CARDINALITY

DISCRETE MATHEMATICS AND THEORY 2

MARK FLORYAN

GOALS!

1. Quick review of functions!

2. How do we use functions to compare the sizes of sets? Why might this be useful as we move forward talking about computation?

3. Do all infinite sets have the same size? What can this tell us (already) about the theory of computation?

PART 1: QUICK REVIEW OF FUNCTIONS

DEFINING FUNCTIONS

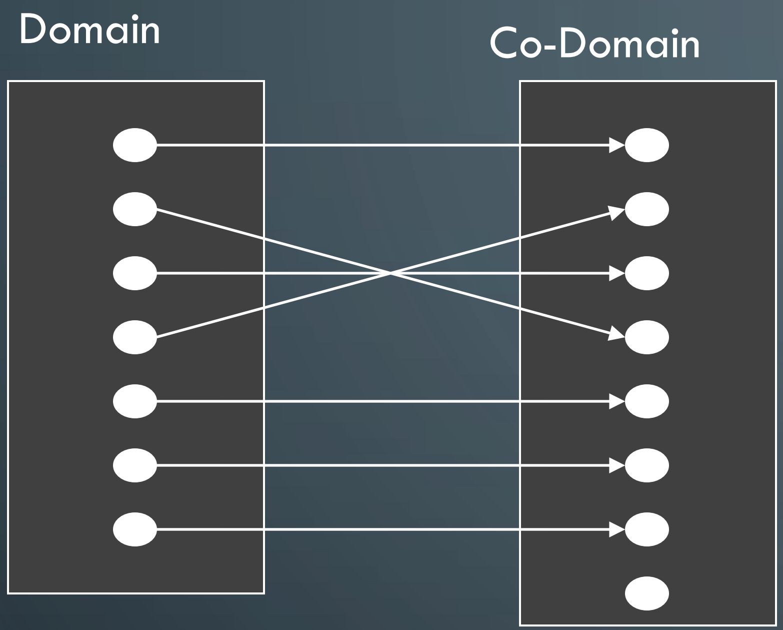
Function: a "mapping" from input to output

- $f: D \to C$
  - Function f maps elements from the set D to an element from the set C
  - D: the domain of f
  - C: the co-domain of f
  - Range/image of f: $\{f(d): d \in D\}$
    - The elements of C that are "mapped to" by something

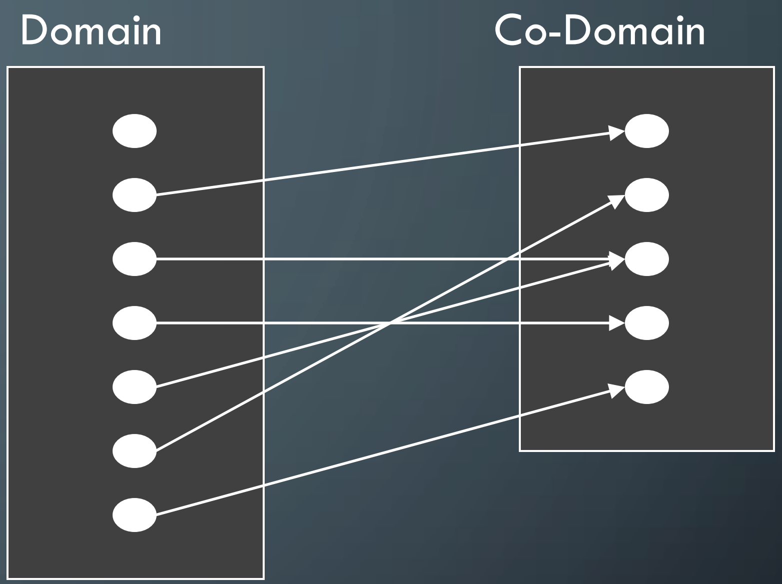
Finite function: a function with a finite domain

$f: D \to C$ is a finite function if D is finite. Otherwise it's an infinite function

INJECTIVE FUNCTIONS



INJECTIVE FUNCTION



NON-INJECTIVE FUNCTION

One-to-one (injective)

$x \neq y \Rightarrow f(x) \neq f(y)$

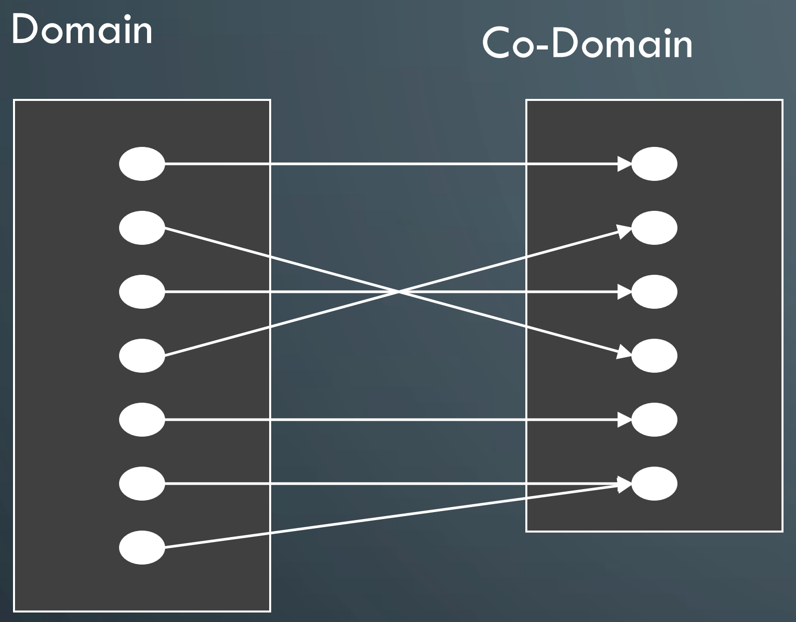
Different inputs yield different outputs

