**[Enable multiple shares!]**

**[Get 75% of students to turn on cameras]**

Recall that we write "$f\colon A \to B$" to signify that $f$ is a function from $A$ to $B$, that is, a function with domain $A$ and codomain $B$.

(Here " $\to$" does not mean "implies"; it's a different meaning of an arrow.)

Another way to talk about injectivity and surjectivity is to talk about preimages of elements of $Y$, where for a given function $f$ from $X$ to $Y$, and a given element $y \in Y$, the preimage of $y$ under the map $f$ is $\{x \in X: f(x) = y\}$.
Note that this set can be empty, or it can have one element, or it can have many elements.
E.g., for the function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$, the preimage of 1 is $\{+1, -1\}$, the preimage of 0 is $\{0\}$ (not to be confused with 0), and the preimage of $-1$ is the empty set (not to be confused with 0).

$f$ is injective if the preimage of every $y \in Y$ has cardinality at most 1.
$f$ is surjective if the preimage of every $y \in Y$ …
..?..
has cardinality at least 1.
$f$ is bijective if the preimage of every $y \in Y$ …
..?..
has cardinality exactly 1.

If $f$ is a function from $X$ to $Y$, and $y$ and $y'$ are **different** elements of $Y$, then the preimage of $y$ and the preimage of $y'$ are **disjoint** subsets of $X$.
(Proof: If $x$ belongs to the preimage of $y$ and the preimage of $y'$, then $f(x) = y$ and $f(x) = y'$, which contradicts $y \neq y'$.)

Also, every element of $X$ belongs to the preimage of **exactly** one element of $Y$.
(Proof: If $x \in X$ then there is a unique $y \in Y$ satisfying $y = f(x)$ because that's what "function" means.)

So if $X$ and $Y$ are finite, $|X|$ is equal to $\Sigma_y$ |Preimage($y$)|.

Consequently:

If $f: X \to Y$ is injective, $|X| \leq |Y|$.

(Proof: $|X| = \Sigma_y$ |Preimage($y$)| $\leq \Sigma_y 1 = |Y|$.)

If $f: X \to Y$ is surjective, $|X| \geq |Y|$.

(Proof: $|X| = \Sigma_y$ |Preimage($y$)| $\geq \Sigma_y 1 = |Y|$.)

If $f: X \to Y$ is bijective, $|X| = |Y|$.

(Proof: $|X| = \Sigma_y$ |Preimage($y$)| $= \Sigma_y 1 = |Y|$.)

[Refer to "Discrete Mathematics with Ducks" picture.]

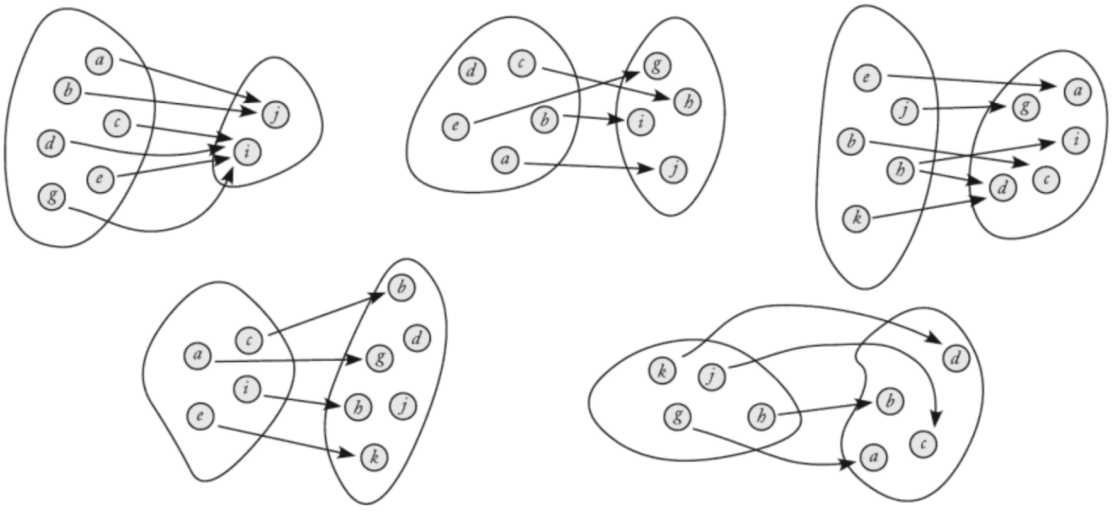

Figure 3.1. Exactly three of these are functions. Which three?

Discuss Pigeonhole Principle

My version of 7.2.11: “Suppose $n$ is a nonnegative integer, $X$ and $Y$ are finite sets and $f$ is a function from $X$ to $Y$. If $|X|$ is greater than $n|Y|$ then there exists some $y$ in $Y$ whose preimage $\{x \text{ in } X: f(x) = y\}$ has cardinality greater than $n$.”

Demonstrate it for $|Y| = 2$, $n = 2$.

Application: We can use the Pigeonhole Principle to show that any subset of {1,2,3,…,100} of size 51 must contain two consecutive integers.

