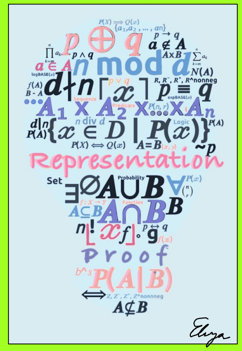
Discrete Structures



Lecture 15: Functions

Susan L. Epstein

HUNTER

1

Last time

★ **Set theory proofs rely on definitions**

- Set theory properties are analogous to those of CSCI 150 formal logic
- Set theory proofs are either element proofs that rely on definitions, or algebraic proofs that rely on set theory laws
- A Boolean algebra has identities and complements for 2 operations that are associative, commutative, and distributive

propositional logic set theory

Fall 2023 CSCI 150 2/25

2

Today's outline

- Broader function definitions
- Properties of functions

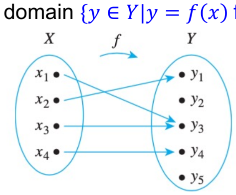
Functions are ubiquitous and powerful

3

Basic ideas

- Binary relation R from set X to set Y is **any** subset of their Cartesian product $X \times Y$
  If $X = \{1,23\}, Y = \{4,20\}, X \times Y = \{(1,4), (1,20), (23,4), (23,20)\}$
- Binary function f from set X to set Y is a relation with domain X and co-domain $Y \ni$ for every $x \in X$ there is **exactly one** $y \in Y$ so $(x, y) \in f$
  - Notation: $f: X \rightarrow Y$
  - If $(x, y) \in f$ and also $(x, z) \in f$ then $y = z$
  - If $(x, y) \in f$, then y is written $f(x)$ and read "f of x" or "the value of f at x" or "the image of x under f" $\quad f(x_1) = y_3$
  - If $(x, y) \in f$, the inverse image of y is $f^{-1}(y) = \{x \in X | f(x) = y\}$
- Range of f (aka image of X under f) = all elements in its co-domain that are images of some element in its domain $\{y \in Y | y = f(x)$ for some $x \in X\}$

domain? $\{x_1, x_2, x_3, x_4\}$
co-domain? $\{y_1, y_2, y_3, y_4, y_5,\}$
range? $\{y_1, y_3, y_4\}$



4

Functions you already know

- Sequence: subset of $\boldsymbol{N} \times \boldsymbol{R}$
  domain: $\{ i \in \boldsymbol{N}, i \geq 2\}$ range: $\left\{\frac{i}{i+1} | i \geq 2\right\}$ $f = \{(2, \frac{2}{3}), (3, \frac{3}{4}), (4, \frac{4}{5}), \ldots\}$
- Truth tables: {value tuples for propositional logic symbols} × {T,F})
  domain: $\{T, F\} \times \{T, F\}$ range: $\{T, F\}$
  $f = \{((T,T),T), ((T,F),F), ((F,T),F), ((F,F),F)\}$
  $g = \{((T,T),T), ((T,F),T), ((F,T),T), ((F,F),F)\}$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

- Input/output tables: defined on black boxes

- mod and div: subsets of $\boldsymbol{Z} \times \boldsymbol{Z}$
  domain: $\boldsymbol{Z}$ range: $\{0,1,2\}$ $f = \{\ldots, (0,0)(1,1), (2,2), (3,0), (4,1), (5,2), \ldots\}$
  domain: $\boldsymbol{Z}$ range: $\boldsymbol{Z}$ $g = \{\ldots, (0,0), (1,0), (2,1), (3,1), (4,2), (5,2) \ldots\}$
- Floor and ceiling: subsets of $\boldsymbol{R} \times \boldsymbol{Z}$
  domain: $\boldsymbol{R}$ range: $\boldsymbol{Z}$ $f = \{(a,b) | a \in \boldsymbol{R}$, largest integer $b \leq a\}$
  domain: $\boldsymbol{R}$ range: $\boldsymbol{Z}$ $f = \{(a,b) | a \in \boldsymbol{R}$, smallest integer $b \geq a\}$

