CSE 20
DISCRETE MATH

Fall 2017

http://cseweb.ucsd.edu/classes/fa17/cse20-ab/

Today's learning goals

- Represent functions in multiple ways
- Define and prove properties of: domain of a function, image of a function, composition of functions
- Determine and prove whether a function is one-to-one, onto, bijective
- Apply the definition and properties of floor function, ceiling function, factorial function
- Define and compute the cardinality of a set: Finite sets, countable sets, uncountable sets
- Use functions to compare the sizes of sets

λ empty string

Also: questions from the review quiz

Basis Step

Recursive Step

Concatenating strings if w is a string then $w \cdot \boxed{\lambda} = w$

and if w_1 and w_2 are both strings, x is 0 or 1 then $w_1 \cdot \boxed{(w_2 x)} = (w_1 \cdot w_2)x$

Length function on strings (Basis) $l(\lambda) = 0$ (Recursive) $l(wx) = l(w) + 1$ when w a string, x 0 or 1

Flavors of induction

$\forall x \; P(x)$

- Mathematical induction
- Strong induction
- $\boxed{\text{Structural induction}}$

Domain

$\{x \in \mathbb{Z} \mid x \geq b\}$

Strong IH: Assume $P(\ldots)$ true at more elements in domain

Domain: rec def set

1, 1, 2, 3, 5, ...

Fibonacci numbers

Rosen p. 158, 347

$$f_0 = 1, \; f_1 = 1, \; \boxed{f_n = f_{n-1} + f_{n-2}}$$

Theorem: For each integer n >= 2, $f_n >= 1.5^{n-2}$

exponential growth!

Proof by strong mathematical induction:

$\boxed{\text{Basis step:}}$

f_2

f_3

(Strong) induction step:

Case <

f_{n-1}

f_{n-2}

Details on slides

Looking back

- We now have all the tools we need to rigorously prove
  - Correctness of **greedy change-making algorithm** with quarters, dimes, nickels, and pennies *Proof by contradiction, Rosen p. 199*
  - The **division algorithm** is correct *Strong induction, Rosen p. 341*
  - **Russian peasant multiplication** is correct *Induction*
  - Largest **n-bit binary** number is 2^n-1 *Induction, Rosen p. 318*
  - Correctness of **base b conversion** (Algorithm 1 of 4.2), *Strong induction*
  - Size of the **power set** of a finite set with n elements is 2^n *Induction, Rosen p. 323*
  - Any int greater than 1 can be written as **product of primes** *Strong induction, Rosen p. 323*
  - There are infinitely many **primes** *Proof by contradiction, Rosen p. 260*
  - **Sum** of geometric progressions $\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}$ when $r \neq 1$, *Induction, Rosen p. 318*

Every number has a binary representation

Theorem: Every $\underbrace{\text{positive integer}}_{}$ $\underbrace{\text{can be written as a sum of distinct powers of 2.}}_{P(k)}$

k

no two terms are equal

Proof by strong mathematical induction:

Basis step: WTS $P(1)$

Note $1 = 2^0$ ← a power of 2

(Strong) induction step: Let k be arb pos int.

Assume (S I H) j can be expressed as sum of distinct powers of 2 for each $1 \le j \le k$.

WTS $k+1$ can be expressed as sum of distinct powers of 2.

Cautionary tales

- The **basis step** is absolutely necessary … and might need more than one!
- Make sure to stay in the **domain**.

Recommended practice

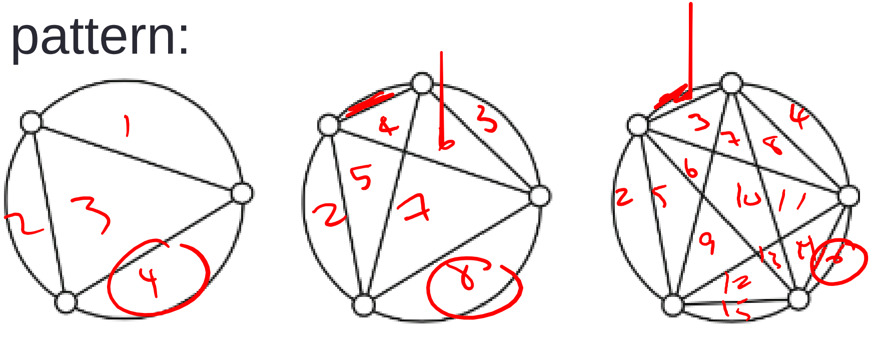
Section 5.1 #49, 50, 51

Section 5.2 #32

- A few **examples** do not guarantee a pattern:

cake cutting conundrum. Join all pairs of points among N marked on circumference of cake.

Conj: 2^N



N=3 N=4 N=5

Where to now?

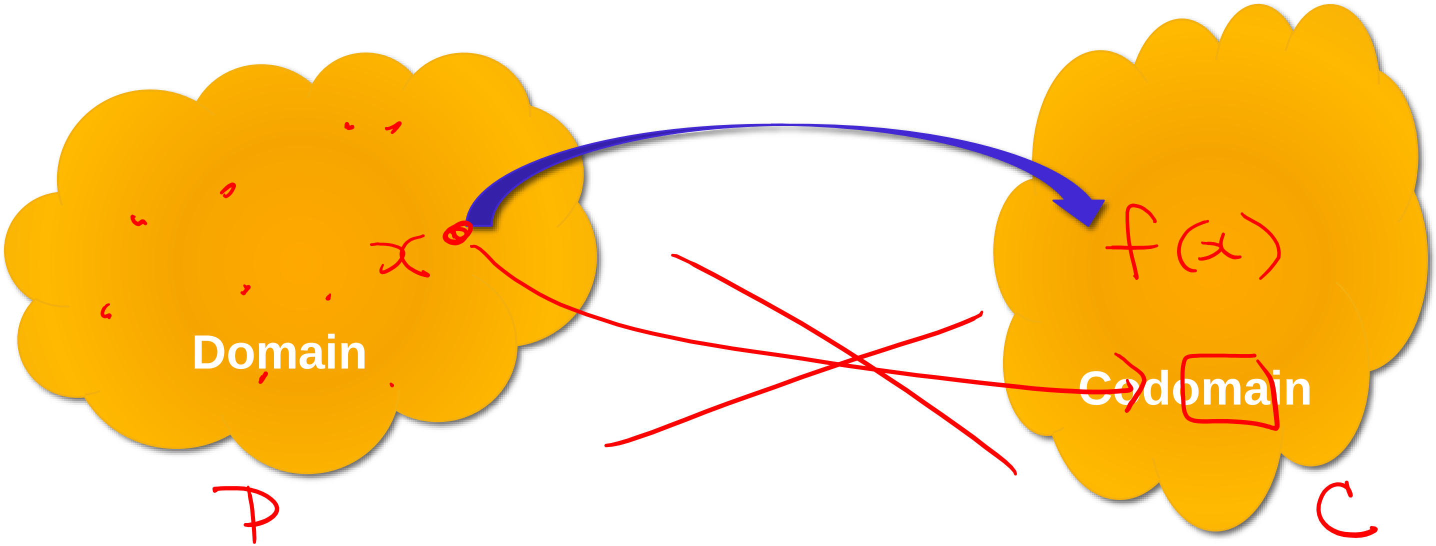
Apply proof strategies to new concepts

- Sizes of sets – what's possible, impossible?
- Number theory – cryptography, hashing, proof by cases

Rec Def of function

Functions

Rosen Sec 2.3; p. 138



Function **Mapping** **Transformation**

$$\boxed{\forall a}(a \in D \rightarrow \exists! b\,(b \in C \wedge f(a) = b))$$

exactly one outgoing arrow from each pt on left

Unique?

also written $\exists^{1} b$

How do we express

$$\forall a(a \in D \to \exists! b\,(b \in C \wedge f(a) = b))$$

with our notation?

$$\exists! x\ P(x) \equiv \exists x\,(P(x) \wedge \forall y\,(y \neq x \to \neg P(y)))$$