..?..

Write the subset as $a_1, a_2, \ldots, a_{51}$,

let $X = \{1,2,3,\ldots,51\}$, let $Y = \{1,2,3,\ldots,50\}$,

and let $f(x) = \text{floor}(a_n/2)$.

Since $|X| > |Y|$, there must exist two elements $m,n$, in $X$ satisfying $f(m) = f(n)$.

So $\text{floor}(a_m/2) = \text{floor}(a_n/2)$.

But then $a_m$ and $a_n$ are consecutive.

(Can we strengthen the claim to "Any subset of {1,2,3, …,100} of size 50 must contain two consecutive integers"?

..?..

No; the set {2,4,6,…,100} contains 50 elements but contains no consecutive integers.

Where does the proof break down, then?

..?..

The hypothesis $|X| > |Y|$ fails.)

**OMIT?**

If $A$ is finite, then a function $f: A \to A$ is injective iff it is surjective.

[Demonstrate with $|A| = 3$.]

On infinite sets, things can be weird; for instance, the map from $\mathbb{Z}$ to itself that sends $n$ to $2n$ (for all $n$) is injective but not surjective.

Relatedly, let $g$ be the function from $\mathbb{Z}$ to $2\mathbb{Z}$ that sends $n$ to $2n$. (Same map, different codomain.) It's a bijection, even though $2\mathbb{Z}$ is a subset of $\mathbb{Z}$!

Let's get back to finite sets.

**OMIT IN FALL 2021**

Two functions that have different domains are different functions, even if they are given by the same formula.

What about two functions that have the same domain and the same formula but different codomains?

E.g., consider $f: \mathbb{Z} \to \mathbb{Z}$ and $g: \mathbb{Z} \to \mathbb{R}$ given by $f(n) = n^2$ and $g(n) = n^2$. Are they the same function?

For purposes of this class, the answer will be "yes" (because they're the same set of ordered pairs).

But be aware that for certain applications involving "typed data", the answer should be "no".

(Think about subroutines that accept input in a specific data type, like integer or floating point. A subroutine that squares an integer and returns the answer in integer format does not have the same functionality as one that squares an integer and returns it in floating point format!)

**OMIT IN FALL 2021**

Representing a function as a set of ordered pairs has its uses, but if you pursue theoretical CS, it's not the only representation you'll encounter.

In some object-oriented languages, a function comes attached with contextual information, such as what type of input it can accept and what type of output it can produce. In such a setting, one might say that a function is *not* just a set of ordered pairs, because the function also "knows" what its domain and codomain are.

**Section 7.3: Function Composition**

- Know basic terminology: function equality, identity function
- Compute the composition of functions.
- Compute the inverse of a function.
- If $f$ is a function whose inverse $f^{-1}$ exists, then $f \circ f^{-1}$ and $f^{-1} \circ f$ are equal to the appropriate identity functions.

The function $i : A \to A$ satisfying $i(x) = x$ for all $x \in A$ is called the identity function on $A$.

We've learned about relations, composition of relations, and functions (which are special kind of relations).
So now let's think about what happens when you treat two functions as relations and compose them.

[Draw arrow diagram for composition of two functions.]

If $r$, $s$ are associated with functions $f$: $A \to B$ and $g$: $B \to C$, so that $r = \{(x, f(x)) \mid x \in A\}$ and $s = \{(y, g(y)) \mid y \in B\}$, then it can be shown that $rs = \{(x, h(x) \mid x \in A\}$ where the function $h$ satisfies $h(x) = g(f(x))$ for all $x \in A$.
We write $h$ as $g \circ f$ (NOT as $f \circ g$); make sure you don't trip on this notational convention. When you apply $g \circ f$ to $x$, you first apply $f$ to $x$ and then apply $g$ to the result.

“We apply functions in a composition of functions from right to left.”

But:

“We apply relations in a composition of relations from left to right.”

Sorry!

Wait: does order matter when you’re composing functions?

Unfortunately, yes!

Example: Let $f, g: \mathbb{R} \to \mathbb{R}$ be given by $f(x) = 2x$, $g(x) = x+1$.

$(f \circ g)(x) = f(g(x)) = f(x+1) = 2(x+1) = 2x + 2$

$(g \circ f)(x) = g(f(x)) = g(2x) = 2x+1 \neq 2x + 2$

So $f \circ g$ and $g \circ f$ are not equal as functions.

Suppose $f$, $g$, and $h$ are functions, with $h(x) = g(f(x))$.

Let $r_f$, $r_g$, and $r_h$ be the relations associated with $f$, $g$, and $h$, so $r_f = \{(x,y): y=f(x)\}$, $r_g = \{(y,z): z=g(y)\}$, $r_h = \{(x,z): z=h(x)\}$, and let $M_f$, $M_g$, $M_h$ be the associated Boolean matrices. Then $h = g \circ f$ but $r_h = r_f\, r_g$ and $M_h = M_f\, M_g$.

If $f$: $A \to B$ and $g$: $B \to C$ are injective , then $g \circ f$ is too.

