MATH 287:

Mathematical Proofs and Methods

Brennan Becerra

Fall, 2023

Lecture 2

Brennan Becerra

2023-08-24

Defining Mathematical Proof

Propositional Symbols:

$P = \{p_1, p_2, \ldots, p_n\}$

denote statements.

Examples:

- 3 is a prime number
- If x then y
- The sky is red means the ground is made of bananas

Connectives:

- $\land$ ("and")
- $\lor$ ("or")
- $\neg$ ("not")
- $\implies$ "if, then"

Example: $p_1 \land p_2 \lor p_3$ is ambiguous however. We must distinguish characteristics of statements with parentheses.

Propositional Logic Language

Propositional logic language $\mathcal{L}_P$ denotes all finite sequences that can be built from the alphabet consisting of all the propositional, and connective symbols

$$\mathcal{L}_p := P \cup \{\land, \lor, \neg, \implies, (,)\}$$

Example:

1. $\neg\neg\neg\neg$
2. $p_1 \neg \wedge)()p_5 \neg\neg$

We next identify/define the meaningful members of $\mathcal{L}_p$. We will do this via the *well-formed formula*.

Well-Formed Formula

Let Ψ be an element of $\mathcal{L}_p$. Ψ is a well formed formula, if

1. $\Psi \in P$
2. Ψ is $\neg\Phi$ where Φ is a well-formed formula.
3. Ψ is $\Phi \wedge \Gamma$ where Φ, Γ are well-formed formula.
4. Ψ is $(\Phi \vee \Gamma)$ where Φ, Γ are well formed-formula.
5. Ψ is $(\Phi \implies \Gamma)$ where Φ, Γ are well-formed formula

$$\mathrm{WFF}_P = \{\Phi \in \mathcal{L}_p : \Phi \text{ is a well formed formula.}\}$$

Examples:

- $(\neg p_5)$
- $(p_{17} \wedge (\neg p_5))$
- $(p_{23} \vee (p_{17} \wedge (\neg p_5)))$

Truth Values

The set of truth values is $\{\mathrm{T}, \mathrm{F}\}$. Consider the assignment of truth values to proposition symbols

$p_1, p_2, \ldots$

$$A : P \to \{\mathrm{T}, \mathrm{F}\}$$

(A is a function)

Extension of A to $\mathbf{WWF}_P$ is as follows:

Let Φ and Ψ be well formed formulae, for which the values of A are known.

Consider the following:

$A(\neg\Phi)$

Φ	$\neg\Phi$
T	F
F	T

$A(\Phi \wedge \Psi)$

Φ	Ψ	$\Phi \wedge \Psi$
T	T	T
T	F	F
F	T	F
F	F	F

$A(\Phi \vee \Psi)$

Φ	Ψ	$\Phi \vee \Psi$
T	T	T
T	F	T

Φ	Ψ	$\Phi \vee \Psi$
F	T	T
F	F	F

$A(\Phi \implies \Psi)$

Φ	Ψ	$\Phi \implies \Psi$
T	T	T
T	F	F
F	T	T
F	F	T

These represent the functional values of A as truth tables.

Contradictions and Tautologies

Contradiction

A contradiction is a well-formed formula with truth value F for <u>all</u> truth assignments.

- $(p_1 \wedge (\neg p_1))$

Tautology

A tautology is a well-formed formula with truth value T for <u>all</u> truth assignments.

- $(p_1 \vee (\neg p_1))$

- Note that propositions can <u>NOT</u> be a tautology
- Tautologies, propositions and contradictions are disjoint "sets" in $\mathbf{WWF}_P$

Big epic takeaway of the day:

$P \subset \mathbf{WWF}_P \subset \mathcal{L}_P$ (more or less, don't overthink it)

Lecture 3

Brennan Becerra

2023-08-29

Consider the following:
$\phi := ((p_1 \lor (p_2 \land (\neg p_1))) \lor ((\neg p_2) \land p_1))$

We checked that this statement, ϕ is well-formed formula. Is ϕ a tautology? We can check by substituting truth values for p_1, p_2 in a truth table.

p_1	p_2	ϕ
T	F	T
T	T	T
F	T	F
F	F	

In the case where $p_1 = F, p_2 = T$ ϕ is in fact false, so we can see that ϕ is <u>not</u> a tautology or a contradiction(since there are outcomes where ϕ is true).

Let S be a set of well-formed formulae, such that there are truth value assignments A such that each element of S has a truth value of T.

Let ϕ be a well-formed formula. Do all truth value assignments that makes each element of S true, also make ϕ true?

<u>Notion of a formal system:</u>

For some Language $\mathcal{L}_p$ consider WWF_P of that language. Fix a set $H \subset WWF_P \setminus \textbf{contradiction}_P$. H will be called the axioms of the formal system.

