Math 582
Introduction to Set Theory

Kenneth Harris
kaharri@umich.edu

Department of Mathematics
University of Michigan

February 16, 2009

Introduction

We will be working with systems of natural numbers $(\mathbb{N}, 0, S)$ in this lecture. Our aim is to show how more structure can be introduced into these systems through definitions in a *natural way*. There are two objectives in this lecture

1. Define addition and derive the key properties of addition on natural numbers: associativity, commutativity, and the cancellation laws.
2. Define an ordering $\leq$ on natural numbers (using addition) and show that the ordered set $(\mathbb{N}, \leq)$ is a well-ordering.

Recursion Theorem with Parameters

We need a more general form of the Recursion Theorem in order to define two-place functions, like addition. The following is

Corollary (Recursion Theorem with Parameters)

Let $(\mathbb{N}, 0, S)$ be any system of natural numbers. For any sets Y, E and functions

$$g : Y \to E \qquad h : Y \times E \to E$$

there is a unique function $f : Y \times \mathbb{N} \to E$ satisfying

$$\begin{aligned} f(y, 0) &= g(y) && y \in Y \\ f(y, S(n)) &= h(y, f(y, n)) && y \in Y, n \in \mathbb{N} \end{aligned}$$

Note. The parameter y in the function f given by the theorem is simply passed as an argument.

Proof of theorem

Proof. Fix $y \in Y$, and define $h_y : E \to E$ by

$$h_y(e) = h(y, e) \qquad e \in E.$$

By the Recursion Theorem we know that for each $y \in Y$, there is a unique $f_y : \mathbb{N} \to E$ satisfying

$$\begin{aligned} f_y(0) &= g(y) \\ f_y(S(n)) &= h_y(f_y(n)) = h(y, f_y(n)) && n \in \mathbb{N} \end{aligned}$$

By Replacement (and Comprehension) we get the family of functions $\{f_y \,|\, y \in Y\}$. Now, let

$$f = \{(y, n, e) \in Y \times \mathbb{N} \times E \,|\, (n, e) \in f_y\}.$$

Defining addition

Definition

The addition function, $+$, is defined on $n, m \in \mathbb{N}$ by the recurrence equation:

$$\begin{aligned} n + 0 &= n \\ n + S(m) &= S(n + m). \end{aligned}$$

n is the parameter in the equations, m is the recurrence variable.

Justification. Use the Primitive Recursion Theorem with parameters, where

$$\begin{aligned} g &= \{(n, n) \mid n \in \mathbb{N}\} \\ h &= \{(z, n, w) \mid z, n \in \mathbb{N}, w = S(z)\} \end{aligned}$$

So, $+$ is the unique function satisfying:

$$\begin{aligned} +(n, 0) &= g(n) = n & n \in \mathbb{N} \\ +(n, S(m)) &= h(+(n, m), n) = S(+(n, m)) & n, m \in \mathbb{N} \end{aligned}$$

We write $n + m$ for $+(n, m)$.

Associativity of addition

Theorem

Addition is associative: the following equation is valid for all $n, m, k \in \mathbb{N}$

$$(n + m) + k = n + (m + k)$$

Proof of associativity

Proof.

By induction on k.

☞ basis. $k = 0$: for any n, m,

$$(n + m) + 0 = n + m = n + (m + 0)$$

☞ inductive. Suppose associativity holds for k (i.h.) Fix $n, m \in \mathbb{N}$:

$$\begin{aligned} (n+m) + Sk &= S((n+m)+k) \\ &= S(n+(m+k)) && \text{(i.h.)} \\ &= n + S(m+k) \\ &= n + (m + S(k)) \end{aligned}$$

So, associativity holds for $S(m)$.

✓ Thus, associativity holds for all $k \in \mathbb{N}$. □

Commutativity

Theorem

Addition is commutative: the following equation is valid for all $n, m, k \in \mathbb{N}$

$$n + m = m + n$$

Proof of commutativity–basis case

Proof. Proof is by induction on m.

☞ basis. $m = 0$

$$\begin{aligned} n + 0 &= n \\ &= 0 + n \qquad ❀ \end{aligned}$$

✉ We need to justify ❀.

Lemma ❀

Lemma (❀)

$0 + n = n$ for every $n \in \mathbb{N}$.

Proof.

By induction on n.

☞ basis. $0 + 0 = 0$.

