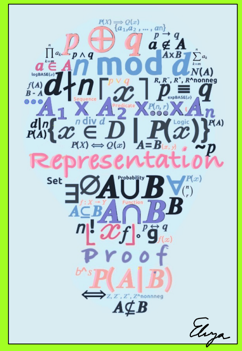
Discrete Structures



Lecture 16: Proofs about functions

Susan L. Epstein

HUNTER

1

Last time

★ **Functions are ubiquitous and powerful**

- Functions can be defined on more than numbers
- Special properties of functions impact computation and storage

Fall 2023 CSCI 150 2/26

2

Today's outline

- Composition of functions
- Cardinality and its properties
- Infinite sets

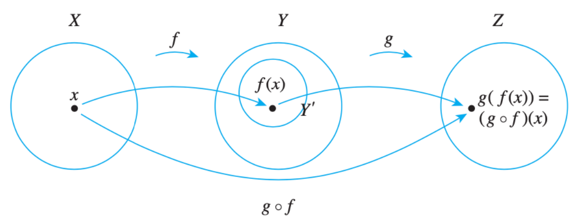
Simple examples yield intuition for hypotheses

3

Composition

For functions $f: X \to Y$ and $g: Y' \to Z$ where the range of f is $Y' \subseteq Y$, $(g \circ f)(x) = g(f(x))$ for all $x \in X$ is the composition of g and f

Read "g circle f" or "g composed with f" or "g of f"



4

2 ways to define a composition

By formula:

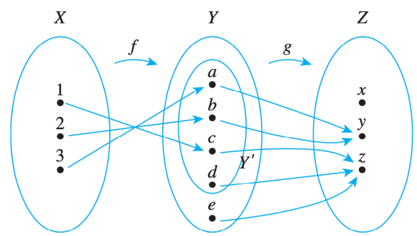
For $f: \boldsymbol{Z} \to \boldsymbol{Z}$ with rule $f(n) = n + 3$ and $g: \boldsymbol{Z} \to \boldsymbol{Z}$ with rule $g(n) = n^2$,

$(g \circ f)(n) = g(f(n)) = g(n+3) = (n+3)^2\ \forall n \in \boldsymbol{Z}$

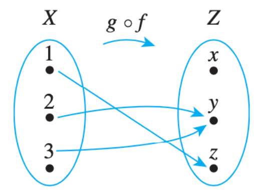
$(f \circ g)(n) = f(g(n)) = g(n^2) = n^2 + 3\ \forall n \in \boldsymbol{Z}$

Note that $(g \circ f)(n) \neq (f \circ g)(n)$

By arrow diagram:



What about $f \circ g$??



Composition with the identity function

Theorem: For function $f: X \to Y$ and identity functions $I_X: X \to X$ and $I_Y: Y \to Y$, $f \circ I_X = f$ and $I_Y \circ f = f$.

Proof:

We must show that for any $x \in X$, $(f \circ I_X)(x) = f(x)$ and $(I_Y \circ f)(y) = y$.
Let x be any element of X.
By definition of composition and identity functions,

$$(f \circ I_X)(x) = f(I_X(x)) = f(x)$$

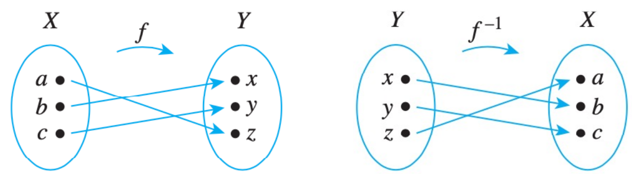
and similarly

$$(I_Y \circ f)(y) = I_Y(f(y)) = f(y).$$

QED

Intuition on inverses of functions

Recall: If $f: X \to Y$, $f^{-1}: Y \to X$ such that $f^{-1}(y) = x$ iff $f(x) = y$



So what do $f \circ f^{-1:}$ and $f^{-1:} \circ f$ look like?

