Lec 13: Functions II

Prof. Adam J. Aviv

GW

CSCI 1311 Discrete Structures I
Spring 2023

Pigeonhole Principle

Theorem (Pigeonhole Principle)

Let n and k be positive integers. When placing n objects (or pigeons) into k boxes (or pigeonholes), if $n > k$ then at least one box must contain more than one object.

Proof.

Proof by contraposition. We can show that: If all k boxes contain *at most* one object, then $k \leq n$.

Observe that the max number of objects n is the same as the number of boxes k since there is at most one per box. It is the case $k \leq n$.

By the contrapositive, we conclude the theorem is true. $\square$

Applying pigeon, examples

For every 27 word sequence in the US constitution, at least two words will start will the same letter.

If you pick five numbers from integers 1 to 8, then two of them must add up to 9.

https://mindyourdecisions.com/blog/2008/11/25/16-fun-applications-of-the-pigeonhole-principle/

Pigoenholes and onto and one-to-one functions

Consider the two sets, $A = \{1, 2, 3\}$ and $B = \{w, x, y, z\}$

- Is it possible to find an one-to-one function from A to B?
- Is it possible to find an onto function from A to B?

- One-to-one: Pigeon hole principle with A being pigeons and B being pigeonholes. A counter example must exists when $|A| > |B|$.
- Onto: Pigeon hole principle with B being pigeons and A being pigeonholes.A counter example must exists when $|B| > |A|$.

What about a one-to-one correspondence?

Cardinality and One-to-one Correspondence Functions

A one-to-one correspondence functions domain must be the same size as the co-domain, otherwise it would either not be onto or not one-to-one. This provides a way to reason about the cardinality of infinite sets.

Definition

Let A and B be any sets. A has the same cardinality as B if, and only if, there exists a one-to-one correspondence from A to B

$\forall$ sets A and B

$$|A| = |B| \iff (\exists f : A \to B)(f \text{ is a one-to-one correspondence})$$

Properties of Cardinality

- **Reflexive property of cardinality**
  - A has the same cardinality as A
- **Symmetric property of cardinality**
  - If A has the same cardinality as B, then B has the same cardinality as A
- **Transitive property of cardinality**
  - If A has the same cardinality as B, and B has the same cardinality as C, then A has the same cardinality as C.

A relation that is reflexive, symmetric, and transitive defines a equality relation. (We'll see this again!)

Proving Reflexive Property

Definition

The identify function $I_A : A \to A$ is a function such that forall $a \in A$, $I_A(a) = a$.

Example: Here are two identity functions for $\mathbb{R}$

- $g(x) = x + 0$
- $h(x) = x \cdot 1$

Is the identity function of a set a one-to-one correspondence?

Identity functions are one-to-one correspondences

Proof.

The identity function I_A is one-to-one because if $I_A(x_1) = I_A(x_2)$, then $x_1 = x_2$ because $I_A(x) = x$ for all inputs.

The identify function I_A is a onto because if we assume that u is in the co-domain, then we can always find v in the domain such that $I_A(v) = u$. The example is when $u = v$ because then $I_A(v) = v$ and $v = u$. □

So, **cardinality is reflexive** ($|A| = |A|$) because the identity function I_A is a one-to-one corresponds between A and A.

Proving symmetry of cardinality

If we assume that $|A| = |B|$ then there exists a one-to-one correspondence function f between A and B, then there exists a inverse function f^{-1} between B and A because all one-to-one correspondence functions are invertabl e.

We need to show that, if $f : A \rightarrow B$ and f is a one-to-one correspondence, and $f^{-1} : B \rightarrow A$ is the inverse function from B to A, then f^{-1} is also a one-to-one correspondence?

Inverse of a one-to-one correspondence is also one-to-one correspondence

Recall the definition of a function and its inverse:

$$f^{-1}(y) = x \iff f(x) = y$$

Proof.

f^{-1} **is one-to-one.** We must show that if $f^{-1}(y_1) = f^{-1}(y_2)$ then $y_1 = y_2$. Let $x = f^{-1}(y_1) = f^{-1}(y_2)$, then by definition of the inverse function, we have

$$x = f^{-1}(y_1) \implies f(x) = y_1$$
$$x = f^{-1}(y_2) \implies f(x) = y_2$$

So $f(x) = y_1$ and $f(x) = y_2$ so $y_1 = y_2$

f^{-1} **is onto.** Let x be in the co-domain f^{-1}, we must show that there exists a $y = f^{-1}(x)$. By definition of the inverse function, $f(x) = y$ and so we can find a y such that $f^{-1}(x) = y$

$\square$

Transitivity and composition of functions

Definition

Let $f : X \to Y'$ and $g : Y' \to Z$ be functions, then $g \circ f : X \to Z$ is the composition of f and g

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

Example, $f(x) = x + 1$ and $g(n) = n^2$ both be functions from $\mathbb{Z} \to \mathbb{Z}$, then

$$g \circ f = g(f(x)) = (x + 1)^2$$

and

$$f \circ g = f(g(n)) = n^2 + 1$$

Exercise

Prove the following

If $f : X \to Y$, then $f \circ I_X = f$ and $I_Y \circ f = f$.

