Math 300 **Introduction to Mathematical Reasoning** **Fall 2018**

Handout 12: More About Finite Sets

Please read this handout after Section 9.1 in the textbook.

The Cardinality of a Finite Set

Our textbook defines a set A to be ***finite*** if either A is empty or $A \approx \mathbb{N}_k$ for some natural number k, where $\mathbb{N}_k = \{1, \ldots, k\}$ (see page 455). It then goes on to say that A has ***cardinality k*** if $A \approx \mathbb{N}_k$, and the empty set has cardinality 0.

These are standard definitions. But there is one important point that the book left out: Before we can say that the cardinality of a finite set is a well-defined number, we have to ensure that it is not possible for the same set A to be equivalent to $\mathbb{N}_n$ and $\mathbb{N}_m$ for two different natural numbers m and n. This may seem obvious, but it turns out to be a little trickier to prove than you might expect. The purpose of this handout is to prove that fact.

The crux of the proof is the following lemma about subsets of the natural numbers.

Lemma 1. *Suppose m and n are natural numbers. If there exists an injective function from $\mathbb{N}_m$ to $\mathbb{N}_n$, then $m \le n$.*

Proof. For each natural number n, let $P(n)$ be the following statement:

> For every $m \in \mathbb{N}$, if there is an injective function from $\mathbb{N}_m$ to $\mathbb{N}_n$, then $m \le n$.

We will prove by induction on n that $P(n)$ is true for every natural number n.

We begin with the base case, $n = 1$. Assume for the sake of contradiction that $P(1)$ is false: this means that for some $m \in \mathbb{N}$, there is an injective function $f : \mathbb{N}_m \to \mathbb{N}_1 = \{1\}$ and $m > 1$. Then $m \ge 2$ since m is an integer, so 1 and 2 are both elements of $\mathbb{N}_m$, and the fact that 1 is the only element of $\mathbb{N}_1$ implies that $f(1) = 1$ and $f(2) = 1$. But this contradicts the assumption that f is injective.

Now for the inductive step, let $k \in \mathbb{N}$ and assume that $P(k)$ is true. We need to prove that $P(k+1)$ is true, namely

> For every $m \in \mathbb{N}$, if there is an injective function from $\mathbb{N}_m$ to $\mathbb{N}_{k+1}$, then $m \le k+1$.

To prove this, let $m \in \mathbb{N}$ be arbitrary, and assume there exists an injective function $f : \mathbb{N}_m \to \mathbb{N}_{k+1}$. Either $k+1 \in \operatorname{range}(f)$ or not; and if $k+1$ is in the range of f, then either $k+1 = f(m)$ or $k+1 = f(j)$ for some $j < m$. Thus we can divide the argument into the following three cases.

Case 1: $k+1 \notin \operatorname{range}(f)$. We can define a new function $f' : \mathbb{N}_m \to \mathbb{N}_k$ just by shrinking the codomain of f: $f'(i) = f(i)$ for each $i \in \mathbb{N}_m$. This function is still injective, because if i_1, i_2 are elements of $\mathbb{N}_m$ such that $f'(i_1) = f'(i_2)$, then the definition of f' shows that $f(i_1) = f(i_2)$, so $i_1 = i_2$ because f is injective. We now have produced an injective function $f' : \mathbb{N}_m \to \mathbb{N}_k$, so the inductive hypothesis implies $m \le k < k+1$.