$f \circ f^{-1:} = I_Y$

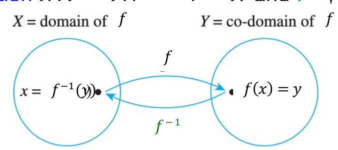
$f^{-1:} \circ f = I_X$

Fall 2023 CSCI 150 7/26

7

Composition with the inverse of a function

Theorem: For one-to-one and onto function $f: X \to Y$ with inverse $f^{-1:}: Y \to X$ and identity function $I_Y: Y \to Y$. $f^{-1:} \circ f = I_Y$ and $f \circ f^{-1:} = I_X$.



Proof:

We must show that for any $x \in X, (f^{-1:} \circ f)(x) = I_X(x)$ and for any $y \in Y$, $(f \circ f^{-1:})(y) = I_Y(y)$.

Let x be any element of X such that $f(x) = y$ where $y \in Y$.

By definition of inverse, $f^{-1:}(y) = x$.

By definition of composition, $(f^{-1:} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_X(x)$ by definition of the identity.

Let y be any element of Y such that $f^{-1:}(y) = x$ where $x \in X$.

By definition of inverse, $f^{-1:}(y) = x$. By definition of composition, $(f \circ f^{-1:})(y) = f(f^{-1}(y)) = f(x) = y = I_Y(y)$ by definition of the identity.

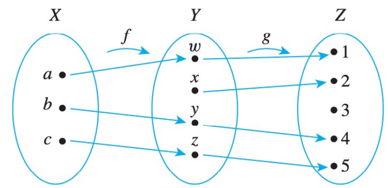
QED

Fall 2023 CSCI 150 8/26

8

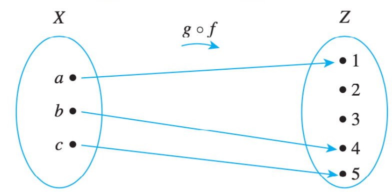
Intuition about one-to-one functions

Recall: $f: X \to Y$ is one-to-one iff $\forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$



So is $g \circ f$ one-to-one?

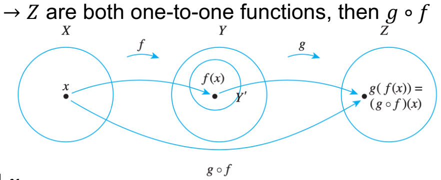
And what about $f \circ g$?



9

Composition of one-to-one functions

Theorem: If $f: X \to Y$ and $g: Y \to Z$ are both one-to-one functions, then $g \circ f$ is also a one-to-one function.



Proof:

We must show that for $g \circ f: X \to Z$. all elements in X have different images in Z.

Assume not, that is, let x_1 and x_2 be distinct elements of X such that $(g \circ f)(x_1)$=$(g \circ f)(x_2)$.

We will show that this assumption logically leads to a contradiction.

By definition of composition, $(g \circ f)(x)$ so $(g(f(x_1)) = g(f(x_2))$.

Because g is one-to-one, $f(x_1) = f(x_2)$

and because f is one-to-one $x_1 = x_2$.

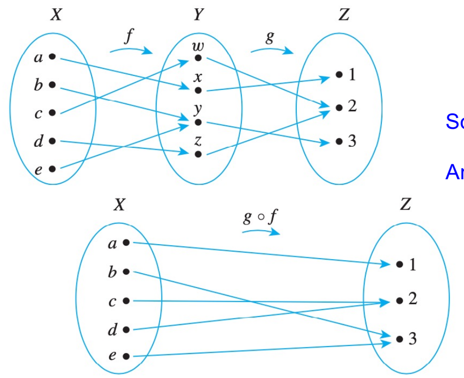
Contradiction. Because the assumption led to a contradiction, $g \circ f$ is also one-to-one.

QED

10

Intuition about onto functions

Recall: $f: X \to Y$ is onto iff $\forall \in Y\ \exists x \in X$ such that $f(x) = y$



So is $g \circ f$ onto?

And what about $f \circ g$?