If $g : X \to Y$ is a one-to-one correspondence function, then $g \circ g^{-1} = I_X$ and $g^{-1} \circ g = I_Y$

Composition of one-to-one functions

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

Proof.

We must show that if $(g \circ f)(x_1) = (g \circ f)(x_2)$ then $x_1 = x_2$. Then by definition of composition of functions

$$(g \circ f)(x_1) = (g \circ f)(x_2)$$
$$g(f(x_1)) = g(f(x_2))$$

Because g is one-to-one, that is $g(z_1) = g(z_2)$ implies $z_1 = z_2$, we can reduce to $f(x_1) = f(x_2)$

But also f is one-to-one, so by the same argument $x_1 = x_2$, which is what we must show.

□

Composition of onto functions

If $f : X \to Y$ and $g : X \to Z$ are both onto, then $g \circ f$ is onto.

Proof.

If $z \in Z$, then we must show there exists an $x \in X$ such that $(g \circ f)(x) = z$.

By definition of composition $(g \circ f)(x) = g(f(x))$, and since g is onto, we know there exists a $z \in Z$ for which $g(y) = z$.

Since f is also onto, we know there exists an $x \in X$ such that $y = f(x)$. And hence there exists an x such that

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

So $(g \circ f)(x)$ is onto.

□

Composition of one-to-one correspondence functions

If $f : X \to Y$ and $g : X \to Z$ are both one-to-one correspondence, then $g \circ f$ is one-to-one correspondence.

This is true based on our two prior results: the composition of onto functions is onto, and the composition of one-to-one functions is one-to-one. Thus, the composition of two one-to-one correspondence functions is also one-to-one correspondence.

How does this result prove transitivity of cardinality?

Transitivity of Cardinality

If A has the same cardinality as B, and B has the same cardinality as C, then A has the same cardinality as C.

Proof.

If A and B has the same cardinality, then there exist a one-to-one correspondence function $f : A \to B$, and the same for B and C, there exists a one-to-one correspondence function $g : B \to C$.

The composition $f \circ g$ is also a one-to-one correspondence with domain A and co-domain C, thus A and C also have the same cardinality.

□

Cardinality of Infinite Sets

This new definition of cardinality allows us to reason about the size of infinite sets: Two sets are the same size if there exists a one-to-one correspondence between them. But this definition can lead to some very, very interesting results.

Let $2\mathbb{Z}$ be the set of even integers, we can show that $|\mathbb{Z}| = |2\mathbb{Z}|$

Can you find a one-to-one correspondence function $f : \mathbb{Z} \to 2\mathbb{Z}$?

Set of Even Integers

Consider the function $f : \mathbb{Z} \to 2\mathbb{Z}, f(n) = 2n$:

$$
\begin{array}{ccccccccc}
(\mathbb{Z}) & \dots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \dots \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
f(n) = 2n & \dots & -3 \cdot 2 & -2 \cdot 2 & -1 \cdot 2 & 0 \cdot 2 & 1 \cdot 2 & 2 \cdot 2 & 3 \cdot 2 & \dots \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
(2\mathbb{Z}) & \dots & -6 & -4 & -2 & 0 & 2 & 4 & 6 & \dots
\end{array}
$$

Is f one-to-one and onto? Yes! So the set of even integers has the same cardinality as the set of *all* integers, and both are of infinite size.

Countable Sets

Definition

A set is countably infinite if, and only if, it has the same cardinality as the set of positive integers $\mathbb{Z}^+$.

A set is countable if, and only if, it is either finite or infinitely countable.

A set that is not countable is called uncountable

Exercises

Find a one-to-one correspondence function between the following infinite sets

The set of positive integers ($\mathbb{Z}^+$) to the set of *all* integers ($\mathbb{Z}$).

The set of positive integers ($\mathbb{Z}^+$) to the set of *even* integers ($2\mathbb{Z}$).

The set of rationals $\mathbb{Q}$ is countable

$$
\begin{array}{ccccccccc}
\frac{1}{1} & \rightarrow & \frac{1}{2} & & \frac{1}{3} & \rightarrow & \frac{1}{4} & & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
\frac{2}{1} & & \cancel{\frac{2}{2}} & & \frac{2}{3} & & \cancel{\frac{2}{4}} & & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{3}{1} & & \frac{3}{2} & & \cancel{\frac{3}{3}} & & \frac{3}{4} & & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
\frac{4}{1} & & \cancel{\frac{4}{2}} & & \frac{4}{3} & & \cancel{\frac{4}{4}} & & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{5}{1} & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \cdots \\
\vdots & \cdots & & & & & & &
\end{array}
$$

$f(1) = 1/1, f(2) = 1/2), f(3) = 2/1, f(4) = 3/1, f(5) = 1/3, f(6) = 1/4, \ldots$

Are the real numbers $\mathbb{R}$ countable?

Every real number can be represented as a decimal expansion

$$z.a_1, a_2, a_3, a_4 \ldots$$

where $z \in \mathbb{Z}$ and $a_i \in [0, 9]$.