Fall 2023 CSCI 150 5/25

5

Equality of functions

Theorem: If $f: X \to Y$ and $g: X \to Y$ are functions, $f = g$ iff $f(x) = g(x)$ for all $x \in X$.
Proof: We must show that $f = g$.
By definition of function, both f and g are subsets of $X \times Y$.
Part 1: We must show that $f \subseteq g$.
Let (x, y) be any element of f. Then $f(x) = y$ but since $f(x) = g(x)$ for all $x \in X$, $(x, y) \in g$, and $f \subseteq g$.
Part 2: We must show that $g \subseteq f$.
Let (x, y) be any element of g. Then $g(x) = y$ but since $f(x) = g(x)$ for all $x \in X$, $(x, y) \in f$, and $g \subseteq f$. Thus $f = g$. **QED**
Let $J = \{0, 1, 2\}$, and define functions f and g from J to J as $f(x) = (x^2 + x + 1) \bmod 3$ and $g(x) = (x + 2)^2 \bmod 3$.

x	x^2+x+1	$f(x) = (x^2+x+1)\ mod\ 3$	$(x+2)^2$	$g(x) = (x+2)^2\ mod\ 3$
0	1	$1\ mod\ 3 = 1$	4	$4\ mod\ 3 = 1$
1	3	$3\ mod\ 3 = 0$	9	$9\ mod\ 3 = 0$
2	7	$7\ mod\ 3 = 1$	16	$16\ mod\ 3 = 1$

This proves that $f = g$.

Fall 2023 CSCI 150 6/25

6

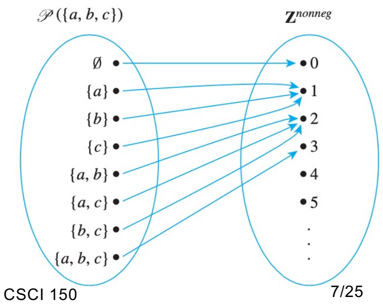
Examples of functions

- Identity function I_X for a set X is $I_X = \{(x, x) | x \in X\}$
  - Simply retains the value of x $\quad I_X(\sqrt[3]{19}) = \sqrt[3]{19}$
- Infinite sequence is a function defined on set of integers $\geq n$

  $1, -\frac{1}{8}, \frac{1}{27}, -\frac{1}{64}, \ldots$ is $f(k) = \frac{(-1)^{k+1}}{k^3}$ $\forall$ integers $k \geq 1$

$f: \mathcal{P}\{a, b, c\} \to \boldsymbol{Z}^{nonneg}$ where f counts the number of elements in a subset has arrow diagram

Here, the domain and range are discrete but the co-domain is infinite



7

Functions on strings

- String over a set of characters S is either the null string of no elements or a nonempty finite sequence of elements of S

  $S = \{a, b, c\}$ $\quad abaaab$ $\quad cbacbcccaaaaa$
- Messages are often transmitted as strings over $\{0,1\}$
- To protect against failure in message transmission, one coding scheme is a function that replaces each boolean character with 3 copies of itself

  10110 is encoded as 111000111111000 which is easy to decode

  If a bit is lost or changed during transmission it can usually be easily detected and corrected
- Hamming distance H between 2 strings of the same length n is a function $S_n \times S_n \to \boldsymbol{Z}^{nonneg}$ the number of positions in which they differ

  For $n = 6, H(001100,111111) = 4$ and $H(001100,000001) = 3$

8

More functions

- For base $b \in \boldsymbol{R}^+, b \neq 1$ and number $r \in \boldsymbol{R}^+$, the logarithm $\log_b r$ with base b of x is $y \in \boldsymbol{R}^+$such that $b^y = x$
  $\log_4 16 = 2$ $\log_2 16 = 4$ $\log_{16} 16 = 1$
  Hint: what power do you have to raise b to to get r?
- Logarithmic function with base $b \neq 1$ is the function from $\boldsymbol{R}^+$ to $\boldsymbol{R}$ that maps x to $\log_b x$
- $\{0,1\}^n$ is the set of all n-tuples of 0's and 1's
- An n-place Boolean function has domain $\{0,1\}^n$ and co-domain $\{0,1\}$