Composition of onto functions

Theorem: If $f: X \to Y$ and $g: Y \to Z$ are both onto functions then $g \circ f$ is also an onto function.

oth onto functions then $g \circ f$ is also an
nto function.
Proof:
We must show that under $g \circ f: X \to Z$
very element in Z is the image of some element in X.
et z be any element in Z.
By definition of onto, there is some $y \in Y$ such that $g(y) = z$.
By definition of onto, there is some $x \in X$ such that $f(x) = y$.
By definition of composition, $(g \circ f)(x) = g(f(x))$, and by substitution
$g \circ f)(x) = g(f(x)) = g(y) = z$
QED

Proof:

We must show that under $g \circ f: X \to Z$ every element in Z is the image of some element in X.

Let z be any element in Z.

By definition of onto, there is some $y \in Y$ such that $g(y) = z$.
By definition of onto, there is some $x \in X$ such that $f(x) = y$.
By definition of composition, $(g \circ f)(x) = g(f(x))$, and by substitution
$(g \circ f)(x) = g(f(x)) = g(y) = z$

QED

Any questions?

Today's outline

- ✓ Composition of functions
- Cardinality and its properties
- Infinite sets

Definitions

- A set is finite iff it is empty or can be put in one-to-one correspondence with a set of the form $\{1,2,\dots,n\}$
- An infinite set is a non-empty set that cannot be put in one-to-one correspondence with a set of the form $\{1,2,\dots,n\}$
- Any sets A and B have the same cardinality $|A| = |B|$ iff there is a function from A to B that is one-to-one and onto
- An equivalence relation $\mathcal{R}(x,y)$ is a binary relation that is reflexive, symmetric, and transitive on its domain
  - $\mathcal{R}$ is reflexive on a set S iff $\forall s \in S\ (s,s) \in \mathcal{R}$ ≤ on $\boldsymbol{N}$
  - $\mathcal{R}$ is symmetric on a set S iff $\forall s,t \in S, (s,t) \in \mathcal{R}, (t,s) \in \mathcal{R}$ = on $\boldsymbol{Z}$
  - $\mathcal{R}$ is transitive on a set S iff $\forall s,t,u \in S, (s,t),(t,u) \in \mathcal{R}, (s,u) \in \mathcal{R}$ > on $\boldsymbol{R}$

Cardinality is reflexive

Binary relation $\mathcal{R}$ is reflexive on a set S iff $\forall s \in S\ (s, s) \in \mathcal{R}$ ≤ on $\boldsymbol{N}$

Theorem: For any set A, cardinality is reflexive, that is, $|A| = |A|$.

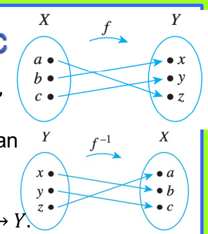
Proof: We must show that there is a one-to-one onto function from A to A.
Let x, y be any elements of A and consider the identity function $I_A\colon A \to A$.
By definition of an identity function, $I_A(x) = x$ and $I_A(y) = y$.
If $I_A(x) = I_A(y)$, by substitution $x = y$, so I_A is one-to-one.
Let y be any element of A.
Because $I_A(y) = y$, so I_A is onto.

Thus I_A is a one-to-one onto function from A to A, and $|A| = |A|$.
QED

Fall 2023 CSCI 150 15/26

15

Cardinality is symmetric



Binary relation $\mathcal{R}$ is symmetric on a set S $\forall s, t \in S, (s, t) \in \mathcal{R}$, iff $(t, s) \in \mathcal{R}$ = on $\boldsymbol{Z}$
Lemma: Any one-to-one onto function between 2 sets has an inverse.
Proof:
Let X and Y be any sets with 1−to−1 correspondence $f\colon X \to Y$.
Define $f^{-1}\colon Y \to X$ as $f^{-1}(y) = x$ iff $f(x) = y$.
$f^{-1}$is a function because f is onto.
Because f is one-to-one, x is unique, and f^{-1} is f's inverse. **QED**
Theorem 15-22 (lecture 15, slide 22): For sets X and Y the inverse of any one-to-one correspondence is also a one-to-one correspondence.
Theorem: For any set A, cardinality is symmetric, that is, if $|A| = |B|$ then $|B| = |A|$.
Proof: We must show that there is a one-to-one correspondence from B to A.
By definition of equal cardinality, ∃ a one-to-one onto function f from A to B.
By the lemma, f^{-1}, the inverse of f, exists. By Theorem 15-22 f^{-1} is also one-to-one and onto. Thus f^{-1} is the desired function.
QED

Fall 2023 CSCI 150 16/26

16

Cardinality is transitive

$\mathcal{R}$ is transitive on a set S iff $\forall s, t, u \in S, (s,t),(t,u) \in \mathcal{R}, (s,u) \in \mathcal{R}$

Theorem 15-22 (lecture 15, slide 22): For sets X and Y the inverse of any one-to-one correspondence is also a one-to-one correspondence.