Rule of Deceleration: "Modes Podens" From $A \wedge (A \implies B)$, deduce B.

(Intuitive justification, but you can prove it with a truth table)

A	B	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

Deduction

A *deduction* in this formal system is a finite sequence

$$\phi_1, \phi_2, \ldots, \phi_k$$

of well formed formulae such that;

1. ϕ_i is an axiom, or
2. there are $\phi_j \wedge \phi_l$ with $l, j < i$ such that ϕ_l is $(\phi_j \implies \phi_i)$

Example:$\phi_1, \ldots, \phi_j, \ldots, \underbrace{\phi_l}_{\phi_j \implies \phi_i}, \ldots, \phi_i, \ldots$

Theorem

ϕ_k is said to be a <u>Theorem</u> of the formal system. The sequence

$$\phi_1, \phi_2, \ldots, \phi_k$$

is said to be a <u>proof</u> of ϕ_k.

Lecture 4

Brennan Becerra

2023-08-31

> ✎ **Satisfiability**
>
> Instance: A finite set S of well-formed formulae of $\mathcal{L}_P$.
> Question: Is there a truth assignment A for the propositions of the language P such that each well-formed formula in S has a truth value of T.

Consider the following:

$\phi_1 : (p_1 \vee p_2) \wedge (\neg p_3)$ $\phi_2 : ((\neg p_1) \wedge (\neg p_3)) \wedge p_4$
$\phi_3 : ((p_1 \implies p_2) \vee (p_3 \wedge p_4))$
$\phi_4 : ((((\neg p_4) \implies p_1) \wedge)(p_2 \implies p_3)) \vee (\neg p_3)$

$S = \{\phi_1, \phi_2, \phi_3, \phi_4\}$.

The question whether or not there is a truth assignment for the members of P such that each formula in S has the truth value of T.

Satisfiablility problem:

(1971) Cook: Satisfiability problem is *NP complete*.

> ✎ **NP Complete**
>
> 1. Given a truth assignment, it can be verified in *polynomial time* whether each element of S has truth value T for this truth assignment.
>   and

2. Coming up with a truth assignment that confirms "yes" is not polynomial time.
3. This decision Problem can be used to answer any other decision problems satisfying 1 and 2.

Polynomial Time

Polynomials that can measure the complexity of an algorithm and the number of steps it takes to complete them.

Lecture 5

Brennan Becerra

2023-09-05

Set

We can define a *set* as a collection of objects.

$$S = \{s_1, \ldots, s_n\}$$

- Order doesn't matter
- No repetitions of objects allowed

Example:

$\{2,5,1,3,4\} \equiv \{5,2,3,4,1\} \equiv \{1,2,3,4,5\}$

Subset

Let A, B be sets. We call $A \subseteq B$ if each object present in A is also present in B .

$$(\forall x \in A) : (x \in B)$$

If A, B have the same elements, we say A is equal to B and we write

$$A = B.$$

If $A \neq B$ we know they are not equal. Suppose A is a subset of B and they are not equivalent, then we know

$$((A \subseteq B) \wedge (A \neq B))$$

we write $A \subset B$. $A \subsetneq B$ is also sufficient.

> ### ✎ Power Set
>
> For a set A, the set of all subsets of A is called the *power set* of A and is denoted $\mathcal{P}(A)$.
>
> $$\mathcal{P}(A) = \{B : B \subseteq A\}$$

Notation: $\emptyset$ denotes the set with no elements, the *empty set*.

Claim: For any set A, $\emptyset \subseteq A$.

proof

Let A be a set. We must show that $\emptyset \subseteq A$, $(\forall x)(x \in \emptyset) \implies (x \in A)$ is true. Thus, let x be the given. We must show that

$$(x \in \emptyset) \implies (x \in A)$$

holds true.

Recall

p_1	p_2	$p_1 \implies p_2$
T	T	T
T	F	F
F	T	T
F	F	T

We focus on the last line of this truth table. Since x cant be in the $\emptyset$ i.e. $(x \in \emptyset)$ is false, we know that x can or cannot be in A. Whether or not $x \in A$ our truth value of this statement holds <u>true</u>, therefore $\emptyset \subseteq A$.

Since A was arbitrary, for any set A, $\emptyset \subseteq A$. $\square$

Back to $\mathcal{P}(A) \equiv \{B : B \subseteq A\}$.

Examples:

1. $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1,2,3\}, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,$
2. $\mathcal{P}(\{a,b,g\}) = \{\emptyset, \{a,b,g\}, \{a\}, \{b\}, \{g\}, \{a,b\}\{b,g$

Question:

Consider: $\mathcal{P}(\mathcal{P}(\{1,2,3\}))$ How many element?

