Additional notes for Feb. 17th

Dr. Holmes

February 17, 2004

The additional remarks for today concern the proof of the pigeonhole principle. My version of this proof is very similar to the author's version in section 6.2, but there's a difference in the way we construct the bijection used in the induction step.

Definition: We define $\mathcal{N}_n$, for each natural number n, as the set $\{m \in \mathcal{N} \mid m \leq n\}$. For example, $\mathcal{N}_3$ is the set $\{1, 2, 3\}$.

Definition: We say that the set A "has n elements" if and only if there is a bijection from $\mathcal{N}_n$ to A. Notice that if f is a bijection from $\mathcal{N}_n$ to A then f^{-1} is a bijection from A to $\mathcal{N}_n$, and if g is a bijection from A to $\mathcal{N}_n$ then f^{-1} is a bijection from $\mathcal{N}_n$ to A: it doesn't really matter which way we suppose that the bijection goes.

Notice that this definition actually corresponds exactly to the way that we count small finite sets using numbers.

We digressed to discuss the usual formal set theoretical definition of the natural numbers. This is motivated by an alternative method of counting which is possible if we have 0 as a natural number: A has n members if and only if there is a bijection between A and the set $\{0, \ldots n-1\}$, the set of all non-negative integers less than n. We can take this farther: we can *define* the natural number n as the set of all natural numbers less than n. This might seem to be circular, but it isn't: it is merely recursive. 0 is defined as the set of all non-negative integers less than 0, which is the empty set. 1 is defined as $\{0\}$, or equivalently $\{\emptyset\}$, the set whose only element is the empty set $\emptyset = \{\}$ (for some reason, students frequently confuse $\emptyset$ and $\{\emptyset\}$ – these sets are quite different – the first one has no elements and the second has one element, for example). 2 is defined as $\{0, 1\}$, which is $\{\emptyset, \{\emptyset\}\}$ by the first two definitions. In this way, each natural number can successfully be identified as a set.

You are not responsible for this "definition": I mention it as an example of a process you will see in mathematical foundations, which is the effort to code all mathematical objects as sets. Another example of this process is the definition of the ordered pair (a, b) as the set $\{\{a\}\{a, b\}\}$. One should not believe that this "definition" of the natural numbers explains what the natural numbers "really are"; in fact, there are other codings of the natural numbers as sets which have been used.

We now return to stuff you are responsible for...

Theorem (Pigeonhole Principle): For any natural numbers n and m, if there is an injection from the set $\mathcal{N}_n$ to the set $\mathcal{N}_m$, then $n \leq m$.

Proof of Pigeonhole Principle: This statement is obviously true, on a common sense understanding of what it says. Proving it is a little tricky.

It is proved by induction. The statement we prove by induction is $(\forall n.P(n))$, where $P(n)$ abbreviates "for all m, if there is an injection from the set $\mathcal{N}_n$ to the set $\mathcal{N}_m$, then $n \leq m$.". Notice how I took a statement with *two* quantifiers over the natural numbers and defined $P(n)$ by peeling off one of the quantifiers. The role of the two variables m and n in the theorem is not symmetrical, and the other approach to setting up the induction would give a rather different proof if it were practical at all (I haven't tried it).

Basis step: "for all m, if there is an injection from the set $\mathcal{N}_1$ to the set $\mathcal{N}_m$, then $1 \leq m$."

This is valid because $1 \leq m$ is true no matter what injections there may be.

Induction step: "for all natural numbers k, if it is true that for all m, if there is an injection from the set $\mathcal{N}_k$ to the set $\mathcal{N}_m$, then $k \leq m$, then it is true that for all m, if there is an injection from the set $\mathcal{N}_{k+1}$ to the set $\mathcal{N}_m$, then $k + 1 \leq m$."

Admittedly, the induction step is rather hard to read. It is probably easier to read in logical notation!

We assume "for all m, if there is an injection from the set $\mathcal{N}_k$ to the set $\mathcal{N}_m$, then $k \leq m$.": this is the inductive hypothesis.

Our goal is to prove using ind hyp that "for all m, if there is an injection from the set $\mathcal{N}_{k+1}$ to the set $\mathcal{N}_m$, then $k+1 \leq m$."

Let m be an arbitrary natural number.

Suppose that there is an injection from the set $\mathcal{N}_{k+1}$ to the set $\mathcal{N}_m$: call it f.

Now our goal is to prove that $k+1 \leq m$.