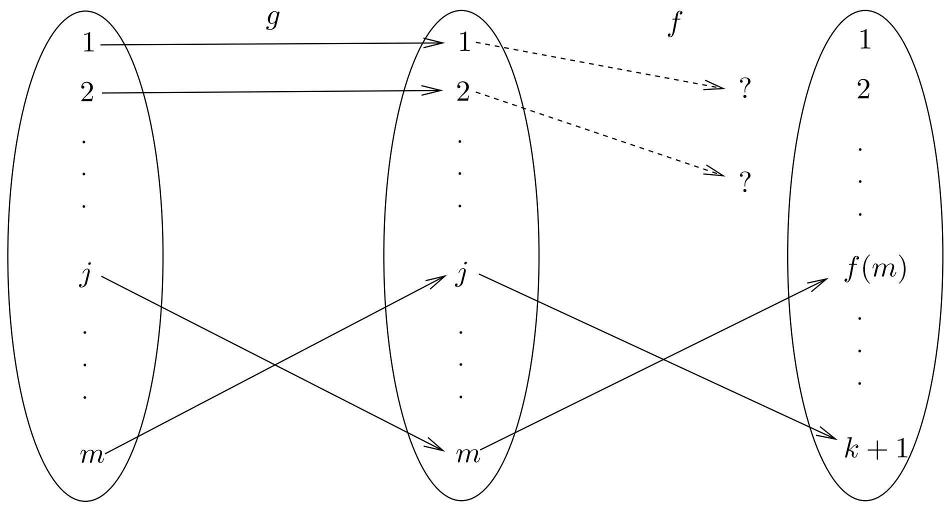

Figure 1: Case 3.

Case 2: $k+1 = f(m)$. If $m = 1$, then $m \le k+1$ automatically, so we can assume $m \ge 2$. In this case, $m-1$ is also a natural number, and we can define a new function $f' \colon \mathbb{N}_{m-1} \to \mathbb{N}_k$ by $f'(i) = f(i)$. The facts that f is injective and $f(m) = k+1$ together imply that $f(i) \neq k+1$ whenever $1 \le i \le m-1$, and thus f' is a well-defined function from $\mathbb{N}_{m-1}$ to $\mathbb{N}_k$. It is injective by exactly the same argument as in Case 1. Now the inductive hypothesis implies $m-1 \le k$, and therefore $m \le k+1$ as desired.

Case 3: $k+1 = f(j)$ for some $j < m$. In this case, we define a function $g \colon \mathbb{N}_m \to \mathbb{N}_m$ that interchanges j and m and leaves everything else alone:

$$g(i) = \begin{cases} m & \text{if } i = j, \\ j & \text{if } i = m, \\ i & \text{if } i \neq j \text{ and } i \neq m. \end{cases}$$

(See Figure 1.) An easy verification shows that $g \circ g$ is the identity map of $\mathbb{N}_m$, so g is bijective (because it is its own inverse function). Then the function $f \circ g \colon \mathbb{N}_m \to \mathbb{N}_{k+1}$ is injective (because it is a composition of injective functions), and it takes m to $k+1$ because $f(g(m)) = f(j) = k+1$. Thus we can apply the argument of Case 2 to $f \circ g$, and conclude again that $m \le k+1$. □

Using this lemma, we can prove the main theorem of this section.

Theorem 2 (The Cardinality of a Finite Set is Well-Defined)**.** *Suppose A is a set. If m and n are natural numbers such that $A \approx \mathbb{N}_n$ and $A \approx \mathbb{N}_m$, then $m = n$.*

Proof. Suppose A is a set such that $A \approx \mathbb{N}_n$ and $A \approx \mathbb{N}_m$. The hypothesis means there are bijections $f \colon A \to \mathbb{N}_n$ and $g \colon A \to \mathbb{N}_m$. The map $f \circ g^{-1} \colon \mathbb{N}_m \to \mathbb{N}_n$ is a composition of bijections, and hence it is injective, so the lemma applies that $m \le n$. Similarly, $g \circ f^{-1}$ is an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$, so $n \le m$. Together, these two inequalities prove that $m = n$. □

Thanks to this theorem, if A is any nonempty finite set, there a *unique* natural number n for which there exists a bijection from A to $\mathbb{N}_n$. This natural number is denoted by $\operatorname{card}(A)$ and is called the ***cardinality of A***.

Properties of Finite Sets

In addition to the properties covered in Section 9.1, we will be using the following important properties of finite sets.