Notation: For a set A,

$$|A|$$

denotes the number of elements in A, or its cardinality.

$|\mathcal{P}(\mathcal{P}(\{1,2,3\}))| = 2^8 = 256.$

We know this because $|\{1,2,3\}| = 3, |\mathcal{P}(\{1,2,3\})| = 8.$

Consider the set S,

$$S = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8\}.$$

1	2	3	4	5	6	7	8
0	1	0	1	1	0	0	1

yields $\{2,4,5,8\}$.

1	2	3	4	5	6	7	8
0	1	1	0	0	0	1	1

yields: $\{2, 3, 7, 8\}$.

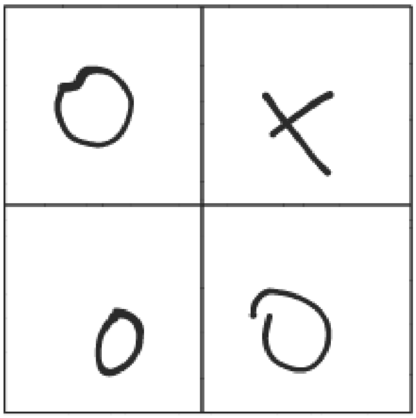
How many ways can we create subsets of length 8? Well obviously, since we have two options, it would be 2^8.

Theorem

Let S be a finite set. Then

$$|\mathcal{P}(S)| = 2^{|S|}.$$

proof



upcoming...(pigeon hole principle)

More methods for building "new" sets from given sets

Union

Let sets A, B be given.

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}$$

"A *union* B"

- How is $A \cup B$ related to $|A|$ and $|B|$?

Theorem (Inclusion - Exclusion Principle)

If A and B are finite sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Intersection

$$(A \cap B) = \{x : ((x \in A) \wedge (x \in B))\}$$

is called the *intersection* of A, B.

Symmetric Difference

$$(A \Delta B) = \{x : ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x$$

Is called the symmetric difference

Definition

$$A \setminus B$$

Reads as A without B

Lecture 6

Brennan Becerra

2023-09-07

What We Have So Far

Set: $A, B, \mathbf{C}..$

"new" sets:

- $\mathcal{P}(A)$
- $A \cup B$
- $A \cap B$
- $A \setminus B$
- $A \Delta B$

Specific Sets:

- $\emptyset$

Exploration

Consider a set A. $A \neq \emptyset$. We know $\emptyset \in \mathcal{P}(A)$. We can think of $[\cup, \cap, \setminus, \Delta]$ as set operations.

For any element $B \in \mathcal{P}(A)$ we know:

- $\emptyset \cup B = B$
- $\emptyset \cap B = \emptyset$
- $\emptyset \Delta B = B$
- $A \cup B = A$
- $A \cap B = B$
- $A \Delta B = A \setminus B$

$A = \{1, 2, 3, 4\}$
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}\{1, 3\}, \{1, 4\}, \{2, 3\}$
Are there operations on this set for which a special element plays the role of 'zero' and 'one' under set operations?

Facts

For any sets A, B, C

1. $A \cap B = B \cap A$ ($\cap$ is commutative)
2. $A \cup B = B \cup A$ ($\cup$ is commutative)
3. $A \Delta B = B \Delta A$ (Δ is commutative)
4. $A \setminus B \neq B \setminus A$ ($\setminus$ is not commutative)
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

proof of 5.

$$(1) \qquad (\forall x)((x \in (A \cap (B \cup C))) \implies (x \in (A \cap B) \cup$$

$$(2) \qquad (\forall x)(x \in (A \cap B) \cup (A \cap C)) \implies (x \in (A \cap$$

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

If $x \in (A \cap (B \cup C))$ is <u>FALSE</u>, then (1) has a truth value of <u>TRUE</u>. Then consider the case where $x \in A \cap (B \cup C)$ is <u>TRUE</u>.

Suppose that contrary to the claim that (1) is TRUE, the statement $x \in (A \cap B) \cup (A \cap C)$ is FALSE. Then $x \in (A \cap B) \cup (A \cap C)$ being false yields the fact that:

$$x \notin (A \cup B) \text{ and } x \notin (A \cup C)$$

is true. That is to say,

$$\begin{array}{ll} (a.) & x \notin (A \cap B) \text{ is true} \\ (b.) & x \notin (A \cap C) \text{ is true} \end{array}$$

thus, by (a.) $x \notin A$ is true, or $x \notin B$ is true. Similarly, by (b.) $x \notin A$ is true or $x \notin C$ is true.

<u>Case 1:</u> $x \notin A$ is true.