Our strategy is as follows: we prove that if there is a bijection f from the set $\mathcal{N}_{k+1}$ to the set $\mathcal{N}_m$, there must be a bijection f^* from the set $\mathcal{N}_k$ to the set $\mathcal{N}_{m-1}$. If we show this, it will follow by the inductive hypothesis that $k \leq m-1$, from which it will follow by standard properties of inequalities that $k+1 \leq m$, which is our goal.

First we need to show that $m > 1$ (so that $m-1$ will make sense). If there is an injection h from $\mathcal{N}_{k+1}$, which has at least the elements 1 and $k+1$, to $\mathcal{N}_m$, then there must be distinct elements $h(1)$ and $h(k+1)$ of $\mathcal{N}_m$ (distinct because h is an injection), so $m \neq 1$, because there are not two distinct elements of $\mathcal{N}_1 = \{1\}$. We know that a natural number not equal to 1 must be greater than 1.

There are two different ways you have been shown to define a bijection f^* from the set $\mathcal{N}_k$ to the set $\mathcal{N}_{m-1}$ given a bijection f from the set $\mathcal{N}_{k+1}$ to the set $\mathcal{N}_m$.

If f doesn't map any value $i \leq k$ to m, then it is easy to get f^* from f: just omit the value of f at $k+1$ and you are done (you now have a map with domain $\mathcal{N}_k$ instead of $\mathcal{N}_{k+1}$ whose range is restricted to $\mathcal{N}_{m-1}$; it is easy to see that it is still an injection).

If f maps some element $i \leq k$ to m, then we appear to have a problem. But it isn't a bad problem. Notice that $f(k+1) < m$ because f is an injection (we can't map two different numbers to m). This means that we can define $f^*(j)$ as $f(j)$ for all $j \neq i$ and define $f^*(i)$ as $f(k+1)$. This will still be an injection: the values of $f^*(j)$ certainly can't cause any trouble, and the value $f(k+1)$ assigned to $f^*(i)$ has to be different from all values $f^*(j) = f(j)$ for $j \neq i$ because f is an injection and so would not map $k+1$ to the same value as any j.

This shows that there is a bijection from the set $\mathcal{N}_k$ to the set $\mathcal{N}_{m-1}$ if there is a bijection from the set $\mathcal{N}_{k+1}$ to the set $\mathcal{N}_m$, and we have already seen that this is enough to prove the theorem.

Thus far, the proof given is the same as in the book. My alternative definition of f^* went as follows: the idea is to remove the arrow from $k+1$ to $f(k+1)$, then reduce each of the range values greater than $f(k+1)$ by one: this will produce a map from the set $\mathcal{N}_k$ to the set $\mathcal{N}_{m-1}$ as desired. The formal definition is

$$f^*(i) = \begin{array}{ll} f(i) & \mathtt{if\ f(i) < f(k+1)} \\ \\ f(i) - 1 & \mathtt{if\ f(i) > f(k+1)} \end{array}$$

for each $i \leq k$. The case $f(i) = f(k+1)$ can't happen because f is an injection. It is also fairly easy to see that this must be an injection. This definition of f^* can be used in exactly the same way as the other to complete the proof.

The Pigeonhole Principle is remarkably powerful for such an "obvious" statement. We will use it initially to show that the number of elements in a finite set is a well-defined notion:

Counting Theorem: Let A be a set. If A has m elements and A has n elements, then $m = n$.

Proof: Suppose A has m elements and A has n elements. By definition of "having a number of elements", we are given a bijection $f : \mathcal{N}_m \to A$ and a bijection $g : \mathcal{N}_n \to A$.

We have proved that compositions of injections are injections and compositions of surjections are surjections, and from this it follows directly that compositions of bijections are bijections.

Notice that f^{-1} is a bijection from A to $\mathcal{N}_m$ and g^{-1} is a bijection from A to $\mathcal{N}_n$. The composition $g^{-1}f$ will be a bijection from $\mathcal{N}_m$ to $\mathcal{N}_n$. By the Pigeonhole Principle, the existence of this bijection implies $m \leq n$. The composition $f^{-1}g$ (the inverse of $g^{-1}f$) will be a bijection from $\mathcal{N}_n$ to $\mathcal{N}_m$. By the Pigeonhole Principle, the existence of this bijection implies $n \leq m$. If $m \leq n$ and $n \leq m$, then $m = n$, which is what we wanted to show.

This Theorem allows us to make the following

Definition: For any set A, we define $|A|$, the cardinality or size of A, as the unique natural number n (if there is one) such that A has n elements.

The theorem allows us to exclude the nasty possibility that there might be more than one number n which could be taken to be $|A|$.