The 3-place Boolean function $f: \{0,1\}^3 \rightarrow \{0,1\}$ defined by $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \bmod 2$ can also be described by this table

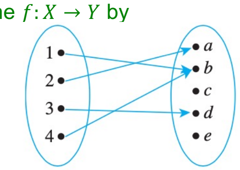
Input			Output
x_1	x_2	x_3	$(x_1 + x_2 + x_3)$ *mod* 2
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

A truth table on n variables is an n-place Boolean function $f: \{0,1\}^2 \rightarrow \{0,1\}$ where T represents 1 and F represents 0

9

Warnings

- Watch the notation: f is a function (a set of ordered pairs) and $f(x)$ is a value
- To be well-defined a function must specify a unique image in its co-domain for every element in its domain
  $f(x): \boldsymbol{R} \rightarrow \boldsymbol{R}$ with rule $x^2 + y^2 = 1$ is a relation not a function because f has no image for $x = 3$
- If $f: X \rightarrow Y$ is a function, $A \subseteq X, B \subseteq Y$, then
  the image of A is $f(A) = \{y \in Y | y = f(x)$ for some $x \in A\}$ and
  the inverse image of B is $f^{-1}(B) = \{x \in X | f(x) \in B\}$
  Let $X = \{1,2,3,4\}$ and $Y = \{a, b, c, d, e\}$, and define $f: X \rightarrow Y$ by
  Let $A = \{1, 4\}, C = \{a, b\}$, and $D = \{c, e\}$.
  What are $f(A), f(X), f^{-1}(C)$, and $f^{-1}(D)$?
  This example shows that even though f is a function f^{-1} may not be a function.



10

Today's outline

- ✓ Broader function definitions
- Properties of functions

You can follow the upcoming proofs, but how to come up with them?

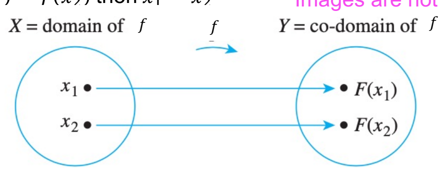
Read the preliminary discussion in your text *before* their proofs

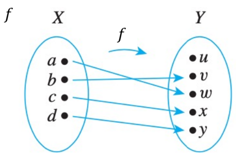
11

One-to-one functions

$f: X \to Y$ is a one-to-one **function** (aka injective) iff $\forall x_1, x_2 \in X$,
if $f(x_1) = f(x_2)$ then $x_1 = x_2$

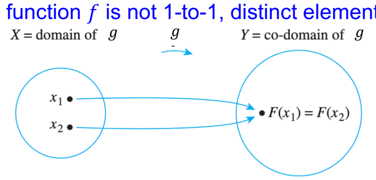
Images are not shared

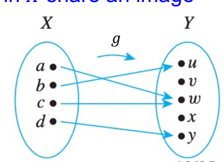




When function f is 1-to-1,distinct elements in X have distinct images in Y

When function f is not 1-to-1, distinct elements in X share an image





12

One-to-one function proofs

- For $f: X \to Y$ with finite X, consider all pairs of distinct elements in X
  - For $|X| = n$ there are $\frac{n(n-1)}{2}$ such pairs
  - Disproof: find a pair that have the same image
  - Proof: show that all pairs have distinct images
- For function $f: X \to Y$ and X is infinite, take 2 arbitrary but distinct elements $x_1, x_2 \in X$ where $x_1 \neq x_2$
  - Proof: We must show that $f(x_1) \neq f(x_2)$.

