Induction, Recursive Definition, and Infinity

Carl Pollard

October 18, 2011

Review of the Natural Numbers (1/3)

- We defined a set to be **inductive** provided:
  - $\emptyset$ is a member, and
  - the successor of every member is a member.
- We defined a set to be a **natural number** provided it is a member of every inductive set.
- We added to our set theory the assumption that there is a set (which we called ω) whose members are the natural numbers.

Review of the Natural Numbers (2/3)

- We proved that ω is inductive.
- We proved that ω is a subset of every inductive set.
- We proved the **Principle of Mathematical Induction (PMI)**, that the only inductive subset of ω is ω.

  Soon we'll see that PMI is an invaluable resource for proving important theorems.

Review of the Natural Numbers (3/3)

- We mentioned the $<$ and $\leq$ relations on ω.
- We mentioned (but didn't prove) that ω is well ordered by $\leq$ (i.e. forms a chain where every nonempty subset has a least member).
- We called the function that maps each natural number to its successor **suc**.
- We mentioned (but didn't prove) that **suc** is a bijection from ω to $\omega \setminus \{0\}$.

- We promised to define the binary operations **addition** ($+$), **multiplication** ($\cdot$), and **exponentiation** ($\star$).
- The missing proofs and definitions are supplied in *FFLT* ch. 4.3; right now we'll just survey the main points.

The $<$ Relation on ω

- We defined $<$ to be proper subset inclusion on ω.
- But it's more convenient to redefine $<$ as the relation

$$< =_{\text{def}} \{\langle m, n\rangle \in \omega \times \omega \mid m \in n\}$$

- Later we'll see that these two definitions are equivalent (in the sense of defining the same set of ordered pairs).

How to Do Inductive Proofs

- PMI is the tool of choice whenever we want to prove that a condition $\phi[n]$ is true for every natural number n.
- The trick is to consider the set

$$\{n \in \omega \mid \phi[n]\}$$

  and show that it is inductive.
- To do that, first we prove $\phi[0]$ (called the **base case**).
- Then we prove that, if we assume $\phi[k]$ for an arbitrary natural number k (the so-called **inductive hypothesis**), then $\phi[\mathbf{suc}(k)]$ follows (the so-called **inductive step**).

A Simple Inductive Proof

Theorem: $\mathsf{ran}(\mathbf{suc}) = \omega \setminus \{0\}$.

Proof. Obviously $0 \notin \mathsf{ran}(\mathbf{suc})$.

Let T be the set of all natural numbers that are either 0 or else the successor of some natural number.

We must show that T is inductive, that is that (1) $0 \in T$ and (2) for each $n \in T, \mathbf{suc}(n) \in T$.

But both of these are immediate consequences of the definition of T. $\square$

Motivating Recursive Definition (1/2)

- Why don't we just say '$1 + n$' instead of '$\mathbf{suc}(n)$'?
- Answer: because we haven't defined + yet!
- Yet it seems clear how + should work: for any $m \in \omega$
  - $m + 0$ should be m
  - if $k \neq 0$, so that $k = \mathbf{suc}(n)$ for some n, $m+k$ should be $\mathbf{suc}(m+n)$.

Motivating Recursive Definition (2/2)

- That is, for each $m \in \omega$ we would like to define addition *recursively* by the equations

$$m + 0 = m$$
$$m + \mathbf{suc}(n) = \mathbf{suc}(m + n)$$

- But how do we know recursive definitions make sense?
- Answer: because of the *Recursion Theorem.*

The Recursion Theorem (RT)

Theorem: Let X be a set, $x \in X$, and $F \colon X \to X$. Then there exists a unique function $h \colon \omega \to X$ such that:

1. $h(0) = x$, and
2. (2) for every $n \in \omega$, $h(\mathbf{suc}(n)) = F(h(n))$.

Proof. By induction. For details, see the Appendix of FFLT. □

Defining Addition (1/2)

- Suppose $m \in \omega$. We will define a unary operation on ω A_m such that

$$A_m(0) = m$$
$$A_m(\mathbf{suc}(n)) = \mathbf{suc}(A_m(n))$$

  using RT with the following instantiations of X, x, and F:
  - $X = \omega$
  - $x = m$
  - $F = \mathbf{suc}$.
- Then the function h whose unique existence is guaranteed by RT has just the properties we want for A_m.

Defining Addition (2/2)

- We then define $+$ to be the binary operation on ω that maps each $\langle m, n\rangle \in \omega \times \omega$ to $A_m(n)$.
- It follows from this definition that for all $m, n \in \omega$:

$$m + 0 = m$$

$$m + \mathbf{suc}(n) = \mathbf{suc}(m + n)$$

Another Simple Inductive Proof (Exercise)

Theorem: For every natural number n, $1 + n = \mathbf{suc}(n)$.

Proof. Exercise.