No two inputs share an output

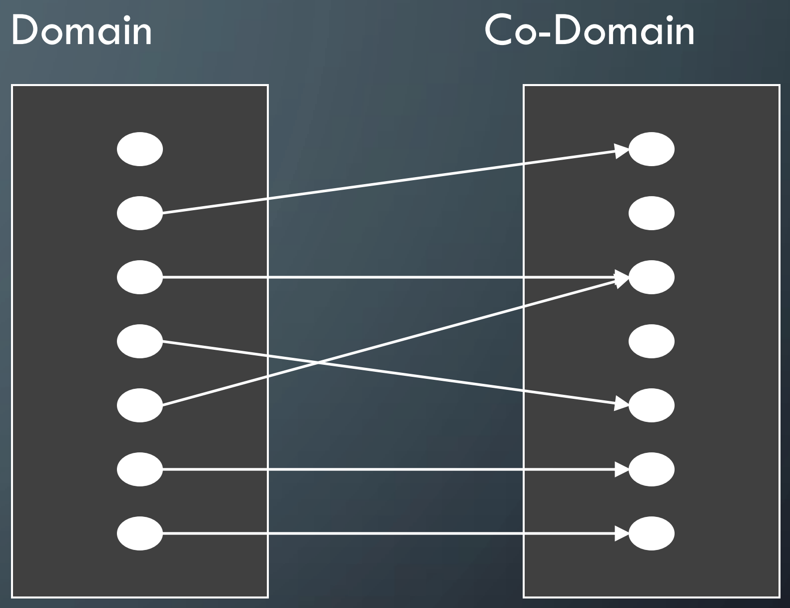
PROPERTIES OF FUNCTIONS

- One-to-one (injective)
  - $x \neq y \Rightarrow f(x) \neq f(y)$
- Onto (surjective)
  - $\forall c \in C, \exists d \in D : f(d) = c$
  - Everything in C is the output of something in d

ONTO, SURJECTIVE FUNCTIONS



SURJECTIVE FUNCTION



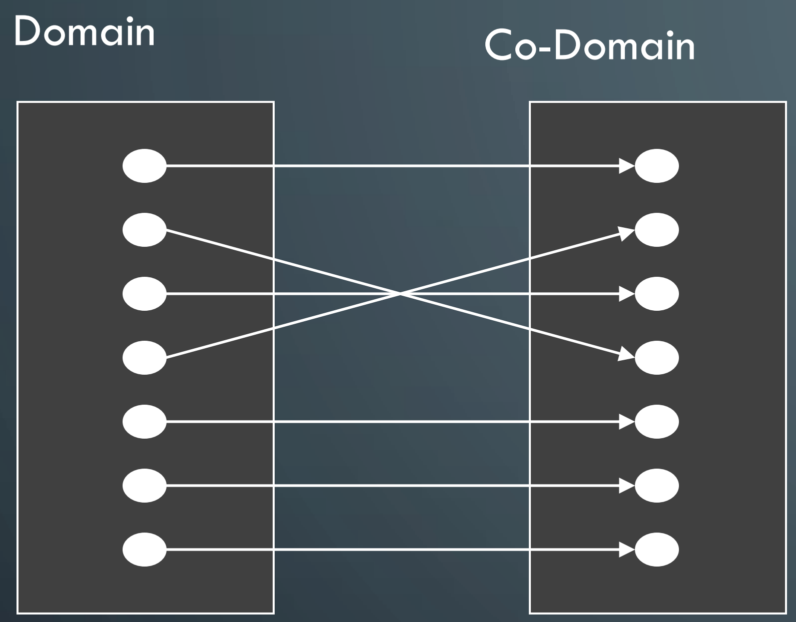
NON-SURJECTIVE FUNCTION

Everything in Co-Domain "receives" something

PROPERTIES OF FUNCTIONS

- One-to-one (injective)
  - $x \neq y \Rightarrow f(x) \neq f(y)$
- Onto (surjective)
  - $\forall c \in C, \exists d \in D : f(d) = c$
- One-to-one Correspondence (bijective)
  - Both one-to-one and surjective
  - Everything in C is mapped to by a unique element in D
  - All elements from domain and co-domain are perfectly “partnered”