The integers are numbers where all decimal places are 0, $\forall i \geq 1, a_i = 0$, and the rationals are numbers for which there are a finite expansion until 0 values are reached, where $\exists k, \forall i > k, a_i = 0$.

Cardinality of the reals (1)

Theorem

The set of all real numbers between 0 and 1 is uncountable

Proof

Suppose the set is countable, then we can write a list of real numbers and count them from (1) through (n)

$$\begin{array}{ccccccccc}
(1) & 0. & a^1_1 & a^1_2 & a^1_3 & \cdots & a^1_n & \cdots \\
(2) & 0. & a^2_1 & a^2_2 & a^2_3 & \cdots & a^2_n & \cdots \\
(3) & 0. & a^3_1 & a^3_2 & a^3_3 & \cdots & a^3_n & \cdots \\
 & & & \vdots & & & & \\
(n) & 0. & a^n_1 & a^n_2 & a^n_3 & \cdots & a^n_n & \cdots \\
 & & & \vdots & & & &
\end{array}$$

Where a^i_j is the i-th number and the digit in the j-th position of the decimal expansion

Cantor's Diagnolization (1)

As a proof by contradiction, we will show that there exists a number between 0 and 1 that is *not* in the list. An example is helpful:

$$\begin{array}{cccccccccc}
0. & \boxed{2} & 0 & 1 & 4 & 8 & 8 & 0 & 2 & \cdots \\
0. & 1 & \boxed{1} & 6 & 6 & 6 & 0 & 2 & 1 & \cdots \\
0. & 0 & 3 & \boxed{3} & 5 & 3 & 3 & 2 & 0 & \cdots \\
0. & 9 & 6 & 7 & \boxed{7} & 6 & 8 & 0 & 9 & \cdots \\
0. & 0 & 0 & 0 & 3 & \boxed{1} & 0 & 0 & 2 & \cdots \\
 & & & \vdots & & & & & &
\end{array}$$

The number $0.21371\ldots$ (highlighted above) is also a number between 0 and 1, and should be somewhere in the list, but what about the number $0.12112\ldots$?

Cantor's Diagnolization (2)

The number 0.12112... is defined such that each digit is 1 if the diagonal is *not* 1, and 2 if it is 1. Then, that number will *always* differ from every number on the list at the diagonal, a_n^n.

$$
\begin{array}{llllllllll}
0. & \boxed{2} & 0 & 1 & 4 & 8 & 8 & 0 & 2 & \cdots \\
0. & \boxed{\cancel{1}} & 2 & 1 & 1 & 1 & 2 & \cdots & & \\
\\
0. & 1 & \boxed{1} & 6 & 6 & 6 & 0 & 2 & 1 & \cdots \\
0. & 1 & \boxed{\cancel{2}} & 1 & 1 & 1 & 2 & \cdots & & \\
\\
0. & 0 & 3 & \boxed{3} & 5 & 3 & 3 & 2 & 0 & \cdots \\
0. & 1 & 2 & \boxed{\cancel{1}} & 1 & 1 & 2 & \cdots & & \\
\\
0. & 9 & 6 & 7 & \boxed{7} & 6 & 8 & 0 & 9 & \cdots \\
0. & 1 & 2 & 1 & \boxed{\cancel{1}} & 1 & 2 & \cdots & & \\
 & & & \vdots & & & & & &
\end{array}
$$

Cardinality of the reals (2)

Proof (cont.)

Construct a new number $d = 0.d_1d_2d_3 \ldots d_n \ldots$ where

$$d_n = \begin{cases} 1 & \text{if } a_n^n \neq 1 \\ 2 & \text{if } a_n^n = 1 \end{cases}$$

Then for all digits $d_k \neq a_k^k$ for all rows of the list, and thus d cannot be in the list: a contradiction.

Thus the set of real numbers between 0 and 1 are not countable. □

The implication is that $|\mathbb{Z}^+| = \infty$ and $|[0,1]| = \infty$, but $|[0,1]| > |\mathbb{Z}^+|$ because we can't count the reals using the positive integers.

Generalizing uncountability

Theorem (Countable Subsets)

Let $B \subseteq A$. If A is countable, then B is countable.

Theorem (contrapositive)

Let $B \subseteq A$. If B is uncountable, then A is uncountable.

By the contrapositive, if $[0,1]$ is uncountable, and $[0,1] \subseteq \mathbb{R}$, then $\mathbb{R}$ is uncountable.

Continuum Hypothesis and $\aleph_0$

Is $|\mathbb{R}| > |[0,1]|$?

Continuum hypothesis

There is no set whose cardinality is strictly between that of the integers and the real numbers.

Symbolically, $\aleph_0$ is the "small" infinite (countable) and the "large" infinite of real numbers is c (the continuum). The question is, does $\aleph_1 = c$, as in the next infinite class (above small) already reaches the continuum.

This is one of the great unproven hypothesis in mathematics, as stated by Gregor Cantor in 1878.

Exercise

Is the following countable or uncountable?

$\mathbb{Z}^+ \times \{1, 2\}$

$\mathcal{P}(\mathbb{Z}^+)$