If $f$: $A \to B$ and $g$: $B \to C$ are surjective , then $g \circ f$ is too.

If $f$: $A \to B$ and $g$: $B \to C$ are bijective , then $g \circ f$ is too.

When the function $f$: $A \to B$ is bijective, we can define a function from $B$ to $A$ called the inverse function of $f$, written $f^{-1}$.

Example: If $A = \{1,2,3\}$ and $B = \{a,b,c\}$ and $f$ is the function from $A$ to $B$ with $f(1) = c$, $f(2) = b$, and $f(3) = a$, then $f^{-1}$ is the function from $B$ to $A$ with $f^{-1}(a) = 3$, $f^{-1}(b) = 2$, and $f^{-1}(c) = 1$.

In ordered-pairs form, $f = \{(1,c),(2,b),(3,a)\}$ and $f^{-1} = \{(a,3),(b,2),(c,1)\}$.

We have $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

(Let's prove the second one. Given $y$ in $Y$, let $x = f^{-1}(y)$ (so that we also have $y = f(x)$). Then $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = i_B(y)$. Since $(f \circ f^{-1})(y) = i_B(y)$ for all $y$, the functions $f \circ f^{-1}$ and $i_B$ are equal, as claimed.

When the Boolean matrix associated with $f$ is $M$, the Boolean matrix associated with $f^{-1}$ is $M^{-1}$.

Confusingly, the symbol "$f^{-1}$" has a (different) standard meaning in the case where $f$ is *not* bijective.
Specifically, $f^{-1}$ denotes a map from $B$ to the *power set* of $A$, where $f^{-1}(b) = \{a \in A: f(a) = b\}$ (which we earlier wrote as Preimage($b$)).

Example: If $f$ is the function whose domain and codomain are the real numbers, given by the formula $f(x) = x^2$ for all $x$, then

$f^{-1}(4) = \{2, -2\}$,

$f^{-1}(0) = \{0\}$, and

$f^{-1}(-1) = \{\}$ (the empty set).

Discuss: Exercise 7.3.12:

Let $f$ and $g$ be functions whose inverses exist. Prove that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

..?..

[Draw arrow-diagram.]

The fact that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ reflects the way the Boolean matrices of $f$ and $g$ act: $(MN)^{-1} = N^{-1} M^{-1}$.

A bijection from a finite set to itself is called a permutation (Definition 7.3.15). Note that this clashes with their earlier definition of the word “permutation”.

Group work: 7.3.3(a) (6 minutes)

Let $A = \{1, 2, 3\}$.

(a) List all permutations of $A$.

(Use the representation of a permutation as a list of ordered pairs; e.g, the identity function $i_A$ would be written as {(1,1),(2,2),(3,3)}.

..?..

{(1,1),(2,2),(3,3)}, {(1,1),(2,3),(3,2)},
{(1,2),(2,1),(3,3)}, {(1,2),(2,3),(3,1)},
{(1,3),(2,1),(3,2)}, and {(1,3),(2,2),(3,1)}.

[Introduce two-line notation]

Group work (6 minutes):

With $A = \{1,2,3\}$ as above,
let $f$ be the permutation $\{(1,2),(2,1),(3,3)\}$
and let $g$ be the permutation $\{(1,1),(2,3),(3,2)\}$.
Compute $f \circ g$ and $g \circ f$. Are they equal?

..?..

$(f \circ g)(1) = f(g(1)) = f(1) = 2$

$(f \circ g)(2) = f(g(2)) = f(3) = 3$

$(f \circ g)(3) = f(g(3)) = f(2) = 1$

so $f \circ g = \{(1,2),(2,3),(3,1)\}$.

$(g \circ f)(1) = g(f(1)) = g(2) = 3$

$(g \circ f)(2) = g(f(2)) = g(1) = 1$

$(g \circ f)(3) = g(f(3)) = g(3) = 2$

so $g \circ f = \{(1,3),(2,1),(3,2)\} \neq f \circ g$.

## Discussion: 7.3.3(c)

(c) Show that the composition of any two permutations of $A$ is a permutation of $A$.

..?..

Hint: Remember Exercise 7.3.12?

..?..

If $f$ and $g$ are permutations of $A$, they are bijections, so $f \circ g$ is a bijection from $A$ to itself, so it too is a permutation of $A$.

Group work: 7.3.3(d) (6 minutes)

(d) Prove that if $A$ is any set where $|A| = n$, then the number of permutations of $A$ is $n!$.

..?..

To pick a bijection $f$ from $A = \{a_1, a_2, a_3, \ldots, a_n\}$ to itself, we can first pick $f(a_1)$ to be any of the $n$ elements of $A$, then we can pick $f(a_2)$ to be any of the $n–1$ remaining elements of $A$ (different from $f(a_1)$), then we can pick $f(a_3)$ to be any of the $n–2$ remaining elements of $A$ (different from $f(a_1)$ and $f(a_2)$), etc., so by the Law of Products, there are exactly

$$n \times (n–1) \times (n–2) \times \ldots \times 3 \times 2 \times 1 = n!$$

bijections from $A$ to itself.

Questions on section 7.3?