CS 173 Lecture 12: Functions (II)

José Meseguer

University of Illinois at Urbana-Champaign

1 The Surjective Function Theorem

For A and B finite sets, the Pigeonhole Principle Theorem gave us the condition $|A| \leqslant |B|$ in order for an *injective* function $f : A \to B$ to exist. Is there a similar cardinality condition in order for a *sujective* function $f : A \to B$ to exist?

Theorem 1 (Surjective Function Theorem (SFT)). Given finite sets A and B with $B \neq \emptyset$, there exists a surjective function $f : A \to B$ if an only if $|B| \leqslant |A|$.

Proof: To see the ($\Leftarrow$) implication, let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ with no repeated elements and, since $B \neq \emptyset$, $m \geqslant 1$. By hypothesis, $m \leqslant n$. Therefore, the function

$$f = \{(a_1, b_1), \ldots, (a_m, b_m), \ldots, (a_n, b_m)\}$$

is surjective.

To prove the ($\Leftarrow$) implication we prove the contrapositive. That is, we assume $n = |A| < |B|$ and prove that $f : A \to B$ is not surjective. Let $f : A \to B$ be *any* function. It must have the form:

$$f = \{(a_1, b_{i_1}), \ldots, (a_n, b_{i_n})\}$$

for some $b_{i_1}, \ldots, b_{i_n} \in B$. But then $im(f) = \{b_{i_1}, \ldots, b_{i_n}\}$ is a set with n, possibly repeated, elements. Therefore, $|im(f)| \leqslant n < |B|$, and therefore, $im(f) \subset B$. Therefore, $f : A \to B$ is not surjective, as desired. This finishes the proof of the SFT Theorem.

2 Bijective Functions

By definition, a function $f : A \to B$ is called *bijective* if and only if it is injective and surjective. As for injective and surjective functions, we are interested in a characterization of the existence of a bijective function between finite sets in terms of their cardinalities.

Theorem 2 (Bijective Function Theorem (BFT)). Given finite sets A and B there exists a bijective function $f : A \to B$ if an only if $|B| = |A|$.

Proof: We reason by cases. **Case 1**. $B \neq \emptyset$. Then a bijection $f : A \to B$ exists iff (i) $|A| \leqslant |B|$ by the Pigeonhole Principle Theorem, and (ii) $|B| \leqslant |A|$ by the SFT Theorem. That is, iff $|B| = |A|$, as desired.

Case 2. $B = \varnothing$. We need to prove that a bijective function $f : A \to B$ exists iff $0 = |B| = |A|$. That is, iff $A = B = \varnothing$. But if $A \neq \varnothing$, since $B = \varnothing$, there are no functions $f : A \to B$ at all, and *a fortiori* no bijective functions. So we just need to prove that there is a bijective function $f : \varnothing \to \varnothing$. But $\varnothing \times \varnothing = \varnothing$, and therefore $\mathcal{P}(\varnothing \times \varnothing) = \mathcal{P}(\varnothing) = \{\varnothing\}$. But the single relation $\varnothing : \varnothing \rightsquigarrow \varnothing$ is actually the *identity function*

$$\varnothing = id_{\varnothing} = \{(x, y) \in \varnothing \times \varnothing \mid x = y\}$$

which, since there are no elements, is vacuously injective, and is of course surjective, since $im(id_{\varnothing}) = \varnothing$. This finishes the proof of the BFT Theorem.

2.1 The Inverse Relation of a Function

Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4\}$. Consider the function $f : A \to B$ defined by:

$$f = \{(a, 2), (b, 2), (c, 4), (d, 4)\}.$$

Since $f : A \to B$ is a function, it is of course a typed relation, and therefore it has an inverse relation $f^{-1} : A \rightsquigarrow B$. However, we shall see that, unless f is bijective, $f^{-1} : A \rightsquigarrow B$ is *not* a function. In particular, in the above example we have:

$$f^{-1} = \{(2, a), (2, b), (4, c), (4, d)\}$$

which is neither total nor single-valued.

Beware of Nonsense! Speaking or writing nonsense is the easiest thing there is. *Mathematical* nonsense is the easiest kind of nonsense one can speak or write; nonsense that can easily remain *undetected* by the very speaker or writer of it. In particular, *misuse* of mathematical notation can get the notation abuser into a hopeless state of confusion. Some of the best examples of such notation abuse nonsense are expressions like:

$$f^{-1}(x) = y$$

for f a function. It confusedly *assumes* that f^{-1} is a function; but f^{-1} is *not* a function, unless (as we shall see) f is bijective. This is clearly illustrated by the above example. Of course, given a function $f : A \to B$, what one *can* always write without any nonsense for some $b \in B$ is $f^{-1}[b] = A'$, where $A' \subseteq A$ is the set $A' = \{x \in A \mid (x, b) \in f\}$. In the above example we have $f^{-1}[1] = f^{-1}[3] = \varnothing$, $f^{-1}[2] = \{a, b\}$, and $f^{-1}[4] = \{c, d\}$. Mathematics textbook writers are not without blame about sowing confusion in student's minds by writing nonsense notation like $\sqrt{x}$, because $\sqrt{\ }$ is *not* a function at all: it is only the *inverse relation* of the square function $\lambda x \in \mathbb{R}.\ x^2 \in \mathbb{R}$, so that, e.g., $\sqrt{\ }[-3] = \varnothing$, and $\sqrt{\ }[3] = \{+\sqrt{3}, -\sqrt{3}\}$.

The Inverse Relation of an Injective Function.

Theorem 3. A function $f : A \to B$ is injective if and only if $f^{-1} : A \rightsquigarrow B$ is single-valued.