↖ $P(\ldots)$ is T about x
and F about everything else in domain

To specify a function

(1) Domain (2) Codomain (3) Assignment

Operations on functions

Rosen p. 141,147

real valued function

If f: A → **R**, g: A → **R** f+g: A → **R** fg: A → **R**

If f: B → C, g: A → B f∘g: A → C

composition

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

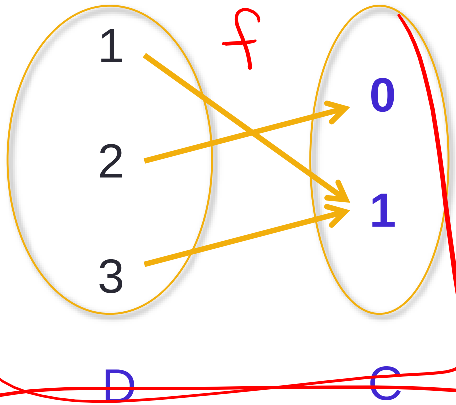
$A \xrightarrow{g} B \xrightarrow{f} C$

Properties of functions

Rosen p. 143

possible

- A function f is **onto** (surjective) means **at least one input for every output**



$$\forall b(b \in C \rightarrow \exists a\,(a \in D \wedge f(a) = b))$$

D	C
1	1
2	0
3	1

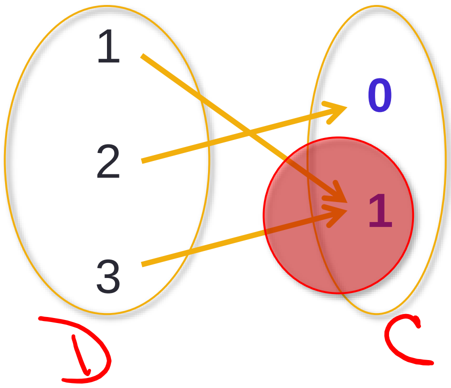
"every elt on right (C) has at least one incoming arrow"

$f(1)=1$, $f(2)=0$, $f(3)=1$

Properties of functions

Rosen p. 141

- A function f is **one-to-one** means no duplicate images (injective)



How can we formalize this?

~~A~~. $\forall a \forall b((a \in D \wedge b \in D) \rightarrow f(a) \neq f(b))$

b/c a=b possible

B. $\forall a \forall b((\underline{a \in D \wedge b \in D}) \rightarrow (\underline{f(a) = f(b)} \rightarrow \underline{a = b}))$

~~C~~. $\forall a \forall b((a \in C \wedge b \in C) \rightarrow a \neq b)$

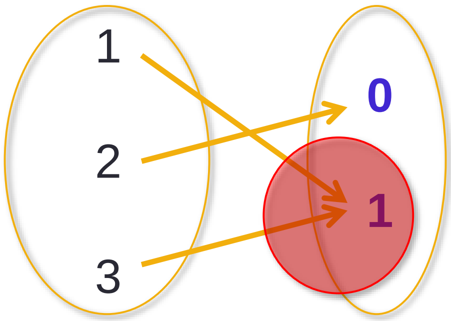
~~D~~. $\forall a \forall b((a \in C \wedge b \in C) \rightarrow f(a) \neq f(b))$

E. None of the above

Properties of functions

Rosen p. 141

- A function f is **one-to-one** means **no duplicate images**
  (injective)



$$\forall a \forall b((a \in D \wedge b \in D) \rightarrow (f(a) = f(b) \rightarrow a = b))$$