BIJECTIVE FUNCTIONS



BIJECTIVE FUNCTION

Because Onto:
Everything in Co-Domain “receives” something

Because 1-1:
Nothing in Co-Domain “receives” two things

Conclusion:
Things in the Domain exactly “partner” with things in Co-Domain

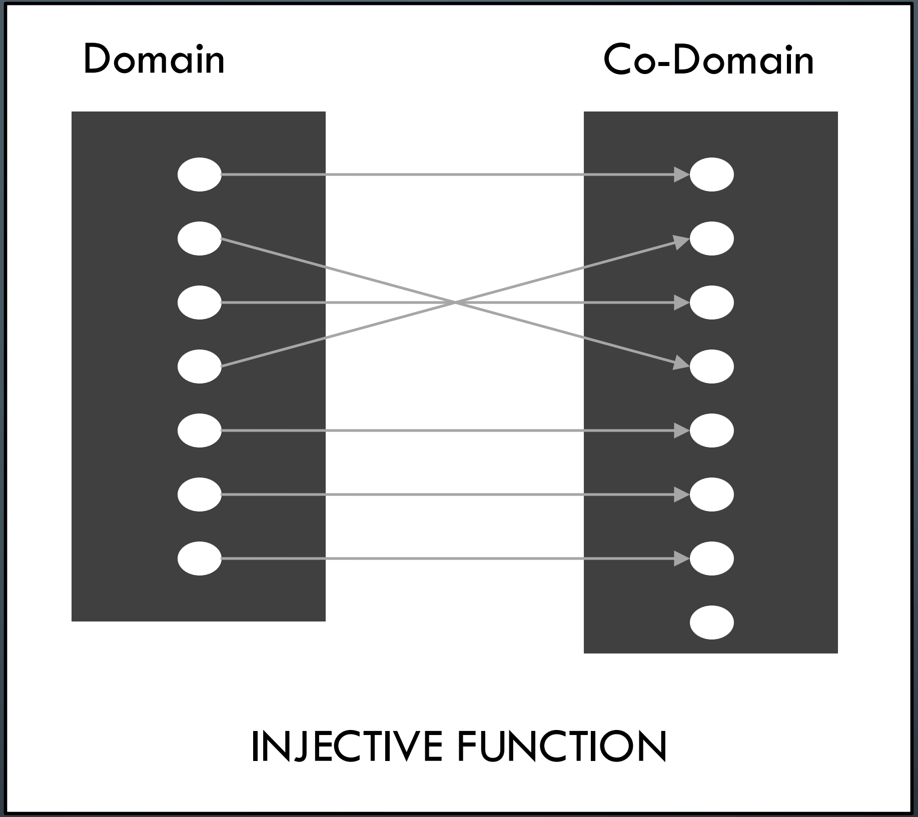
PART 2: USING FUNCTIONS TO COMPARE SIZES OF SETS

COMPARING CARDINALITIES WITH FUNCTIONS

- Let f be a finite function
  - $f: D \to C$
- Consider the following possible characteristics of f
  - Injective
  - Surjective
  - Bijective

Each of these will tell us something about the relative sizes of D and C

1-1, INJECTIVE FUNCTIONS



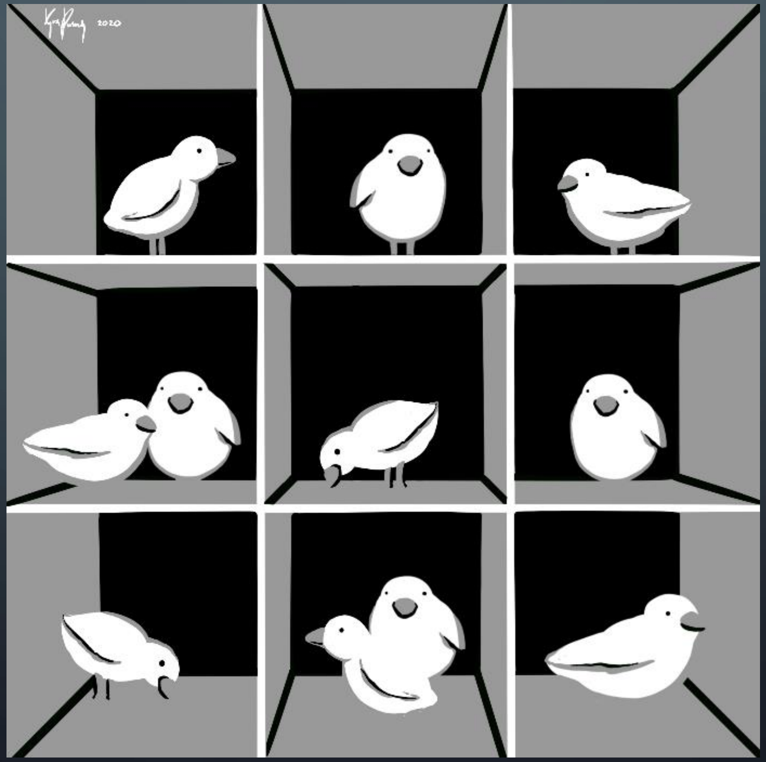
Thus, showing there exists an injective function from D to C is one way to show that $|C| \geq |D|$