Theorem: For any sets A, B, C, cardinality is transitive, that is, if $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$.

Proof: We must show that there is a one-to-one correspondence from A to C.

By definition of equal cardinality, there is a one-to-one onto function f from A to B and a one-to-one onto function g from B to C.

Because (slide 10) the composition of two one-to-one functions is one-to-one, $g \circ f$ is one-to-one.

Because (slide 12) the composition of two onto functions is onto, $g \circ f$ is onto.

Thus $g \circ f$ is both onto and one-to-one and is the desired function.

QED

Hence cardinality is an equivalence relation

Fall 2023 CSCI 150 17/26

17

Today's outline

- ✓ Composition of functions
- ✓ Cardinality and its properties
- Infinite sets

Fall 2023 CSCI 150 18/26

18

Brace yourselves…

An infinite set and its proper subset can have the same cardinality

Consider $\boldsymbol{Z}$ and its proper subset $\boldsymbol{Z}^{even} = \{0,2,4, \ldots\}$.
Define the function $f: \boldsymbol{Z} \to \boldsymbol{Z}^{even}$ by the rule $f(n) = 2n$.

$$\begin{array}{ccccc} \ldots -4, & -2, & 0, & 2, & 4, \ldots \\ \downarrow & \downarrow, & \downarrow & \downarrow & \downarrow \\ \ldots -2, & -1, & 0, & 1, & 2, \ldots \end{array}$$

Let $a, b \in \boldsymbol{Z}$ such that $f(a) = f(b)$. Then $2a = 2b$, so $a = b$ and f is one-to-one.
Let c be any element of $\boldsymbol{Z}^{even}$.
Then c is even and by definition of even, $c = 2m$ for some $m \in N$, so $f(m) = c$ and f is onto.
Thus f establishes a one-to-one correspondence between $\boldsymbol{N}$ and its proper subset $\boldsymbol{Z}^{even}$ and $|\boldsymbol{Z}| = |\boldsymbol{Z}^{even}|$

But just because 2 sets are both infinite does not mean that they have the same cardinality…you have to **find the function that is a one-to-one correspondence** between them.

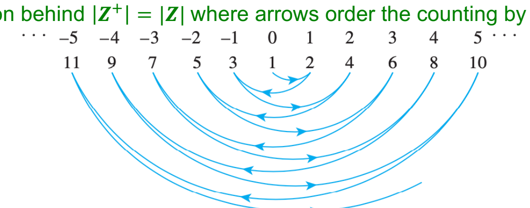
Fall 2023 CSCI 150 19/26

19

Countability

- The paradigm for countability is the positive integers $\boldsymbol{Z}^+$
- A set is said to be countably infinite iff it has the same cardinality as $\boldsymbol{Z}^+$
- A set is said to be countable iff it is finite or countably infinite

Intuition behind $|\boldsymbol{Z}^+| = |\boldsymbol{Z}|$ where arrows order the counting by $\boldsymbol{Z}^+$



For $n \in \boldsymbol{Z}, \boldsymbol{f}: \boldsymbol{Z} \to \boldsymbol{Z}^+$ $\quad f(n) = \begin{cases} 2n \text{ if } n \in \boldsymbol{Z}^+ \\ 2n+1 \text{ otherwise} \end{cases}$

Fall 2023 CSCI 150 20/26

20

Many sets are countably infinite

- $|\boldsymbol{N}| = |\boldsymbol{N}^{even}|$ even though $\boldsymbol{N}^{even} \subset \boldsymbol{N}$
- $|\boldsymbol{N}| = |\boldsymbol{N}^{odd}|$
- $|\boldsymbol{N}| = |\boldsymbol{Z}|$ even though $\boldsymbol{N} \subset \boldsymbol{Z}$
- Let $A = \{x|x \in Z$ and x mod $3 = 0\}$. $|A| = |\boldsymbol{Z}|$
- Let $B = \{x|x \in Z$ and x mod $1000 = 0$. $|A| = |\boldsymbol{Z}|$
- $|A| = |B|$

Cardinality equivalence proof always finds a function that is a one-to-one correspondence between two sets

Can you think of a set with cardinality larger than Z^+?

