

There is nothing in the axioms we have assumed that tells us everyday things such as “how many” elements a set has! All we have is the definition of “finite set” in terms of “equipotence.” So, we have to *prove* some of these things, just to see that they *can* be proved.

Here are two theorems that are obviously true. The problem is to *deduce* the theorems from axioms and previously proved theorems.

Theorem *If A is a subset of a finite set B , then A is finite.*

Proof: We have to show that, if $B \sim S_n$ for some $n \in \mathbb{N}$, and $A \subseteq B$, then $A \sim S_m$ for some $m \in \mathbb{N}$. Let us call this statement $P(n)$. For later use we need to recall that $S_n = \{k \in \mathbb{N} : k < n\}$.

Let us first prove this when $B = S_n$ for some $n \in \mathbb{N}$, using induction.

Thus, if $n = 0$ and $A \subseteq B = S_0 = \emptyset$, then $A = \emptyset = S_0$ hence A is finite, so $P(0)$ is true.

Now we suppose our statement $P(k)$ is true for all $k < n$, where $n > 0$, and seek to show that it is true for $k = n$ as well.

A very easy case occurs when $A = S_n$, for the set S_n is finite by definition. We don't actually use this case.

Another easy case: suppose $A \subseteq S_n$ and suppose that $n - 1 \notin A$. Then A is a subset of S_{n-1} so A is finite by the induction assumption. We *will* use this case.

We have to consider the main case, when $A \subseteq S_n$, and $n - 1 \in A$. We set $A' := A \setminus \{n - 1\}$. Then $n - 1 \notin A'$, so A' is a subset of S_{n-1} hence A' is finite, by the induction assumption. That is, there exists $m' \in \mathbb{N}$ and a function $g' : A' \rightarrow S_{m'}$ that is one-to-one and onto. Since $S_{m'} \cup \{m'\} = S_{m'+1}$ we can define a function $g : A \rightarrow S_{m'+1}$ by adding the ordered pair $(n - 1, m' + 1)$ to the function g' . That is, $g := g' \cup \{(n - 1, m' + 1)\}$ (this is one of the few instances where it is useful to have defined “function” as a set of ordered pairs!) It is trivial to show that g maps $A = A' \cup \{n - 1\}$ onto $S_{m'+1}$ in a one-to-one manner. (You should be able to show it “in your head”)

To conclude we set $m := m' + 1$, so $P(n)$ is true when we restrict B to be one of the sets S_n .

Having finished the proof when B is one of the S_n , it remains to deal with the case when B is some other finite set. Any function $f : B \rightarrow S_n$ that is one-to-one and onto maps A onto $f(A)$ in a one-to-one and onto manner. Then $f(A)$ is finite since it is a subset of S_n . There is then some $m \in \mathbb{N}$ and a function $g : f(A) \rightarrow S_m$ that is one-to-one and onto. It is trivial to show that the composite mapping $g \circ f$ is the desired equivalence between A and S_m . This completes the proof of the Theorem.

We say that a set B **has** n **elements** if there exists $n \in \mathbb{N}$ and a function $f : B \rightarrow S_n$ that is one-to-one and onto. In proving the next Theorem we will have occasion to use the result of Special problem 3.

Theorem *If B has n elements and A has m elements and $n > m$ then there does not exist a function $h : A \rightarrow B$ that is onto.*

Proof: Suppose, to be contrary, that there exists $f : A \rightarrow B$ that is onto. We are given that there exist one-to-one and onto functions $g : A \rightarrow S_m$ and $h : B \rightarrow S_n$. Let k denote the composite function $h \circ f \circ g^{-1}$, so $k : S_m \rightarrow S_n$, and because each of our functions h , f and g^{-1} is *onto*, so is k . In particular, there exists $x_o \in S_m$ such that $k(x_o) = n - 1$. We recall that $k = \{(x, k(x)) : x \in S_m\}$. Now we construct a new function $K : S_n \rightarrow S_n$ by setting

$$K := k \cup \{(x, x) : x \in S_n \setminus S_m\}.$$

Since k was already onto, so is K . By the theorem proved in Special Problem 3, K is also one-to-one. But $K(n - 1) = n - 1$ and $K(x_o) = k(x_o) = n - 1$. Since $x_o \neq n - 1$ and K is one-to-one we have the contradiction $K(n - 1) = K(x_o)$. This completes the proof.

Here is another theorem – I believe this is essentially the “pigeonhole principle” – that you might try to prove now.

Theorem *If B has n elements and A has m elements and $n > m$ then there does not exist a function $h : B \rightarrow A$ that is one-to-one.*