Nothing in Co-Domain "receives" two things

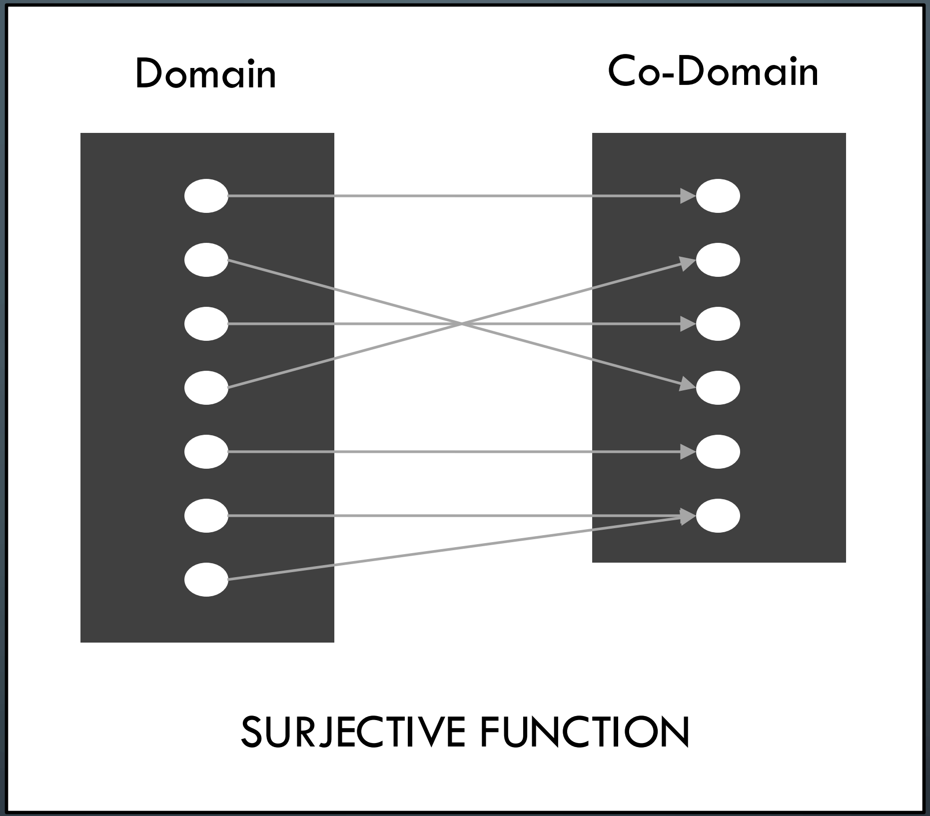
****Only possible if** $|C| \geq |D|$

PIGEONHOLE PRINCIPLE

- Every pigeon is sitting in a hole
- There are more pigeons than there are holes
- At least one hole has at least two pigeons



ONTO, SURJECTIVE FUNCTIONS



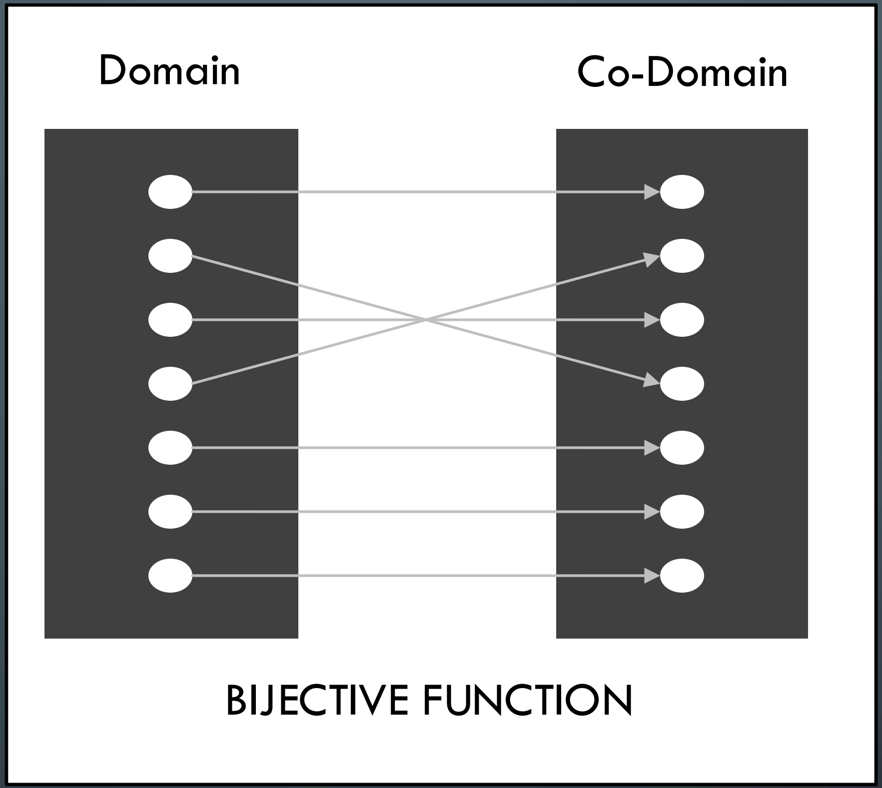
Thus, showing there exists a surjective function from D to C is one way to show that $|D| \geq |C|$

Everything in Co-Domain “receives” something

****Only possible if** $|D| \geq |C|$

BIJECTIVE FUNCTIONS

Because 1-1:
Nothing in Co-Domain "receives" two things
$|C| \geq |D|$



Because Onto:
Everything in Co-Domain "receives" something
$|D| \geq |C|$

Conclusion:

Things in the Domain exactly "partner" with things in Co-Domain

****Note: This means that** $|D| = |C|$

COMPARING CARDINALITIES WITH FUNCTIONS

- To show $|S| \geq |T|$
  - Find a surjective function $f: S \to T$
  - Find an injective function $f: T \to S$
- To show $|S| = |T|$
  - Find a bijective function $f: S \leftrightarrow T$
  - Find both a surjective function $f_1: S \to T$ and an injective function $f_2: S \to T$

PRACTICE: $|\{0,1\}^n| = 2^n$ VIA BIJECTION

Theorem: $|\{0,1\}^n| = 2^n$

How do we show this? Any ideas?