Fall 2023 CSCI 150 21/26

21

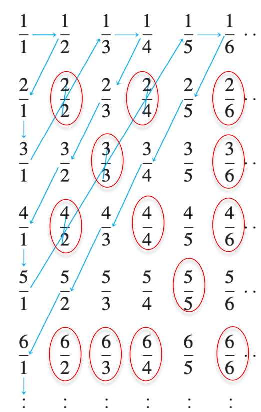
$\boldsymbol{Q}$ is countable

This diagram describes a one-to-one onto function that maps $\boldsymbol{Z}^+ \rightarrow \boldsymbol{Q}^+$ so $|\boldsymbol{Q}^+| = |\boldsymbol{Z}^+|$ Follow the arrows and skip over any equivalent fractions that have already been assigned.

But $|\boldsymbol{Z}^+| = |\boldsymbol{Z}|$, so $|\boldsymbol{Q}^+| = |\boldsymbol{Z}|$

What about $|\boldsymbol{Q}|$?
Not surprisingly, $|\boldsymbol{Q}| = |\boldsymbol{Q}^+|$

Are there **un**countably infinite sets ?



Fall 2023 CSCI 150 22/26

22

Cardinalities and infinite sets

- Any subset of a countable set is countable
- 1874 Georg Cantor proved that $\boldsymbol{R}$ is uncountably infinite
- Other uncountably infinite sets
  - Number of real numbers within any interval of the real number line
  - Any set with an uncountable subset
- Cardinalities of infinite sets have assigned symbols

  $|\boldsymbol{N}| = \aleph_0$ read as "aleph null"

  $|\boldsymbol{R}| = \aleph_1$ read as "aleph one"

  $\aleph_0 < \aleph_1$
- For any set S, $|S| < |\mathcal{P}(S)|$ even if $S = \emptyset$?
- Thus $|\boldsymbol{Z}| < |\mathcal{P}|\boldsymbol{Z}|| < |\mathcal{P}(\mathcal{P}(|\boldsymbol{Z}|))| < \left|\mathcal{P}\left(\mathcal{P}(\mathcal{P}(|\boldsymbol{Z}|))\right)\right| < \cdots$
- This leads to infinitely many symbols for infinite cardinality

  $\aleph_0 < \aleph_1 < \aleph_2 < \ldots$

23

Applications

- The set of all strings on a finite alphabet is countable (Hint: put them in alphabetical order)
- The set of all computer programs in a given programming language is countable (because they are just strings on a finite alphabet)
- The set of all functions from $\boldsymbol{N}^+$ to $\{0,1,2,3,4,5,6,7,8,9\}$ is uncountable (proof in your text)
- Together these indicate that

There are non-computable functions

24

Proof methods (so far)

Truth table
Sequence of statements with reasons
Logic (modus ponens, modus tollens,…)
Predicate logic (quantification, vacuous truth)
Generalization from the generic particular
Proof by contradiction
Proof by contraposition
Proof by cases
Mathematical induction
Strong mathematical induction
Proof by set element
Algebraic set proof
Algebraic proof by properties of functions
Cardinality proof by one-to-one correspondence

Fall 2023 CSCI 150 25/24

25

What you should know

★ **Simple examples yield intuition for hypotheses**

- How compositionality works
- How to build proofs with one-to-one functions, onto functions, and one-to-one correspondences
- What cardinality is
- How to measure the size of infinite sets


Any questions?

Next up: *Counting and probability*

Time to finish up that Opening sheet!

Problem set 15,16 is due on Monday, November 6 at 11PM

Fall 2023 CSCI 150 26/26

26