Theorem 3 (Fundamental Properties of Finite Sets)**.** *Suppose A and B are finite sets.*

(*a*) *Every subset of A is finite, and has cardinality less than or equal to that of A.*

(*b*) *$A \cup B$ is finite, and*

$$\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A \cap B).$$

(*c*) *$A \times B$ is finite, and*

$$\operatorname{card}(A \times B) = \operatorname{card}(A) \cdot \operatorname{card}(B).$$

Proof. Part (a) is Theorem 9.6 in the textbook. For the proofs of parts (b) and (c), see the exercises at the end of this handout. □

Theorem 5 below gives some very useful criteria for showing that a set is finite. Before proving it, though, we need the following lemma. (The proof of this lemma actually appears as part of the proof of Theorem 9.6 in the textbook. But for future reference, it's useful to state and prove it as a separate lemma.)

Lemma 4. *Suppose A and B are nonempty sets, and $f\colon A \to B$ is an injective function. Then A is equivalent to the nonempty subset $f(A) \subseteq B$.*

Proof. We can define a new function $g\colon A \to f(A)$ just by setting $g(x) = f(x)$ for every $x \in A$. The assumption that $A \neq \emptyset$ means there exists some $x_0 \in A$, and thus $f(x_0)$ is an element of $f(A)$, showing that $f(A)$ is nonempty. We will show that g is bijective, from which the conclusion follows.

First suppose $y \in f(A)$ is arbitrary. By definition, this means that there exists some $x \in A$ such that $f(x) = y$. By the way we defined g, this also means $g(x) = y$, showing that g is surjective.

Next, suppose x_1 and x_2 are elements of A such that $g(x_1) = g(x_2)$. Then the definition of g shows that $f(x_1) = f(x_2)$, and injectivity of f implies $x_1 = x_2$. Thus g is also injective. □

Theorem 5. *Let A be a nonempty set.*

(*a*) *If there exists an injection from A to a finite set, then A is finite.*

(*b*) *If there exists a surjection from a finite set to A, then A is finite.*

Proof. First suppose B is finite and there exists an injection $f\colon A \to B$. Then Lemma 4 shows that A is equivalent to the nonempty subset $f(A) \subseteq B$, and Theorem 3(a) above shows that $f(A)$ is finite. Thus A is also finite by Theorem 9.3 in the text.

Now suppose B is finite and there exists a surjection $f\colon B \to A$. The fact that A is nonempty guarantees that B is also nonempty (can you see why?). Exercise 10 on page 461 of the text shows that there is an injection $h\colon A \to B$, and then it follows from part (a) above that A is finite. $\square$

Exercises

Note: In doing these exercises, you may use the results of this handout, along with any of the theorems and exercises in Section 9.1 of the textbook.

1. (a) Prove that if A and B are disjoint finite sets, then $A \cup B$ is finite and $\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B)$. [Hint: In the case that A and B are nonempty, consider the function $h\colon A \cup B \to \mathbb{N}_{m+n}$ defined by

$$h(x) = \begin{cases} f(x), & \text{if } x \in A, \\ g(x) + m, & \text{if } x \in B. \end{cases}$$

where $f\colon A \to \mathbb{N}_m$ and $g\colon B \to \mathbb{N}_n$ are bijections. What happens if A or B is empty?]

(b) Prove that if A and B are any two finite sets (not necessarily disjoint), then $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$, and these three sets are pairwise disjoint.

(c) Prove part (b) of Theorem 3. [Hint: Exercise 10 on page 253 might come in handy.]

2. Given natural numbers m and n, define a function $f\colon \mathbb{N}_m \times \mathbb{N}_n \to \mathbb{N}_{mn}$ by $f(i, j) = (i-1)n + j$. Prove that f is bijective. [Hint: The Division Theorem might come in handy. You might have to handle numbers in $\mathbb{N}_{mn}$ that are divisible by n as a separate case.]

3. Prove part (c) of Theorem 3. [Hint: Use Exercise 7(a) on page 460 of the textbook, together with Exercise 2 above.]