$|\{0,1\}^n| = 2^n$ VIA BIJECTION

- Proof idea:
  - Find a bijection $f_n: \{0,1\}^n \leftrightarrow \{x \in \mathbb{N} | x < 2^n\}$

- Given $b \in \{0,1\}^n$, what is $f_n(b) \in \{x \in \mathbb{N} | x < 2^n\}$?
  - $f_n(b) = \sum_{i=0}^{n-1} b_i \cdot 2^i$
  - E.g. $1101 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$
  - In other words, let each item b map to the natural number corresponding to the binary representation!!

CALCULATING BINARY OF 13

- 13 is odd, so last bit is 1
  - $x = \left\lfloor \frac{13}{2} \right\rfloor = 6$
- 6 is even, so next bit is 0
  - $x = \left\lfloor \frac{6}{2} \right\rfloor = 3$
- 3 is odd, so next bit is 1
  - $x = \left\lfloor \frac{3}{2} \right\rfloor = 1$
- 1 is odd, so next bit is 1

$b =$

1	1	0	1

…and fill with the last n-4 zeros to ensure there are n digits

PRACTICE: $|\{0,1\}^n| = 2^n$ VIA BIJECTION

Theorem: $|\{0,1\}^n| = 2^n$

Is the mapping we provided injective (Every input has unique output)? Why?

> Take two unique inputs B1 and B2
> B1 and B2 differ in at least one digit
> Thus, values differ if no other way to produce the exact value of that bit
> Consider case where B1 and B2 differ in multiple bits, but sum of difference of sum bits equals difference in another bit.
> This is impossible because sum of powers of two can never equal another power of 2.
> Thus B1 and B2 map to two different outputs. Function is injective.

Is the mapping we provided surjective (Every value less than 2^n is covered)? Why?

> Take an arbitrary natural num. less than 2^n
> Convert it into a bitstring as per the function on previous slide.
> This bitstring must use fewer than n bits because 2^n exactly would use the nth bit (indexing from 0).
> Thus, every number 0 through $2^n - 1$ is mapped onto by some bitstring.

PRACTICE 2

Theorem: For a finite set S, $|\mathcal{P}(S)| = 2^{|S|}$

How do we show this? Any ideas?

FOR A FINITE SET S, $|\mathcal{P}(S)| = 2^{|S|}$

- Find a function $f: \mathcal{P}(S) \leftrightarrow \{0,1\}^{|S|}$
- Example: let $S = \{1,2,3\}$
- $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$
- $f(\{1,2\}) = 110$
- $f(\emptyset) = 000$
- Bijection: give each value of S an index, for a particular subset of S, make the bit at that index 0 if it is absent, otherwise make it 1.

WHY IS THIS A BIJECTION?

Show that it's injective

- Different subsets of S result in different strings
- This holds because for two subsets of S, call them X and Y, if $X \neq Y$ there must be some value $a \in S$ such that $(a \in X) \wedge (a \notin Y)$ or $(a \notin X) \wedge (a \in Y)$. This means that $f(X)$ is different from $f(Y)$ at the bit associated with element a.

Show that it's surjective

- Every string is mapped to by some subset of S
- Consider that we have some string $b \in \{0,1\}^{|S|}$. We can find the subset of S called B such that $f(B) = b$ by including the value associated with bit i in b provided that bit is 1

PART 3: COMPARING SIZES OF INFINITE SETS

INFINITE CARDINALITY

How do we compare the sizes of two infinite sets? Wait…do they not automatically have the same size?

INFINITE CARDINALITY

We say that for (infinite) sets A and B, that $|A| = |B|$ if there is a bijection $f: A \leftrightarrow B$

COUNTABILITY AND UNCOUNTABILITY

A set S is countable if $|S| \leq |\mathbb{N}|$

If $|S| = |\mathbb{N}|$, then S is "countably infinite"

A set S is countable if there is an onto (surjective) function from $\mathbb{N}$ to S

Otherwise a set is uncountable.

PRACTICE: SHOW THAT $|\{0,1\}^*| = |\mathbb{N}|$

$\{0,1\}^*$ IS COUNTABLE

- Need to “represent” strings with naturals
- Idea: build a “list” of all strings, represent each string by its index in that list

LISTING ALL STRINGS (BAD WAY)