□

Defining Multiplication (1/2)

- Suppose $m \in \omega$. We will define a unary operation on ω M_m such that

$$M_m(0) = 0$$

$$M_m(\mathbf{suc}(n)) = m + (M_m(n))$$

  using RT with the following instantiations of X, x, and F:

  - $X = \omega$
  - $x = m$
  - $F = A_m$.

- Then the function h whose unique existence is guaranteed by RT has just the properties we want for M_m.

Defining Multiplication (2/2)

- We then define $\cdot$ to be the binary operation on ω that maps each $\langle m, n\rangle \in \omega \times \omega$ to $M_m(n)$.
- It follows from this definition that for all $m, n \in \omega$:

$$m \cdot 0 = m$$

$$m \cdot (1 + n) = m + m \cdot n$$

  Note 1: You might recognize this last equation as an instance of the Distributive Law, but we haven't proved that yet.

  Note 2: As in everyday life, the '$\cdot$' for multiplication is often omitted.

Yet Another Simple Inductive Proof (Exercise)

Theorem: For every natural number n, $1 \cdot n = n$.

Proof. Exercise.

$\square$

Five Laws of Arithmetic

The following can all be proved inductively:

1. Commutativity of Addition:

$$m + n = n + m$$

2. Associativity of Addition:

$$m + (n + p) = (m + n) + p$$

3. Commutativity of Multiplication:

$$mn = nm$$

4. Associativity of Multiplication:

$$m(np) = (mn)p$$

5. Distributivity of Mulitplication over Addition:

$$m(n + p) = mn + mp$$

Some Notation

- Recall that an A**-string of length** n is a function $f\colon n \to A$, i.e. a member of A^n.
- Suppose that for each $i < n$, $f(i) = x_i$. Then $\bigcup \mathsf{ran}(f)$ is often written as $\bigcup_{i<n} x_i$.
- By an **infinite sequence** in A, we mean a function $f\colon \omega \to A$.
- Suppose that for each $i \in \omega$, $f(i) = x_i$. Then $\bigcup \mathsf{ran}(f)$ is often written as $\bigcup_{i\in\omega} x_i$.
- *Example:* For any A, let f_A be the infinite sequence in $\wp(\omega \times A)$ that maps each $i \in \omega$ to A^i. Then $\bigcup_{i\in\omega} A_i$ is the set of all A-strings, usually abbreviated as A^*.

The (Reflexive) Transitive Closure of a Relation

Suppose R is a binary relation on A. Then informally, the **transitive closure** of R, written R^+, is usually recursively "defined" as follows:

- For all $n \in \omega$, define $h(n)$ by:

$$h(0) =_{\text{def}} \text{id}_A$$
$$h(n+1) =_{\text{def}} h(n) \circ R.$$

- Then $R^+ =_{\text{def}} \bigcup_{n\in\omega} h(n+1)$.

- And the **reflexive transitive closure** of R is defined as:

$$R^* =_{\text{def}} R^* \cup \text{id}_A = \bigcup_{n\in\omega} h(n).$$

Exercise: Use RT to give a *formal* recursive definition of h.

The Transitivity of R^+

Theorem: Suppose R is a binary relation on A. Then R^+ is transitive.

Proof. Exercise.

□

A Characterization of R^+

Theorem: Suppose R is a binary relation on A. Then R^+ is the intersection of all transitive relations on A which are supersets of R.

Proof. Exercise.

□

Transitive Sets (1/2)

- A set A is said to be **transitive** iff every member of a member of A is itself a member of A.

- It is easy to show that each of the following three conditions on A are equivalent to transitivity:

  1. $(\bigcup A) \subseteq A$
  2. every member of A is a subset of A
  3. $A \subseteq \wp(A)$

Transitive Sets (2/2)

Lemma: If A is transitive, then $\bigcup s(A) = A$.

Proof. See FFLT, ch. 4. $\square$

Lemma: Every natural number is transitive.

Proof. Exercise. [Hint: use induction.] $\square$

Injectivity of the Successor Function

Theorem: suc is injective.

Proof. See FFLT, ch. 4. $\square$

Note: Soon we will use this to prove that ω is *infinite* (not in one-to-one correspondence with any natural number).

More Key Facts about ω

Remember that by definition:

$$m < n \text{ iff } m \in n$$
$$m \leq n \text{ iff } m < n \text{ or } m = n$$

- For all $n \in \omega$, $n = \{m \in \omega \mid m < n\}$.
- For all $n \in \omega$, $n \notin n$.
- $<$ is transitive, irreflexive, and connex.
- For all $m, n \in \omega$, $m \in n$ iff $m \subsetneq n$.
- $\leq$ is a chain.
- Every nonemempty subset of ω has a least element (and so $\leq$ is a well-ordering).

Equinumerosity, Finiteness and Infinity

- Two sets A and B are said to be **equinumerous**, written $A \approx B$, iff there is a bijection from A to B.
- A set is called:
  - **finite** iff it is equinumerous with a natural number
  - **infinite** iff it is not finite
  - **Dedekind infinite** iff it is equinumerous with a proper subset of itself
- We've already shown that **suc** is a bijection from ω to $\omega \setminus \{0\}$, so ω is Dedekind infinite.