☞ inductive. Suppose $0 + n = n$ (i.h.). Compute

$$0 + S(n) = S(0 + n) = S(n).$$

✓ Therefore, $0 + n = n$ for every $n \in \mathbb{N}$.

□

Proof of commutativity–inductive case

☞ inductive. Assume $n + m = m + n$ for every $n \in \mathbb{N}$ (i.h.) Compute:

$$
\begin{aligned}
n + S(m) &= S(n+m) && \\
&= S(m+n) && (i.h.) \\
&= m + S(n) && \\
&= S(m) + n && ☎
\end{aligned}
$$

✉ We need to justify ☎.

Lemma ☎

Lemma (☎)

$m + S(n) = S(m) + n$ for every $m, n \in \mathbb{N}$.

Proof.

By induction on n.

☞ basis. $n = 0$. Let $m \in \mathbb{N}$ be arbitrary,

$$m + S(0) = S(m+0) = S(m) = S(m) + 0$$

☞ inductive. Suppose $m + S(n) = S(m) + n$ for every m (i.h.). Compute

$$
\begin{aligned}
m + S(S(n)) &= S(m + S(n)) && \\
&= S(S(m) + n) && \text{(i.h.)} \\
&= S(m) + S(n) &&
\end{aligned}
$$

✓ Therefore, $m + S(n) = S(m) + n$ for every $m, n \in \mathbb{N}$. □

Left Cancellation for addition

Theorem

The left cancellation law holds for addition: For all $n, s, t \in \mathbb{N}$,

$$n + s = n + t \quad \to \quad s = t.$$

Proof. By induction on n.

☞ basis. $n = 0$. Let $s, t \in \mathbb{N}$ be arbitrary.
Suppose $0 + s = 0 + t$. Then

$$s = 0 + s = 0 + t = t.$$

The first and third identities follow from commutativity and the definition of addition.

Inductive step of right cancellation

☞ inductive. Suppose that for any $s, t \in \mathbb{N}$

$$n + s = n + t \to s = t \qquad \text{(i.h.)}$$

Fix arbitrary $s, t \in \mathbb{N}$ and suppose $S(n) + s = S(n) + t$. Then

$$S(n) + s = S(n + s) \qquad S(n) + t = S(n + t)$$

(by Commutativity and definition of addition.)

$$\begin{aligned} S(n+s) &= S(n+t) && \text{previous} \\ n+s &= n+t && (\mathbf{N3}) \\ s &= t && \text{(i.h.)} \end{aligned}$$

Thus,

$$S(n) + s = S(n) + t \to s = t \qquad \text{for any } s, t \in \mathbb{N}$$

✓ Therefore, the right cancellation holds for addition in $\mathbb{N}$.

Order

Informally, $n \leq m$ if we can reach m by applying successor a finite number of times starting at N:

$$n \leq m \quad \leftrightarrow m = S^{(k)}(n) \qquad \text{for some } k \in \mathbb{N}$$

Formally,

Definition

The order relation $\leq$ on $\mathbb{N}$ is defined by

$$n \leq m \quad := \quad \exists k \in \mathbb{N}\,(n + k = m).$$

The strict order $<$ is defined by

$$n < m \quad := \quad n \leq m \wedge n \neq m.$$

Lemma on order

Lemma

$$\forall n, m \in \mathbb{N}\,\big(n \leq S(m) \quad \leftrightarrow \quad n \leq m \vee n = S(m)\big)$$

Proof.

$(\leftarrow)$. If $n \leq m$, then $\exists k\,\big(n + k = m\big)$; so, $S(n + k) = n + S(k) = S(m)$.

$(\rightarrow)$. Suppose $n \leq S(m)$. So, $S(m) = n + k$ for some k. Two cases

(a) $k = 0$. Then $S(m) = n + 0 = n$.

(b) $k \neq 0$. Then $k = S(\ell)$ for some $\ell \in \mathbb{N}$. So,

$$S(m) = n + k = n + S(\ell) = S(n + \ell)$$

so, $m = n + \ell$ by (**N3**), i.e. $n \leq m$.

$\square$

$\leq$ a total order

Theorem

$(\mathbb{N}, \leq)$ *is a totally ordered set. (Alternative terminology, a linear order.)*

Proof. The proof will establish four properties: reflexivity, transitivity, antisymmetry, trichotomy.

Reflexivity and Transitivity

- Reflexivity

$n + 0 = n$, so $n \leq n$.