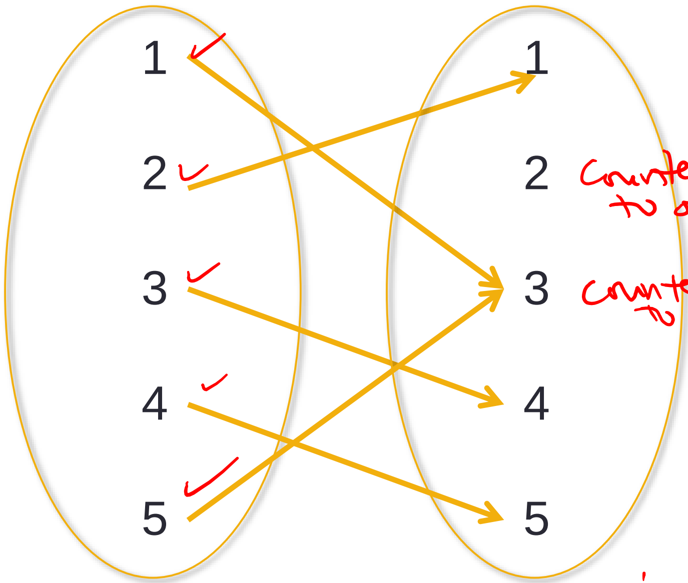
$$\forall a \forall b((a \in D \wedge b \in D) \rightarrow (a \neq b \rightarrow f(a) \neq f(b)))$$

Onto $\forall b\,(b \in C \rightarrow \exists a\,(a \in D \wedge f(a) = b))$

Onto? One-to-one?

1-1 $\forall a\, \forall b\,([a \in D \wedge b \in D] \rightarrow (f(a) = f(b) \rightarrow a = b))$

Consider the function over domain and codomain {1,2,3,4,5} defined by



counter ex to onto

counter ex to 1-1

This function is

A. Well defined, onto, and one-to-one.
B. Well defined, but neither onto nor one-to-one.
C. Well defined, onto, but not one-to-one.
D. Not well-defined, not onto, not one-to-one.
E. None of the above.

ex

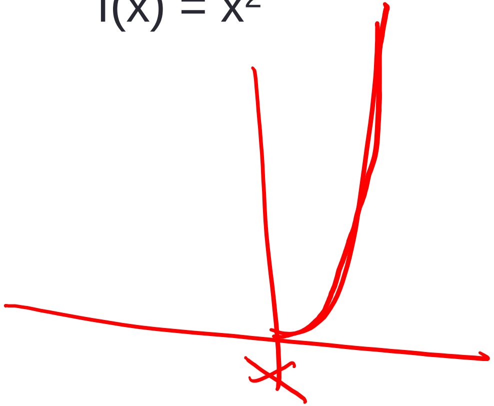
fn 1-1 but not onto? onto but not 1-1?

Onto? One-to-one?

$\mathbb{R}^{\geq 0}$

Consider the function over domain and codomain $\boxed{\mathbf{R}^{\geq 0}}$ defined by

$f(x) = x^2$



This function is

A. Well defined, onto, and one-to-one.
B. Well defined, but neither onto nor one-to-one.
C. Well defined, onto, but not one-to-one.
D. Not well-defined, not onto, not one-to-one.
E. None of the above.

Proving a function is …

Rosen p. 145

Define f:{0,1}* → **N** by f(w) = l(w) = |w|. *Recall: recursive definition*

$$\begin{cases} f(\lambda) = 0 & \text{Basis Step} \\ f(w0) = f(w) + 1 \\ f(w1) = f(w) + 1 \end{cases}$$

} Rec Step

Fact: This function is onto.

$\forall b\,(b \in \mathbb{N} \to \exists a\,(a \in \{0,1\}^* \wedge f(a) = b))$

Pf Let b be arbitrary element of $\mathbb{N}$.

WTS $\exists a\,(a \in \{0,1\}^* \wedge f(a) = b)$

Build $a = \underbrace{0 \cdots\cdots 0}_{b \text{ times}}$

Apply f rec to prove f(a) = b ☺

Proving a function is …

Define f:{0,1}* → **N** by f(w) = l(w) = |w|. *Recall: recursive definition*

$$\begin{cases} f(\lambda) = 0 \\ f(w0) = f(w) + 1 \\ f(w1) = f(w) + 1 \end{cases}$$

Fact: This function is not one-to-one.

