Functions: One-to-One and Permutations

Magritte

Discrete Structures (CS 173)

Gul Agha

Based in part on slides by Derek Hoiem, University of Illinois

Administrative

- Moodle Activity due Wednesday evening
- Exam next Thursday
  - Remember your discussion section time
- Review materials available online
  - Read them and prepare questions for discussion section
  - Test will not cover functions but everything else since the last examlet.

Common gotchas (feedback from TAs)

- Assuming conclusion holds
  - Remember to “suppose” the hypothesis holds and work your way from that to the conclusion
  - Don’t assume conclusion holds
- Equivalent vs. equals ($\equiv$ vs. $=$)
  - Equals means that two elements have the same value (e.g., $3^2 = 9$)
  - Equivalent (\equiv) means that they are in the same equivalence set (e.g., $3 \equiv 5 \pmod 2$)
- mod as a function vs. a relation
  - In most programming languages “mod” is a function (e.g., `3 = mod(21, 9)`), but mathematically mod is a relation: a whole set of integers is congruent to $x \pmod k$

Last class: functions

- A *function* is a relation ‘mapping’ every element in the domain to an element in the range so that each element is mapped to a unique element in the range.
- For two functions to be *equal*, both have the same domain and range, and each assignment is the same.
- A function is *onto* (or *surjective*) iff every output element is assigned at least once.

$$f: A \to B \text{ such that } f(x) = \cdots$$

domain co-domain

Today’s class: more with functions

- When is a function “*one-to-one*” (or *injective*).
- When is a function “bijective”?
- What is the inverse of a function?
- Onto, One-to-One, Bijective and Cardinalities of Domain and Range
- The Pigeonhole principle
- Permutations and their applications

One-to-one

x is a *preimage* of y if $f(x) = y$.

One-to-one: no two inputs map to the same output (i.e., no output has more than one preimage):

$$f: A \to B, \forall x, y \in A, (x \neq y) \to (f(x) \neq f(y))$$

What is the contraposition?

overhead

Proof of one-to-one

Claim: $f: \mathcal{R} \rightarrow \mathcal{R}, \quad f(x) = 2x - 1$ is one-to-one.

Definition: $f: A \rightarrow B, f(x)$ is one-to-one iff $\forall x, y \in A, (f(x) = f(y)) \rightarrow (x = y)$

overhead

Proof that one-to-one is compositional

Claim: For any sets A, B, C and functions $f: A \to B$, $\mathrm{g}: \mathrm{B} \to C$, if f and g are one-to-one, then $g \circ f$ is also one-to-one.

Definition: $f: A \to B, f(x)$ is one-to-one iff $\forall x, y \in A, (f(x) = f(y)) \to (x = y)$

Bijection and inversion

A function is *bijective* if it is onto (surjective) and one-to-one (injective).

Inverse function

if $f: A \to B, f(x) = y$, then $f^{-1}: B \to A, f^{-1}(y) = x$.

$$\forall x \in A, f^{-1}\big(f(x)\big) = x$$

overhead

Onto and Set Cardinality

If there is a function $f: A \to B$, such that f is onto, then $|A| \geq |B|$

The converse also holds.

Example

- Cardinality of the set of all ordered pairs of integers is greater than or equal to the cardinality of the set of rational numbers

$$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$$

Proof: Need a map $f: \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ which is one to one.

Map each rational number $\frac{p}{q}$ to (p, q)

Is the function onto? (No! *Why?*)

Diagonalization

Claim: For any set A, $|\mathrm{A}| < |\boldsymbol{\mathcal{P}}(A)|$

Proof: Let $f\colon \mathrm{A} \to \boldsymbol{\mathcal{P}}(A)$, such that f is onto (surjective).

Consider $T = \{s \in \mathrm{A} \mid s \notin f(s)\}$

Clearly, $T \subseteq \mathrm{A}$.

Now $\forall s \in A$, either (1) $s \in T$ or (2) $s \notin T$.

Case 1. If $s \in T$ then $s \notin f(s)$, thus $T \neq f(s)$.

Case 2. If $s \notin T$ then $s \in f(s)$, thus $T \neq f(s)$.

So T is not in the image of f

Thus there is no $s \in A$ such that $T = f(s)$, thus f is not onto.