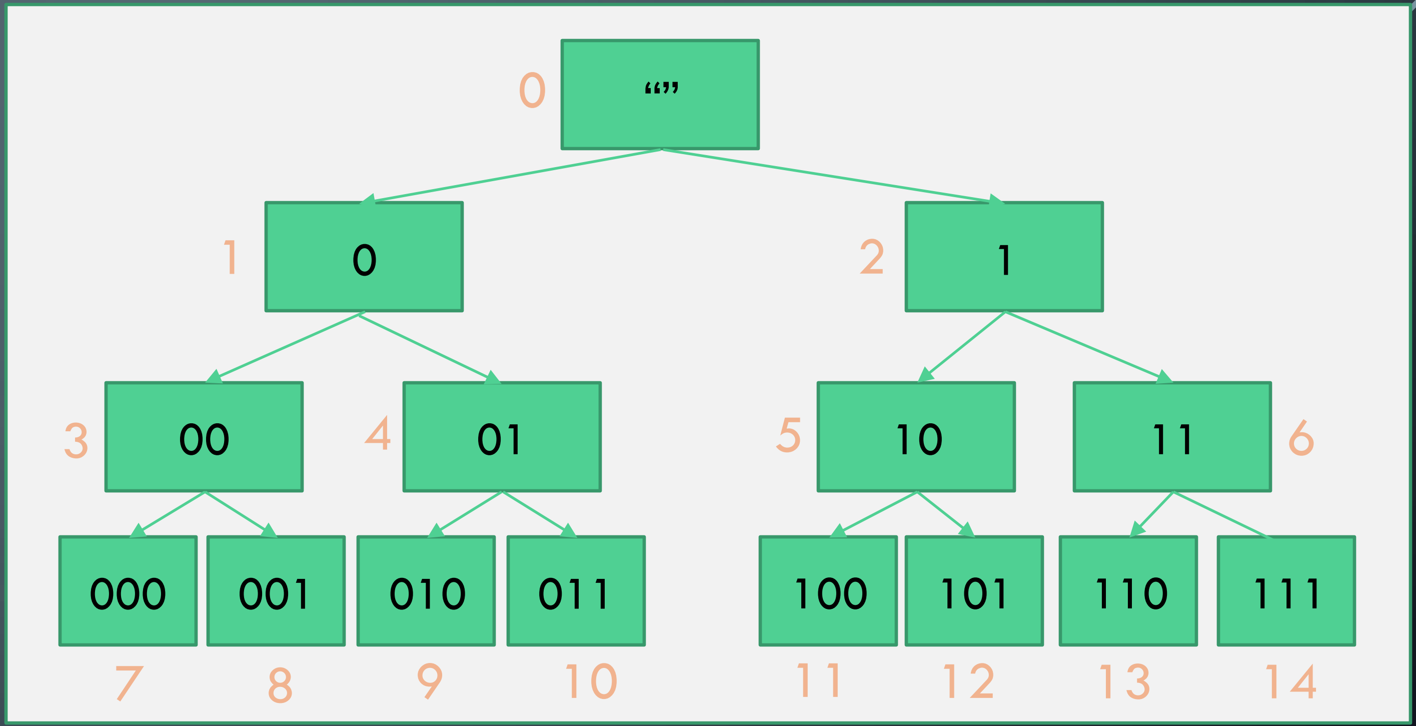
$f_{bad}: \{0,1\}^* \rightarrow \mathbb{N}$ can be defined as follows:

$f_{bad}(s) =$ the number that s represents

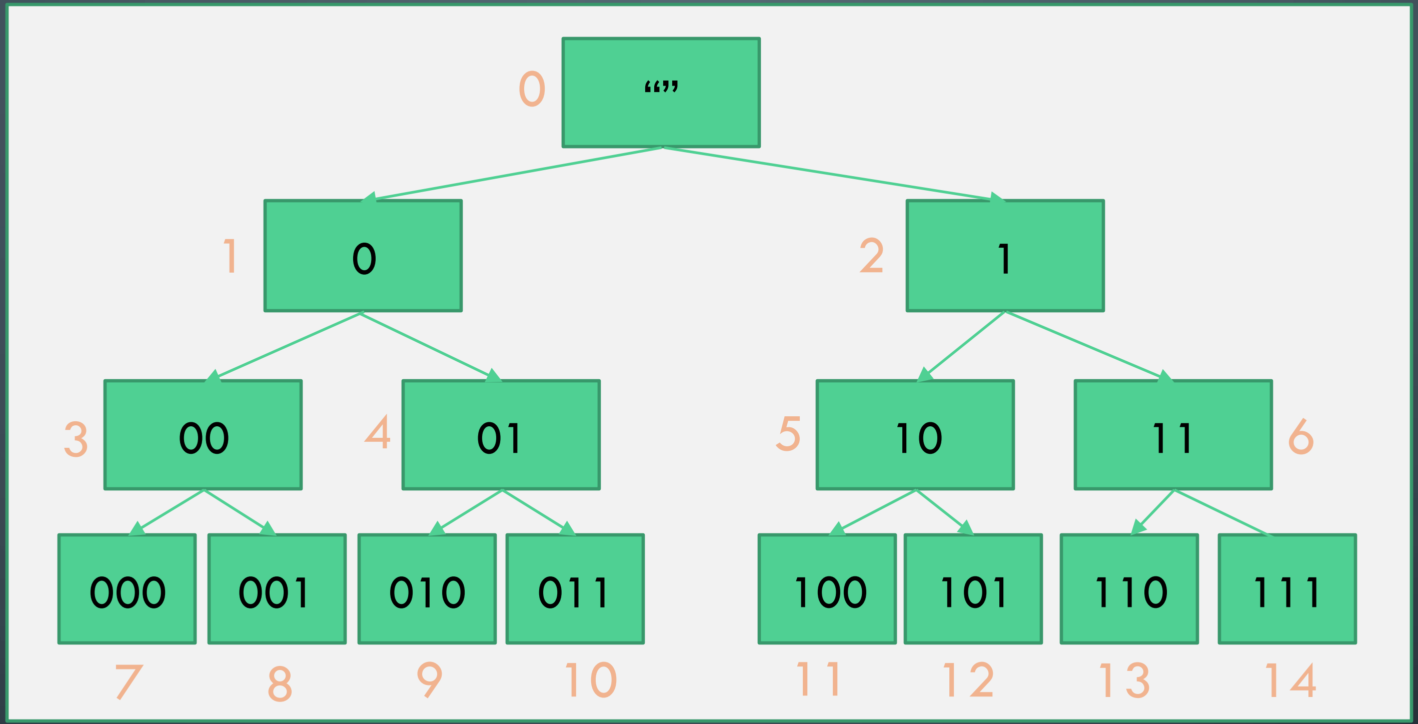
Why is this function not a bijection?