- Transitivity

Suppose $n \leq m$ and $m \leq p$. Then for some $k, \ell \in \mathbb{N}$

$$m = n + k \qquad p = m + \ell$$

so,

$$p = (n + k) + \ell = n + (k + \ell)$$

Thus, $n \leq p$.

Antisymmetry

➤ Antisymmetry

Suppose $n \leq m$ and $m \leq n$. We must show $n = m$. By hypothesis, there are $k, \ell \in \mathbb{N}$

$$m = n + k \qquad n = m + \ell$$

so that $m = (m + \ell) + k = m + (\ell + k)$.

Since $m + 0 = m = m + (\ell + k)$ we have $0 = \ell + k$. We show $k = 0$:

Suppose $k \neq 0$. Then $k = S(j)$ for some $j \in \mathbb{N}$, so

$$0 = \ell + k = \ell + S(j) = S(\ell + j)$$

which is impossible by (**N4**). $\lightning$ So, $k = 0$.

✓ Therefore, $m = n + 0 = n$

Trichotomy

➤ Trichotomy

We will show by induction on m that $\forall n \in \mathbb{N}\,(m \leq n \ \vee \ n \leq m)$.

☞ basis. $0 \leq n$ for every $n \in \mathbb{N}$.

☞ inductive. Suppose $\forall n \in \mathbb{N}\,(m \leq n \ \vee \ n \leq m)$ (i.h.)

Fix $n \in \mathbb{N}$. We must show: $n \leq S(m) \vee S(m) \leq n$. Two cases.

(a) $n \leq m$. Since $m \leq S(m)$ (by Lemma), we have $n \leq S(m)$.

(b) $m \leq n$. So, $n = m + k$ for some $k \in \mathbb{N}$. Two cases.

(i) $k = 0$. Then $n = m + 0 = m$, so $n = m \leq S(m)$.

(ii) $k \neq 0$. Then $k = S(\ell)$ for some $\ell \in \mathbb{N}$. So,

$$\begin{aligned} n &= m + S(\ell) \\ &= S(m + \ell) \\ &= S(m) + \ell && \text{Commutativity and definition of } + \end{aligned}$$

So, $S(m) \leq n$.

Thus, $n \leq S(m) \ \vee \ S(m) \leq n$, which completes the inductive step.

✓ Therefore, trichotomy holds.

Strong Induction Scheme

We now turn to show that $(\mathbb{N}, \leq)$ is well-founded. It is convenient to prove a useful form of the Induction Scheme:

Theorem (Strong Induction Scheme)

Let $\varphi(x)$ be any formula, and assume the following holds

$$\forall n \in \mathbb{N} \left(\forall k < n \, \varphi(k) \quad \to \quad \varphi(n)\right) \quad \ast$$

Then $\forall n \in \mathbb{N} \, \varphi(n)$.

Proof of Strong Induction Scheme

Proof.

Assume

$$\forall n \in \mathbb{N} \left(\forall k < n \, \varphi(k) \quad \to \quad \varphi(n)\right) \quad \ast$$

Define $\psi(n) \ := \ \forall k < n \, \varphi(k)$. We will show $\forall n \, \psi(n)$ by Induction. It will follow that $\forall n \, \varphi(n)$, since $\psi(S(n)) \to \varphi(n)$.

- basis. $\psi(0)$ is trivially true.
- inductive. Suppose $\psi(n)$ holds (i.h.). It follows from this and $\ast$ that

$$\forall k < n \, \varphi(k) \ \wedge \ \varphi(n).$$

Since $k < S(n)$ iff $k \leq n$ (by Lemma), we have show $\forall k < S(n) \, \varphi(k)$, that is $\psi(S(n))$.

✓ Therefore, $\forall n \, \psi(n)$ holds, so that $\forall n \, \varphi(n)$ as well. □

$\leq$ is well-founded

Theorem

$(\mathbb{N}, \leq)$ *is a well-ordered set.*

Proof.

We have only to prove $\leq$ is well-founded on $\mathbb{N}$. Let $X \subseteq \mathbb{N}$ is nonempty; suppose X has no least element. Set $Y = \mathbb{N} - X$.

We will prove $Y = \mathbb{N}$ by Strong Induction, by showing

$$\forall k < n\, k \in Y \quad \to \quad n \in Y \quad \ast .$$

Suppose that for all $k < n$, $k \in Y$. If $n \notin Y$ then $n \in X$, and is the least in X!! Since X has no least element, $n \in Y$. So $\ast$.