Pf WTS $\neg \forall a \forall b \left((a \in \{0,1\}^* \wedge b \in \{0,1\}^*) \rightarrow \left(\underbrace{f(a) = f(b)}_{T} \rightarrow \underbrace{a = b}_{F} \right) \right)$

Consider counterex $a = 0$, $b = 1$.

$f(a) = f(0) = f(\lambda 0) = f(\lambda) + 1 = 0 + 1 = 1$

$f(b) = f(1) = f(\lambda 1) = f(\lambda) + 1 = 0 + 1 = 1$

Proving a function is …

$f(\{1,2,3\}) = \{1,2,3\} \cap \{2,4,6\} = \{2\}$

Let A = {1,2,3} and B = {2,4,6}.

Define a function from the power set of A to the power set of B by:

$$\boxed{f : \overset{D}{\mathcal{P}(A)} \to \overset{C}{\mathcal{P}(B)}}$$

$$f(X) = X \cap B$$

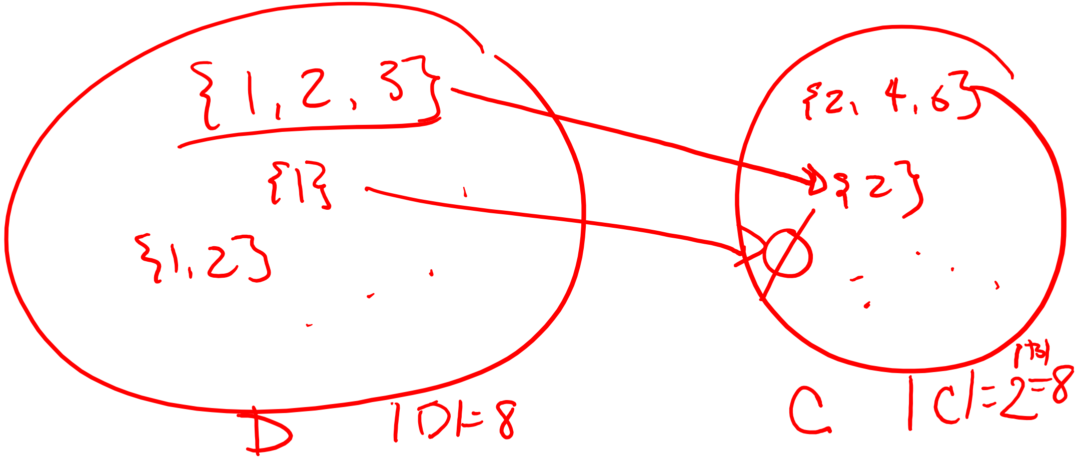
in D

$f(\{1\}) = \{1\} \cap \{2,4,6\} = \emptyset$

Well-defined?

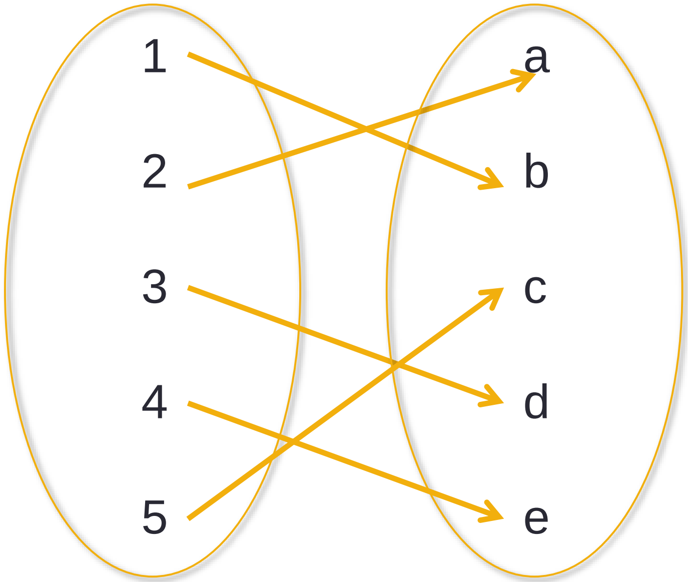
Onto?