LISTING ALL STRINGS

- $\{0,1\}^0 = \{""\}$ (index: 0)
- $\{0,1\}^1 = \{0,1\}$ (indices: 1 2)
- $\{0,1\}^2 = \{00,01,10,11\}$ (indices: 3 4 5 6)
- $\{0,1\}^3 = \{000,001,010,011,100,101,110,111\}$ (indices: 7 8 9 10 11 12 13 14)



LISTING ALL STRINGS



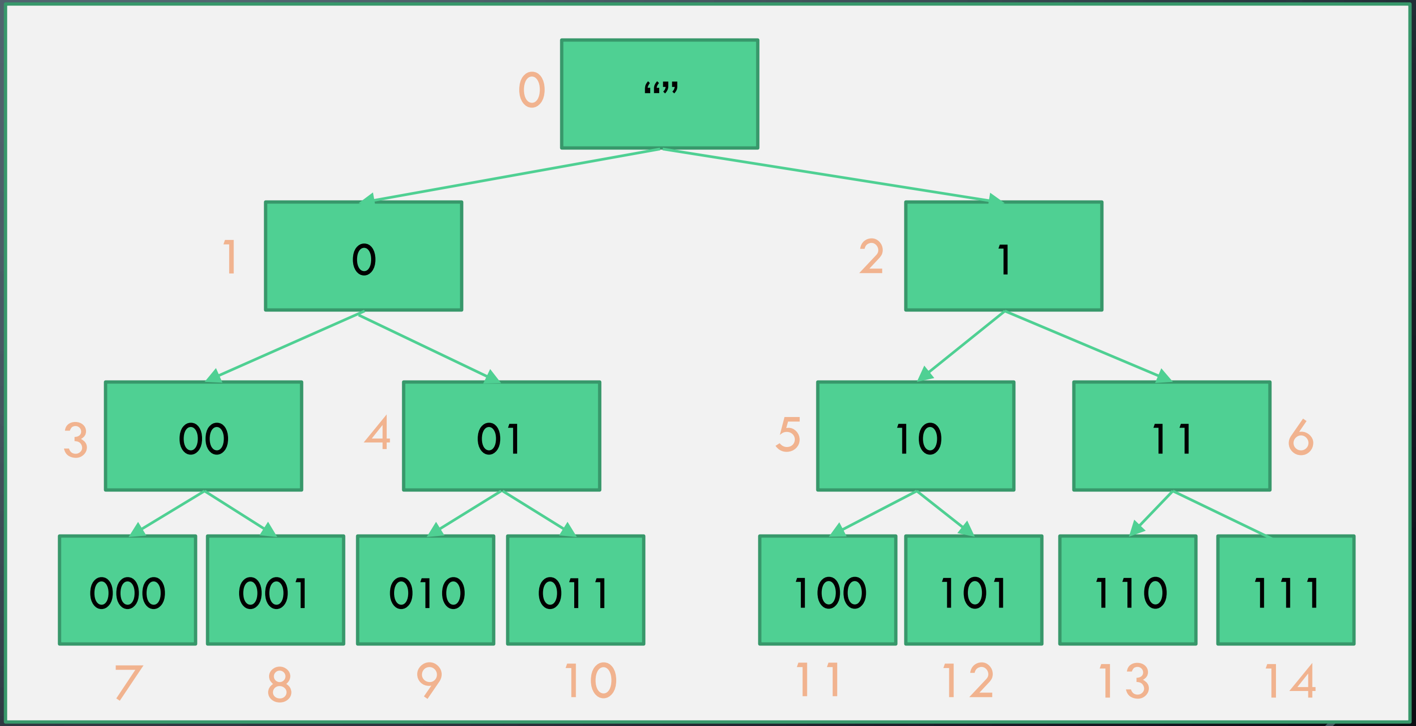
Formulaic version:

$$f(w \in \{0,1\}^*) = 2^{|w|} - 1 + b(w)$$

**Where b(w) is the integer value of the binary bitstring w

WHY IS THIS A BIJECTION?

- ***Injective***: different strings map to different numbers:
  - Different strings map to different nodes in the tree
  - No two nodes in the tree have the same index
- ***Surjective***: every number appears
  - We listed them one by one and there are an infinite number of nodes.



DEMONSTRATE THAT EACH OF THE FOLLOWING IS COUNTABLE

- $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$
- $\{n \in \mathbb{N} | n \text{ is even}\}$
- $\{n \in \mathbb{N} | n \text{ is odd}\}$
- $\mathbb{Z}$
- $\mathbb{N} \times \mathbb{N}$
- $\mathbb{Q}$

PROOF: $\mathbb{Z}^+$ IS COUNTABLE

- $f_+ : \mathbb{Z}^+ \leftrightarrow \mathbb{N}$

PROOF: $\{n \in \mathbb{N} | n \text{ IS EVEN}\}$ IS COUNTABLE

- $f_e: \{n \in \mathbb{N} | n \text{ is even}\} \leftrightarrow \mathbb{N}$

PROOF: $\{n \in \mathbb{N} | n \text{ IS ODD}\}$ IS COUNTABLE

- $f_0 : \{n \in \mathbb{N} | n \text{ is odd}\} \leftrightarrow \mathbb{N}$

$\mathbb{Z}$ IS COUNTABLE

- To build $f_z: \mathbb{Z} \leftrightarrow \mathbb{N}$
  - Idea: map natural numbers to evens, map negative numbers to odds
- $f_z(x) =$
  - $f_e^{-1}(x)$ If $x \in \mathbb{N}$
  - $f_o^{-1}(-x)$ if $x \in \mathbb{Z}^-$
- Note that this means that if A and B are both countable then $A \cup B$ is also countable!