Thus, $Y = \mathbb{N}$ $\lightning$ (since $X \neq \emptyset$.) Thus, X has a least element.

$\square$

Canonical operations on systems of natural numbers

The canonical operations of $+$ (addition) is natural on any natural number system $(\mathbb{N}, 0, S)$ in the sense that:

Theorem

Suppose $(\mathbb{N}_1, 0_1, S_1)$ *and* $(\mathbb{N}_2, 0_2, S_2)$ *are two systems of natural numbers, where* $+_1, +_2$ *are their respective canonical operations of addition. Then the canonical isomorphism* $\pi : \mathbb{N}_1 \rightleftarrows \mathbb{N}_2$ *respects this operation: for all* $n, m \in \mathbb{N}_1$*,*

$$\pi(n +_1 m) \quad = \quad \pi(n) +_2 \pi(m)$$

Proof. Homework 3.

Well-ordering on systems of natural numbers

The canonical relation of $\leq$ (addition) is natural on any natural number system $(\mathbb{N}, 0, S)$ in the sense that:

Theorem

Suppose $(\mathbb{N}_1, 0_1, S_1)$ and $(\mathbb{N}_2, 0_2, S_2)$ are two systems of natural numbers, where $<_1, <_2$ are their respective canonical well-orders. Then the canonical isomorphism $\pi : \mathbb{N}_1 \rightleftarrows \mathbb{N}_2$ is order preserving: for all $n, m \in \mathbb{N}_1$:

$$n <_1 m \;\leftrightarrow\; \pi(n) <_2 \pi(m).$$

Proof. Homework 3.

Gödel's Incompleteness Theorem

Gödel's Incompleteness Theorem (1931) states that

- No reasonable system of axioms which is strong enough for the development of arithmetic can prove every true statement of arithmetic.

☞ A reasonable system of axioms is one for which there is an algorithm for determining what is an axiom. (Thus, there is no algorithm for generating all and only truths of arithmetic.)

☞ Very little of arithmetic needs to be developed – little more than addition, multiplication and order.

Arithmetic in $ZF^- - P$

☞ We have been developing arithmetic in ZF^- without the Power Set Axiom (Axiom 8.) ZF^- (and in fact all of ZFC) is a reasonable system of axioms strong enough for developing arithmetic, so it is incomplete: there are truths of set theory (in fact, truths about systems of natural numbers) which cannot be proven in set theory.

☞ In fact, no way of reasonable way of extending the axioms of ZFC is sufficient to make-up for this deficiency of strength – there will still be truths of arithmetic which are unprovable.

Arithmetic in Second-Order Logic

Second-Order Logic is an extension of first-order logic (the logic of set theory) which allows two kind of quantifiers: quantifiers over objects and quantifiers over classes of objects. These are two different types of entities, so that classes of objects are not objects.

The Dedekind-Peano axioms can be formulated as a single statement $\Phi(N, 0, S)$ in second-order logic: the conjunction of five statements (notice that (**N5**) is a single statement about all classes of entities):

N1 $0 \in N$

N2 $S : N \to N$

N3 $\forall n, m(S(n) = S(m) \to n = m)$ (i.e. S is injective),

N4 $\forall n\, S(n) \neq 0$

N5 **Induction Principle**. For every $X \subseteq N$,

$$0 \in X \wedge \forall n \in N(n \in X \to S(n) \in X) \quad \to \quad X = N$$

Arithmetic in First-Order Logic

Arithmetic can be developed in first-order logic by extending the logic to include $0, S, +, \cdot$ and adding infinitely many axioms, the Peano Axioms (the Induction Principle (**N5**) can no longer be stated in first-order logic, but must be replaced by the Induction Scheme):

P1 If $S(n) = S(m)$ then $n = m$.

P2 $S(n) \neq 0$.

P3 $n + 0 = n$.

P4 $n + S(m) = S(m + n)$.

P5 $n \cdot 0 = 0$.

P6 $n \cdot S(m) = n \cdot m + m$.

P7 If $n \neq 0$ then $n = S(k)$ for some k.

P8 For any first-order formula in the language of arithmetic, φ,

$$\varphi(0) \land \forall n\,(\varphi(n) \to \varphi(S(n))) \quad \to \quad \forall n\,\varphi(n).$$