Every Set is 'Smaller' than its Powerset

Theorem: No set is equinumerous with its powerset.

Proof. Let g be any function from A to $\wp A$, and let $B = \{x \in A \mid x \notin g(x)\}$.

We will show $B \notin \mathsf{ran}(g)$, so that g cannot be surjective (and therefore cannot be bijective).

Suppose it were true that $B \in \mathsf{ran}(g)$. Then there would have to be some $y \in A$ such that $B = g(y)$.

But then we would have $y \in B$ iff $y \notin g(y)$, i.e. $y \in B$ iff $y \notin B$, which is a contradiction.

So our assumption that $B \in \mathsf{ran}(g)$ must have been false.

$\square$

Facts about Finite and Infinite Sets (1/2)

Theorem: No natural number is Dedekind infinite.

Proof. Exercise.

$\square$

Corollary: No finite set is Dedekind infinite (and so every Dedkind infinite set is infinite).

Proof. Exercise.

$\square$

Corollary: ω is infinite.

Proof. Immediate.

$\square$

Facts about Finite and Infinite Sets (2/2)

Corollary: No two distinct natural numbers are equinumerous.

Proof. Exercise. □

Corollary: Each finite set A is equinumerous with a unique natural number $|A|$, called its **cardinality**.

Proof. Exercise. □

Theorem: Every subset of a finite subset is finite.

Proof. See ch. 5. □

Domination

- We say a set A is **dominated** by a set B, written $A \preceq B$, iff there is an injection from A to B, or, equivalently, iff A is equinumerous with a subset of B.
- If $A \preceq B$ and $A \not\approx B$, A is said to be **strictly dominated** by B, written $A \precnapprox B$ or $A \prec B$.
- *Exercises* For any sets A, B, and C:
  - $A \preceq A$
  - if $A \preceq B$ and $B \preceq C$ then $A \preceq C$
  - $A \preceq \wp(A)$

The Schröder-Bernstein Theorem

Theorem:
For any sets A and B, if $A \preceq B$ and $B \preceq A$, then $A \approx B$.

Proof. See the Appendix of FFLT. The proof is not hard, but extraordinarily ingenious and a bit on the long side. □

Choice Functions

- For any set A, the **nonempty powerset** of A, written $\wp_{ne}(A)$, is the set $\wp A \setminus \{\emptyset\}$ of nonempty subsets of A.
- A **choice function** for A is a function $c \colon \wp_{ne}(A) \to A$ such that, for each nonempty subset B of A, $c(B) \in B$.

Assumption 7: Choice

Every set has a choice function.

About Choice

- It has been proved (Cohen, 1963) that Choice is *independent* of our other assumptions, i.e. if if our other assumptions are consistent, then either Choice or its denial can be consistently added.
- Some mathematicians consider Choice less intuitive than the other assumptions.
- But most mathematicians assume Choice, because there many useful theorems can't be proved without it, such as the following.

ω is a 'Least' Infinite Set

Theorem: If A is infinite, then $\omega \preceq A$.

Proof. See the Appendix of *FFLT*. This is another clever proof, and not too long. It makes crucial use of Choice.

□

Corollary (Dedekind-Peirce Theorem): Every infinite set is Dedekind infinite.

Proof. See *FFLT*, ch. 5. (Note that the converse, proved earlier, did not require Choice.)

□

Countable and Denumerable Sets

A set is called:

- **countable** iff it is dominated by ω
- **denumerable**, **denumerably infinite**, or **countably infinite** iff it is countable and infinite

Theorem: Any countably infinite set is equinumerous with ω.

Proof. Exercise.

□

Theorem: Any infinite subset of ω is equinumerous with ω.

Proof. Exercise.

□

Some Countably Infinite Sets

- ω (natural numbers)
- $\omega \times \omega$ (ordered pairs of natural numbers)
- $\omega \setminus \{0\}$ (positive natural numbers)
- $\{2n \mid n \in \omega\}$ (even natural numbers)
- the primes
- $\mathbb{Z}$ (the integers)
- $\mathbb{Q}$ (the rationals)
- A^* (the A-strings, for any nonempty finite A)

Nondenumerable Sets

- A set is called **uncountable**, **nondenumerable**, or **nondenumerably infinite**, iff it is not countable.
- Some nondenumerable sets equinumerous with $\wp(\omega)$:
  - $\mathbb{R}$ (the reals)
  - $\{r \in \mathbb{R} \mid 0 \leq r \leq 1\}$ (the unit interval)
  - $\mathbb{R} \setminus \mathbb{Q}$ (the irrationals)
  - $\mathbb{R} \times \mathbb{R}$ (the plane)
  - ω^ω (infinite sequences of natural numbers)
  - $\wp(A^*)$ (the A-**languages**, i.e. sets of A-strings, for any nonempty finite A)