$\mathbb{N} \times \mathbb{N}$ IS COUNTABLE

Thoughts on how to prove it?

ℕ × ℕ IS COUNTABLE

ℕ →

ℕ ↓

	0	1	2	3	4	5	
0	0,0	0,1	0,2	0,3	0,4	0,5	…
1	1,0	1,1	1,2	1,3	1,4	1,5	…
2	2,0	2,1	2,2	2,3	2,4	2,5	…
3	3,0	3,1	3,2	3,3	3,4	3,5	…
4	4,0	4,1	4,2	4,3	4,4	4,5	…
	⋮	⋮	⋮	⋮	⋮	⋮	

$\mathbb{Q}$ IS COUNTABLE

- Idea: there is a surjective mapping from $\mathbb{Z} \times \mathbb{Z}^+$ to $\mathbb{Q}$
- This one is left as an exercise (could be on homework or quiz)

NUMBER OF PROGRAMS AS NUMBER OF FUNCTIONS

HOW MANY PYTHON/JAVA PROGRAMS?

- How do we represent Java/Python programs?
- How many things can we represent using that method?

HOW MANY FUNCTIONS $\Sigma^* \to \Sigma^*$?

- Short answer: Too many!
  - Uncountable
  - $|\{f \mid f : \Sigma^* \to \Sigma^*\}| > |\mathbb{N}|$
- Conclusion: Some functions cannot be computed by any java/python program
- How to prove this?

HOW TO SHOW SOMETHING IS UNCOUNTABLE?

UNCOUNTABLY MANY FUNCTIONS

- If we show a subset of $\{f \mid f: \Sigma^* \rightarrow \Sigma^*\}$ is uncountable, then $\{f \mid f: \Sigma^* \rightarrow \Sigma^*\}$ is uncountable too

- Consider just the "yes/no" functions (decision problems):

$$\{\boldsymbol{f} \mid \boldsymbol{f}: \{\mathbf{0}, \mathbf{1}\}^* \rightarrow \{\mathbf{0}, \mathbf{1}\}\}$$

b	$f(b)$
""	1
0	0
1	0
00	1
01	1
10	1
11	1
000	0
001	0

GOAL: $\{f: \{0,1\}^* \rightarrow \{0,1\}\}$ IS UNCOUNTABLE

- Each function can be represented by a single infinite bitstring : $\{0,1\}^\infty$ is a simpler representation of f

- Show there is no onto mapping from $\mathbb{N}$ to $\{0,1\}^\infty$

b	$f(b)$
“”	1
0	0
1	0
00	1
01	1
10	1
11	1
000	0
001	0

For example, this function can be fully described by the outputs only (the order of the inputs is fixed). So the right column (100111100…) fully describes this unique function

$|\{0,1\}^\infty| > |\mathbb{N}|$

- Idea:
  - show there is no way to “list” all infinite length binary strings
  - Any list of binary strings we could ever try will be leaving out elements of $\{0,1\}^\infty$

$|\{0,1\}^{\infty}| > |\mathbb{N}|$

Attempt at mapping $\mathbb{N}$ to $\{0,1\}^{\infty}$

	b_0	b_1	b_2	b_3	b_4	b_5	b_6
0	1	1	1	1	1	1	1
1	0	0	0	0	0	0	0
2	1	0	1	0	1	0	1
3	1	1	0	1	1	0	1
4	1	0	1	1	0	1	0
5	1	0	0	1	1	1	0
6	0	0	0	1	1	1	1
…							
	0	1	0	0	1	0	0

A string that our attempt missed

Derive by selecting each b_i as the opposite of the b_i from row i

$|\{0,1\}^\infty| > |\mathbb{N}|$

Attempt at mapping $\mathbb{N}$ to $\{0,1\}^\infty$

	b_0	b_1	b_2	b_3	b_4	b_5	b_6
0	**1**	1	1	1	1	1	1
1	0	**0**	0	0	0	0	0
2	1	0	**1**	0	1	0	1
3	1	1	0	**1**	1	0	1
4	1	0	1	1	**0**	1	0
5	1	0	0	1	1	**1**	0
6	0	0	0	1	1	1	**1**
…							
	0	1	0	0	1	0	0

Take the bolded bits across the diagonal. Select a bitstring where each of these bits is flipped. In this example: **0100100…**

OTHER COUNTABLE/UNCOUNTABLE SETS

- Countable sets:
  - Integers
  - Rational numbers
  - Any finite set
- Uncountable Sets:
  - Real numbers
  - The power set of any infinite set

CANTOR'S THEOREM

- For any set S, $|S| < |2^S|$
- Even if S is infinite!
- Idea:
  - $|S| \leq |2^S|$ (why?)
  - There cannot be a bijection between S and 2^S
  - Not going to prove

CONCLUSION

- There are countably many strings
  - And therefore binary strings, programs, etc.
- There are uncountably many functions
- ***Some functions can't be implemented***