  If $f: \boldsymbol{R} \to \boldsymbol{R}$ with $f(x) = 3x + 2$, then since multiplication and addition in $\boldsymbol{R}$ preserve inequality and $x_1 \neq x_2$, $3x_1 \neq 3x_2$ and $3x_1+2 \neq 3x_2+2$. Thus $f(x_1) \neq f(x_2)$. **QED**
  - Disproof: find a counterexample (look for particular element(s) in X)

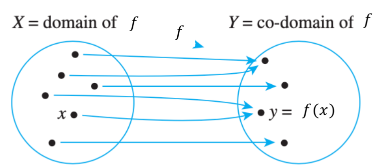
  For $g: \boldsymbol{R} \to \boldsymbol{R}$ with $g(x) = x^4$, consider $1, -1 \in \boldsymbol{R}$.
  Since $g(-1) = 1 = g(1)$, g is not one-to-one

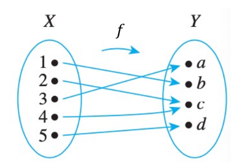
13

Onto functions

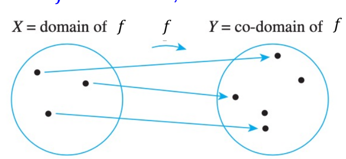
Function $f: X \to Y$ is onto (aka surjective) iff $\forall x_1, x_2 \in X$, if $\forall \in Y\ \exists x \in X$ such that $f(x) = y$ Every co-domain element is an mages

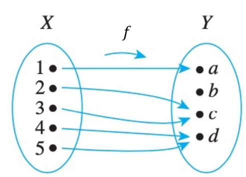
When f is onto, every element in Y is the image of some element in X





When f is not onto, some element in Y is **not** the image of any element in X





14

Onto proofs

- For function $f: X \to Y$ with finite Y, consider all elements in Y
  - How many are there?
  - Disproof: find an element that is not the image of any element in X
  - Proof: show that every element in Y is the image of some $x \in X$
- For function $f: X \to Y$ if Y is infinite, take an arbitrary $y \in Y$
  - Proof: We must show that for some $x \in X, f(x) = y$.

  If $f: \boldsymbol{R} \to \boldsymbol{R}$ with $f(x) = 3x + 2$, then if $y = 3x + 2,\ y - 2 = 3x, x = \frac{y-2}{3}$.

  By substitution $f\left(\frac{y-2}{3}\right) = 3\left(\frac{y-2}{3}\right) + 2 = y - 2 + 2 = y$ and since $\boldsymbol{R}$ is closed under subtraction and under division by a non-zero number, $\frac{y-2}{3} \in \boldsymbol{R}$ and $f\left(\frac{y-2}{3}\right) = y$. QED
  - Disproof: find a counterexample

  For $g: \boldsymbol{Z} \to \boldsymbol{Z}$ with $g(x) = 3x + 2$, consider $4 \in \boldsymbol{R}$. Since $g(x) = 3x + 2$, $4 = 3x + 2$ with solution x= $\frac{4-2}{3} = \frac{2}{3} \notin \boldsymbol{Z}$.

  Thus g is not onto.

15

Application: hashing

- Efficient storage and retrieval for a set S of items with unique identifiers (keys) with maximum value m students' SSNs → CUNY IDs
- Could use an array because its entries can be accessed in constant time but for large m, that is too much space
- Instead, use an array A of size $|S| = n << m$ with entries $a[1], a[2], \ldots a[n]$ and a hash function $h: S \to \{1,2, \ldots, n\}$ that maps from the key for an item in S to an index for an element in A

  $h(s) = (key(s)) \bmod 7$ $h(513408716) = 2$
- But for large $|S|$, h may not be one-to-one, that is, there may be collisions where $x_1 \neq x_2$ but $h(x_1) = h(x_2)$ $h(908371011) = h(513408716) = 2$
- Collision resolution algorithm(s) address this

  "take the next empty location" would store item with key 908371011 in $a[4]$

0	356-63-3102
1	
2	513-40-8716
3	223-79-9061
4	
5	328-34-3419
6	

16

Exponents and logs

- Properties of exponentiation: For all $b, c \in \boldsymbol{R}^{+}$ and all $u.v \in \boldsymbol{R}$

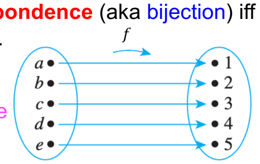
$$b^u b^v = b^{u+v}$$
$$(b^u)^v = b^{uv}$$
$$\frac{b^u}{b^v} = b^{u-v}$$
$$(bc)^u = b^u c^u$$

