcal{C}$.

Now, we tackle the first condition for this Γ. First, let us look at the set $G = \theta(\Gamma) \cup \{(1, s)\}$. Why should we look at G? I find it a bit difficult to explain this, but it is similar to the property of $\mathbb{N}$ that we studied, $\mathbb{N} = \sigma(\mathbb{N}) \cup \{1\}$. Then clearly $G \subset \Gamma$, since both $\theta(\Gamma)$ and $\{(1, s)\}$ are contained in Γ. On the other hand, $(1, s) \in G$ and $\theta(G) \subset \theta(\theta(\Gamma)) \cup \theta(\{(1, s)\} \subset \theta(\Gamma) \subset G$. So, $G \in \mathcal{C}$ and thus by definition of Γ, we get $\Gamma \subset G$. This shows that

$$\theta(\Gamma) \cup \{(1, s)\} = G = \Gamma. \tag{1}$$

Now, we check that the first projection $p : \Gamma \to \mathbb{N}$ is a bijection. We use induction for this and so define a set,

$$T = \{n \in \mathbb{N} | p^{-1}(n) \subset \Gamma \text{ has exactly one element}\}.$$

Notice that as usual, we have defined this set so that if we can show $T = \mathbb{N}$, then p would be a bijection.

We have $p((1, s)) = 1$ and we wish to show that $p^{-1}(1) = \{(1, s)\}$. If not, say $(1, t) \in p^{-1}(1)$ with $t \neq s$. By equation 1, we see that $(1, t) \in \theta(\Gamma)$. So, there exists an element $(n, u) \in \Gamma$ such that $(1, t) = \theta((n, u)) = (\sigma(n), f(u))$. This says in particular, $1 = \sigma(n)$ contradicting Peano's axiom. This proves that $p^{-1}(1) = \{(1, s)\}$ and hence $1 \in T$.

Next, assume that $n \in T$. Then by definition, we have $p^{-1}(n) = \{(n, w)\}$. Since $(n, w) \in \Gamma$, we know that $\theta((n, w)) = (\sigma(n), f(w)) \in \Gamma$, since $\theta(\Gamma) \subset \Gamma$. Thus $p^{-1}(\sigma(n))$ contains $(\sigma(n), f(w))$. If we can show this is the only element in this set, we would have shown $\sigma(n) \in T$ and then by induction, we would be done. So, assume that $(\sigma(n), x) \in \Gamma$ and we want to show that $x = f(w)$. By Peano's axiom, $(\sigma(n), x) \neq (1, s)$ and hence, from equation 1, we see that $(\sigma(n), x) \in \theta(\Gamma)$ and thus there is an element $(m, y) \in \Gamma$ with $\theta((m, y)) = (\sigma(n), x)$. Then $\sigma(m) = \sigma(n)$ and $f(y) = x$. By injectivity of σ, we get $m = n$. Since $(m, y) = (n, y) \in \Gamma$ and $n \in T$ implies $y = w$. Then $x = f(w)$ and thus $(\sigma(n), x) = (\sigma(n), f(w))$ proving what we set out to prove. Thus $T = \mathbb{N}$ and hence p is a bijection.

Thus we have created a function $\phi : \mathbb{N} \to S$ satisfying the two required conditions.

The above argument shows uniqueness too, since Γ determines ϕ and Γ was forced to be the intersection of all elements in $\mathcal{C}$, so it had no choice. But, no harm in reproving it.

To show uniqueness, let $\phi' : \mathbb{N} \to S$ be another function satisfying the two conditions of the theorem. We wish to show $\phi(n) = \phi'(n)$ for all $n \in \mathbb{N}$ and so it makes sense to define the set $U = \{n \in \mathbb{N} | \phi(n) = \phi'(n)\}$. Then since $\phi(1) = (1, s) = \phi'(1)$ by the first condition, we see that $1 \in U$. If $n \in U$, then we have $\phi(n) = \phi'(n)$ and thus $\phi(\sigma(n)) = f(\phi(n))$ by second condition and hence, $f(\phi(n)) = f(\phi'(n)) = \phi'(\sigma(n))$ again by the second condition for ϕ'. So, $\phi(\sigma(n)) = \phi'(\sigma(n))$, proving $\sigma(n) \in U$. By induction, $U = \mathbb{N}$ and the theorem is proved. □

1.2. **Definition of addition and multiplication.** Now we are ready to rigorously define addition and multiplication of natural numbers. Fix any $m \in \mathbb{N}$. We will define an operation for any $n \in \mathbb{N}$, $m + n \in \mathbb{N}$ such that $m + 1 = \sigma(m)$ and $m + \sigma(n) = \sigma(m + n)$. For this, consider $S = \mathbb{N}$, $f = \sigma$ and $s = \sigma(m)$ in the above theorem 1.1. Then we have a function $\phi : \mathbb{N} \to \mathbb{N}$ such that $\phi(1) = \sigma(m)$ and $\phi \circ \sigma = \sigma \circ \phi$. So, if we call $\phi(n) = m + n$ (the addition symbol just represents this function), then it is trivial to check both the above properties.

To define multiplication, again we take, fixing an $m \in \mathbb{N}$, $S = \mathbb{N}$, $f : \mathbb{N} \to \mathbb{N}$ be, $f(n) = n + m$ (which is laready defined) and $s = m$. Then we get a function $\phi : \mathbb{N} \to \mathbb{N}$ by the Universal property, so that $\phi(1) = m$ and $\phi(\sigma(n)) = \phi(n) + m$. So, if we define $m \cdot n = \phi(n)$, then it staisfies both the properties of multiplication stated earlier and since m was any element of $\mathbb{N}$, we have defined multiplication for any two natural numbers.