Proof:

- $f : A \to B$ injective $\Leftrightarrow_{def}$ $\forall x, x' \in A(f(x) = f(x') \Rightarrow x = x') \Leftrightarrow$
- (by definition of $f(x)$) $\Leftrightarrow \forall x, x' \in A(\forall y \in B((x, y), (x', y) \in f \Rightarrow x = x'))$ $\Leftrightarrow$
- (by $(x, y) \in f \Leftrightarrow (y, x) \in f^{-1}$) $\Leftrightarrow \forall y \in B(\forall x, x' \in A((y, x), (y, x') \in f^{-1} \Rightarrow x = x'))$ $\Leftrightarrow_{def}$
- $\Leftrightarrow_{def}$ $f^{-1} : A \rightsquigarrow B$ is single-valued.

This finishes the proof of the theorem.

The Inverse Function of a Bijective Function.

Theorem 4. A function $f : A \to B$ is bijective if and only if $f^{-1} : A \rightsquigarrow B$ is a function.

Proof: $f : A \to B$ is bijective iff $f : A \to B$ is injective and surjective iff (by Theorem 3, and Exercise in pg. 5 of Lecture 10 solved in Problem 2-(d) in Discussion of Session 2/23) $f^{-1} : A \rightsquigarrow B$ is single-valued and total iff $f^{-1} : A \rightsquigarrow B$ is a function. This finishes the proof of the theorem.

Corollary 1. A function $f : A \to B$ is not bijective if and only if $f^{-1} : A \rightsquigarrow B$ is not a function.

Lemma 1 . If a function $f : A \to B$ is bijective, then

$$(1)\ \ f^{-1} \circ f = id_A \quad \textit{and} \ \ (2)\ \ f \circ f^{-1} = id_B$$

Proof: To prove (1) we need to show that both functions are equal, i.e., that for each $a \in A$ $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a = id_A(a)$. Let $f(a) = b$. Since $f^{-1} : A \to B$ is a function we then have,

$$f(a) = b \ \Leftrightarrow\ (a, b) \in f \ \Leftrightarrow\ (b, a) \in f^{-1} \ \Leftrightarrow\ f^{-1}(b) = a$$

Therefore, $f^{-1}(f(a)) = f^{-1}(b) = a$, as desired.

The proof of (2) follows immediately from (1). This is because, since $(f^{-1})^{-1} = f$ is a function, by Theorem 4 f^{-1} is bijective, and then, by (1), $f \circ f^{-1} = (f^{-1})^{-1} \circ f^{-1} = id_B$, as desired. This finishes the proof of the theorem.

Beware of Compounded Nonsense! Nonsense, like banking interest, can be compounded. If a function $f : A \to B$ is not bijective, writing things like

$$f^{-1}(f(x)) = x \quad \textit{or} \quad f(f^{-1}(y)) = y$$

is not just nonsense, but *compounded nonsense!* $f^{-1}(f(x)) = x$ makes no sense, since by Corollary 1, f^{-1} is *not* a function. The only thing that could make sense would be to write $f^{-1}[f(x)]$; but $f^{-1}[f(x)]$ does *not* denote an element of A. $f^{-1}[f(x)]$ denotes a *subset* of A. Therefore, even writing $f^{-1}[f(x)] = x$ would be nonsense, since x ranges over *elements* of A, which usually are *not* subsets of A. The case of $f(f^{-1}(y)) = y$ is an even more ludicrous kind of nonsense: since $f^{-1}(y)$ makes no sense, $f(f^{-1}(y)) = y$ makes even less sense: it is a piece of *compounded nonsense!*

2.2 Proving Functions Bijective

How do we *prove* that a function $f : A \to B$ is bijective? The most obvious way is of course to prove that: (i) f is injective, and (ii) f is surjective. This is a perfectly fine way to obtain a proof. But the following alternative method can be quite helpful. We can instead: (i) define a function $g : B \to A$, and (ii) prove that $g \circ f = id_A$ and $f \circ g = id_B$. This second method has the added advantage of giving us an *explicit specification* of f^{-1}, since if g satisfies (ii), then $g = f^{-1}$.

Theorem 5.

1. A function $f : A \to B$ is bijective if and only if there exists a function $g : B \to A$ such that $g \circ f = id_A$ and $f \circ g = id_B$.
2. If, given $f : A \to B$, a function $g : B \to A$ satisfies $g \circ f = id_A$ and $f \circ g = id_B$, then $g = f^{-1}$.

Proof: For (1), the proof of the ($\Rightarrow$) implication is clear because of Lemma 1: we can just choose $g = f^{-1}$. We can prove the ($\Leftarrow$) implication for (1) by assuming that such a g exists and then proving $f : A \to B$ injective and surjective:

Injective. Let $a, a' \in A$ be such that $f(a) = f(a')$ we then have $a = g(f(a)) = g(f(a')) = a'$.

Surjective. We just need to show that $\forall y \in B(\exists x \in A(f(x) = y))$. But since $\forall y \in B(f(g(y)) = y)$, we can just pick $x = f(g(y))$.

To prove (2) we assume that, given $f : A \to B$, the function $g : B \to A$ satisfies $g \circ f = id_A$ and $f \circ g = id_B$ and prove $g = f^{-1}$. But, by (1), $f : A \to B$ is then bijective; and by Lemma 1 this implies that $\forall y \in B(f(f^{-1}(y)) = y)$. Therefore, for each $y \in B$ we have:

$$f^{-1}(y) = g(f(f^{-1}(y))) = g(y)$$

proving that $g = f^{-1} : B \to A$. This finishes the proof of the theorem.

The slides for this lecture contain various examples of bijective functions and their inverses.