- For all $b \in \boldsymbol{R}^{+}, b \neq 1$
  - For all $u.v \in \boldsymbol{R}$, if $b^u = b^v$ then $u = v$
  - For all $u.v \in \boldsymbol{R}^{+}$, if $\log_b u = \log_b v$ then $u = v$
  - That is, both the exponential and logarithmic functions are 1-to-1
- For all $b, c, x, y \in \boldsymbol{R}^{+}$, $b \neq 1, c \neq 1$
  - $\log_b(xy) = \log_b x + \log_b y$
  - $\log_b \frac{x}{y} = \log_b x - \log_b y$
  - $\log_b(x^a) = a \log_b x$
  - $\log_c x = \frac{\log_b x}{\log_b c}$

One-to-one correspondences

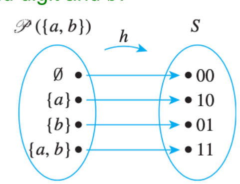
Function $f: X \to Y$ is a one-to-one **correspondence** (aka bijection) iff $\forall x_1, x_2 \in X$, f is both onto and one-to-one.

Images are not shared **and**
Every co-domain element is an image



Consider $h: \mathcal{P}(\{a, b\}) \to \{0,1\}^2$ where the first digit is 1 if a is in the the subset and 0 if it is not, and similarly for the second digit and b.

Subset of $\{a, b\}$	Status of a	Status of b	String in S
$\emptyset$	not in	not in	00
$\{a\}$	in	not in	10
$\{b\}$	not in	in	01
$\{a, b\}$	in	in	11



h is a 1-to-1 correspondence

Functions on 2 variables (1)

$f: A \times B \to C = \{((a,b),c) | (a,b) \in A \times B, c \in C\}$ is a function on 2 variables iff every $(a,b) \in A \times B$ has a unique image $c \in C$

$f(x,y) = (x-y, x+y)$ is a 1-to-1 correspondence from $\boldsymbol{R} \times \boldsymbol{R}$ to itself.

Proof:

Part 1: f is 1-to-1.

Let $(x_1, x_2), (t_1, t_2)$ be any 2 elements in $\boldsymbol{R} \times \boldsymbol{R}$.

We must show that if $f(x_1, x_2) = f(t_1, t_2)$ then $x_1 = t_1$ and $x_2 = t_2$.

By definition of f, $f(x_1, x_2) = (x_1 - x_2, x_1 + x_2)$

$f(t_1, t_2) = (t_1 - t_2, t_1 + t_2)$

If $f(x_1, x_2) = f(t_1, t_2)$ then

$x_1 - x_2 = t_1 - t_2$ and $x_1 + x_2 = t_1 + t_2$

Adding those 2 equations yields $2x_1 = 2t_1$, so $x_1 = t_1$

and by substitution $x_1 - x_2 = x_1 - t_2$ so $x_2 = t_2$.

Thus f is 1-to-1.

But we're not done yet…why not?

Fall 2023 CSCI 150 19/25

19

Functions on 2 variables (2)

$f(x,y) = (x-y, x+y)$ is a 1-to-1 correspondence from $\boldsymbol{R} \times \boldsymbol{R}$ to itself.

Proof:

Part 2: f is onto.

Let (t_1, t_2) be any element of $\boldsymbol{R} \times \boldsymbol{R}$.

We must show that there exists some $(x_1, x_2) \in \boldsymbol{R} \times \boldsymbol{R}$ such that $f(x_1, x_2) = (t_1, t_2)$.

By definition of f, $f(x_1, x_2) = (x_1 - x_2, x_1 + x_2)$ so if $f(x_1, x_2) = (t_1, t_2)$ then

$$x_1 - x_2 = t_1$$
$$x_1 + x_2 = t_2$$

Adding those 2 equations yields $2x_1 = t_1 + t_2$ so let $x_1 = \frac{t_1 + t_2}{2}$.