One-to-one?



One-to-one + onto

Rosen p. 144



one-to-one correspondence

bijection

invertible

The **inverse** of a function f: A→B is the function g: B→A such that

$$\forall b(b \in B \to (g(b) = a \leftrightarrow f(a) = b))$$

Functions and subsets

Rosen Theorem 2, p 174

One-to-one: $\forall a \forall b((a \in D \wedge b \in D) \to (f(a) = f(b) \to a = b))$

Onto: $\forall b(b \in C \to \exists a \, (a \in D \wedge f(a) = b))$

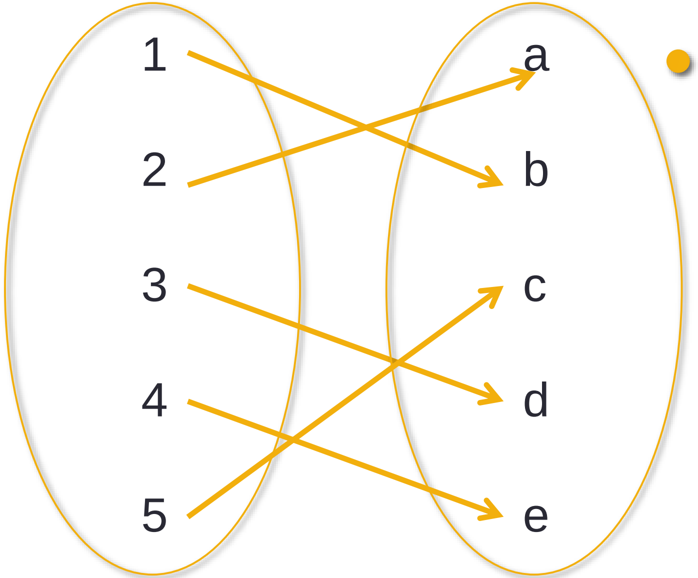
Bijection: both one-to-one and onto

Which of the following is true?

A. If A is a subset of B then there is a one-to-one function from A to B
B. If A is a subset of B then there is an onto function from A to B
C. If A is a subset of B then there is a bijection from A to B
D. None of the above.
E. I don't know

One-to-one + onto

Rosen p. 144



Fact: for finite sets A and B, there is a bijection between them if and only if |A| =|B|.

Beyond finite sets

Rosen Section 2.5

For all sets, we say

$|A| = |B|$ if and only if there is a bijection between them.

Which of the following is true?

A. $|\mathbf{Z}| = |\mathbf{N}|$
B. $|\mathbf{N}| = |\mathbf{Z}^+|$
C. $|\mathbf{Z}| = |\{0,1\}^*|$
D. All of the above.
E. None of the above.

Sizes and subsets

Rosen Theorem 2, p 174

For all sets A, B we say

$|A| \leq |B|$ if there is a one-to-one function from A to B.

$|A| \geq |B|$ if there is an onto function from A to B.

Cantor-Schroder-Bernstein Theorem: $|A| = |B|$ iff $|A| \leq |B|$ and $|A| \geq |B|$

Which of the following is true?

A. If A is a subset of B then $|A| \leq |B|$
B. If A is a subset of B then $|A| \neq |B|$
C. If A is a subset of B then $|A| = |B|$
D. None of the above.
E. I don't know

Beyond finite sets

Rosen Section 2.5

For all sets, we say

$|A| = |B|$ if and only if there is a bijection between them.

Which of the following is true?

A. $|\mathbf{Q}| = |\mathbf{Q}^+|$
B. $|\mathbf{Q}^+| = |\mathbf{N} \times \mathbf{N}|$
C. $|\mathbf{N}| = |\mathbf{Q}|$
D. All of the above.
E. None of the above.

Cardinality

Rosen Defn 3 p. 171

- Finite sets — $|A| = n$ for some nonnegative int n
- Countably infinite sets — $|A| = |\mathbf{Z}^+|$ (informally, can be listed out)
- Uncountable sets — Infinite but not in bijection with $\mathbf{Z}^+$