Diagonalization and Infinities

Claim: The cardinality of the set of real numbers is greater than the cardinality of the set of natural numbers.

$$|\mathbb{N}| < |\mathcal{R}|$$

Cardinality of $\boldsymbol{\mathcal{P}}(\mathbb{N})$

Claim: The cardinality of the powerset of the set of natural numbers is less than or equal to the cardinality of the set of (0,1), where $(0,1) = \{x \in \mathcal{R} | 0 < x < 1\}$.

$$|\boldsymbol{\mathcal{P}}(\mathbb{N})| \leq |(0,1)|$$

(*Note:* In fact $|\boldsymbol{\mathcal{P}}(\mathbb{N})| = |\mathcal{R}|$).

Consider the function f that maps a given subset X of the natural numbers to a real number r in (0,1) expressed in binary (base 2) notation such that *i*th bit of r is 0 if $i \notin X$ and 1 if $i \in X$…

One-to-One and Set Cardinality

If there is a function $f: A \to B$, such that f is one-to-one, then $|A| \leq |B|$

Note: the converse also holds: if $|A| \leq |B|$

then there is a function $f: A \to B$, such that f is one-to-one.

Example

Claim: The cardinality of the set of all ordered pairs of integers is less than or equal to the cardinality of the set of natural numbers.

$$|\mathbb{Z} \times \mathbb{Z}| \leq |\mathbb{N}|$$

Pigeonhole principle (+ short break)

Sherlock Holmes: “When you have eliminated the impossible, whatever remains, however improbable, must be true.”

Pigeonhole principle: if you have more objects than labels, then at least two objects must get the same label

This class has ~400 students. Is every day someone’s birthday? Do two students have the same birthday?

Claim: The first 50 powers of 13 include at least two numbers whose difference is a multiple of 47.

Claim: Suppose n people are at a party and everyone has at least one admirer. At least two people will have the same number of admirers.

Proof with bijective, pigeonhole

Claim: If $f: A \rightarrow B$ is *bijective*, then $|A| = |B|$

Definition: $f: A \rightarrow B$, is *one-to-one* iff every output is assigned at most once

Definition: $f: A \rightarrow B, f(x)$ is *onto* iff every output is assigned at least once

overhead

Cardinality of (0,1)

Claim: The cardinality of the set of real numbers in the interval (0,1) is the same as the cardinality of the set of real numbers:

$$|(0,1)| = |\mathcal{R}|$$

where $(0,1) = \{x \in R | 0 < x < 1\}$

Permutations

Ordered selection

Suppose I have 6 gems, and you get to choose 1. How many different combinations of gems can you choose?

Suppose I have n gems and want to put them in a row from left to right. How many different ways can I arrange them?

Suppose I have 6 gems and want to put three of them in a row from left to right. How many different ways can I arrange them?

Unordered selection

Suppose I have 6 gems, and you get to choose 2. How many different combinations of gems can you choose?

Suppose I have n gems, and you choose $k \leq n$. How many combos?

overhead

Permutations

Suppose $f: A \to B$ with $|A| = k$ and $|B| = n$. How many different one-to-one functions can I create? $P(n, k)$

How many ways can I rearrange the letters in "nan"?

How many ways can I rearrange the letters in "yellowbelly"?

overhead

Proof with one-to-one

Claim: Strictly increasing functions on linearly ordered (totally ordered) sets are bijective. Consider the case where the ordering on the domain and range is the same.

Definition: $f: A \to B$ is a *bijection* iff $\forall x, y \in A, (x \neq y) \leftrightarrow (f(x) \neq f(y))$

Definition: $f: A \to B, f(x)$ is *strictly increasing* iff $\forall x, y \in A, (x < y) \to \big(f(x) < f(y)\big)$

In fact all strictly monotonically increasing functions are one-to-one.

overhead

Things to remember

- Definitions of one-to-one, onto, bijection
- Cardinality and one-to-one, onto, bijection
- Diagonalization
- Pigeonhole principle: if you have more objects than labels, some objects must get the same label
- Permutations: number of ordered combinations $n!/(n-k)!$ divided by number of equivalent orderings
- Examlet 2 on Thursday!