Since $x_1 - x_2 = t_1$, $x_2 = x_1 - t_1$ and by substitution

$$x_2 = \frac{t_1 + t_2}{2} - t_1 = \frac{-t_1 + t_2}{2}$$

Then, $f\left(\frac{t_1 + t_2}{2}, \frac{-t_1 + t_2}{2}\right) = \left(\frac{t_1 + t_2}{2} - \frac{-t_1 + t_2}{2}, \frac{t_1 + t_2}{2} + \frac{-t_1 + t_2}{2}\right) = \left(\frac{2t_1}{2}, \frac{2t_2}{2}\right) = (t_1, t_2)$, Thus f is onto.

Since f is 1-to-1 and onto, it is a 1-to-1 correspondence.

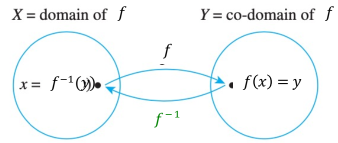
QED

Fall 2023 CSCI 150 20/25

20

Inverse functions

- If $f: X \rightarrow Y$ is a one-to-one correspondence, define its inverse function $f^{-1}: Y \rightarrow X$ with the rule $f^{-1}(y) = x$ iff $f(x) = y$



To find an inverse for $f: \boldsymbol{R} \rightarrow \boldsymbol{R}$ where $f(x) = 13x - 9$, solve $y = 13x - 9$ to get $x = \frac{y+9}{13}$. Then $f^{-1}(y) = \frac{y+9}{13}$

For base $b > 0$ the logarithmic function is the inverse of the exponential function

- Having an inverse is a property of a function
- Many functions are not invertible $\quad f(x) = x^2$

Property of an inverse function

Theorem: For sets X and Y, the inverse $f^{-1}: Y \rightarrow X$ of any 1-to-1 correspondence $f: X \rightarrow Y$ is also a 1-to-1 correspondence.

Proof:

Part 1: We must show that $f^{-1}$is 1-to-1.

Let y_1, y_2 be any 2 elements of Y with $f^{-1}(y_1) = f^{-1}(y_2)$.

By definition of f^{-1}, there is $x \in X$ such that $x = f^{-1}(y_1) = f^{-1}(y_2)$.

Because f is a function, x has a unique image in Y, so $y_1 = y_2$ and $f^{-1}$is 1-to-1.

Part 2: We must show that $f^{-1}$is onto.

Because f is a function, every $x \in X$ has an image $y \in Y$, that is, $f(x) = y$.

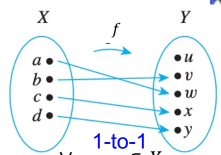
By definition of f^{-1}, $f^{-1}(y) = x$ and f^{-1} is onto.

Because f^{-1} is 1-to-1 and onto, it is a 1-to-1 correspondence.

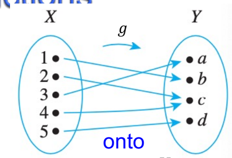
QED

Recall $f: \boldsymbol{R} \times \boldsymbol{R} \rightarrow \boldsymbol{R} \times \boldsymbol{R}$ defined by $f(x, y) = (x - y, x + y)$. f is a 1-to-1 correspondence from $\boldsymbol{R} \times \boldsymbol{R}$ to itself. Therefore its inverse $f^{-1}(x, y) = \left(\frac{x+y}{2}, \frac{-x+y}{2}\right)$ is a 1-to-1 correspondence from $\boldsymbol{R} \times \boldsymbol{R}$ to itself.

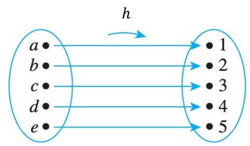
Kinds of functions



1-to-1
$\forall x_1, x_2 \in X$,
if $f(x_1) = f(x_2)$ then $x_1 = x_2$

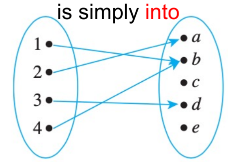


onto
$\forall x_1, x_2 \in X$,
if $\forall \in Y \; \exists x \in X$ such that $g(x) = y$



1-to-1 correspondence
$\forall x_1, x_2 \in X$,
h is both onto and 1-to-1

Anything other function
is simply into



23

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

24

What you should know

⭐ **Functions are ubiquitous and powerful**

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

Next up: *Proofs about functions*

Time to finish up that Opening sheet!

Any questions?

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

25