Then, $x \in A \cap (B \cup C)$ is false. This yields a contradiction to

$$x \in A \cap (B \cup C)$$

Thus, $x \notin A$ is false, where $x \notin B$ is true, and $x \notin C$ is true. Thus, $x \notin B \cup C$ is true. This implies that $x \in B \cup C$ is false. But then $x \in A \cap (B \cup C)$ is false, contradicting the truth of

$$x \in A \cap (B \cup C)$$

yet again. By contradiction, we can infer that 5. is true. $\square$

Proof of 2: left to the student.

(2) $(\forall x)(x \in (A \cap B) \cup (A \cap C)) \implies (x \in (A \cap (B \cup$

Q	P	$Q \implies P$
T	T	T
T	F	F
F	T	T
F	F	T

Lecture 7

Brennan Becerra

2023-09-12

Recap

We consider $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

1. $(\forall x)(x \in A \cap (B \cup C)) \implies (x \in (A \cap B) \cup (A \cap$
2. $(\forall x)((x \in (A \cap B) \cup (A \cap C)) \implies (x \in A \cap (B \cup$

We want to show that we have some $p_1 \land (p_2 \lor p_3)$ and show that it has the same truth value as $(p_1 \land p_2) \lor (p_1 \land p_3)$

So we can create truth tables

$p_1 \land (p_2 \lor p_3)$

$(p_1 \land p_2) \lor (p_1 \land p_3)$

and show that they are the same.

Product of sets

Given: Two sets, A, B. We wish to define the *product* of A and B. We denote this $A \times B$,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

Example:

$A = \{2, 3, 5, 7\}$ $B = \{10, 15, 20, 35, 70\}$

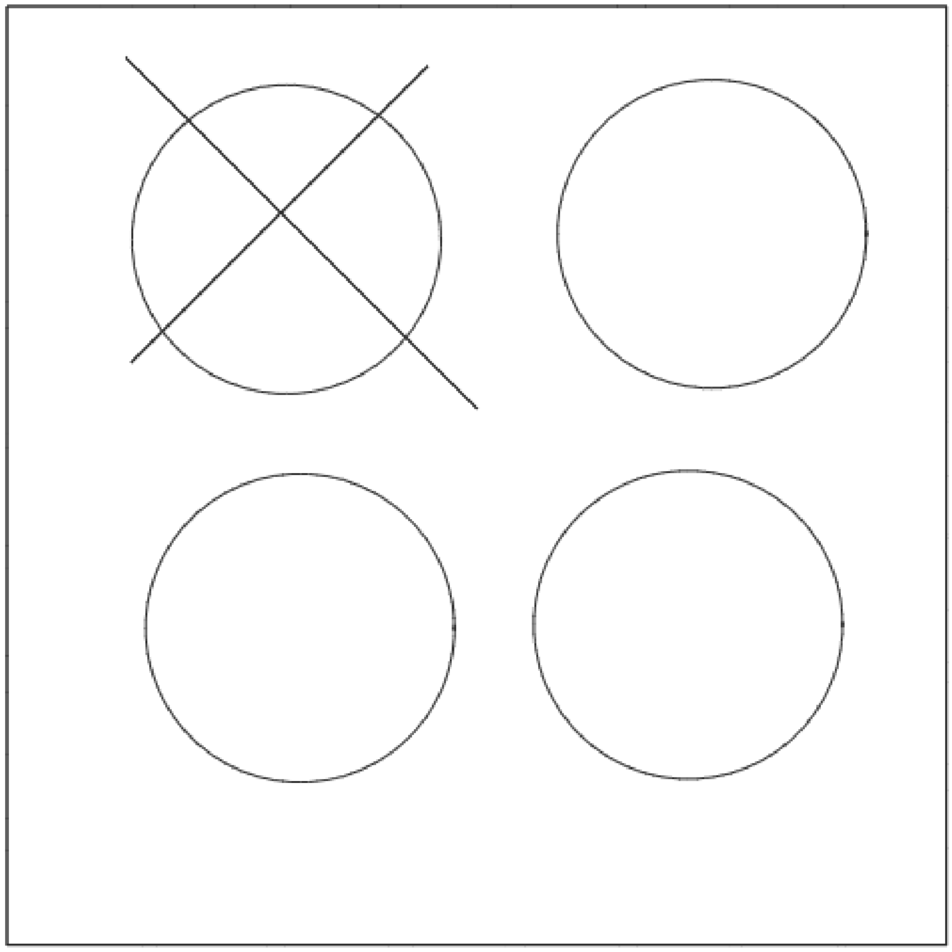
$A \times B = \{(2, 10), (2, 15), (2, 20), (2, 35), (2, 70), (2, 10),$
$(3, 15), (3, 20), (3, 35), (3, 70),$
$(5, 10), (5, 15), (5, 20), (5, 35), (5, 70), (7, 10), (7, 15), (7,$

Theorem

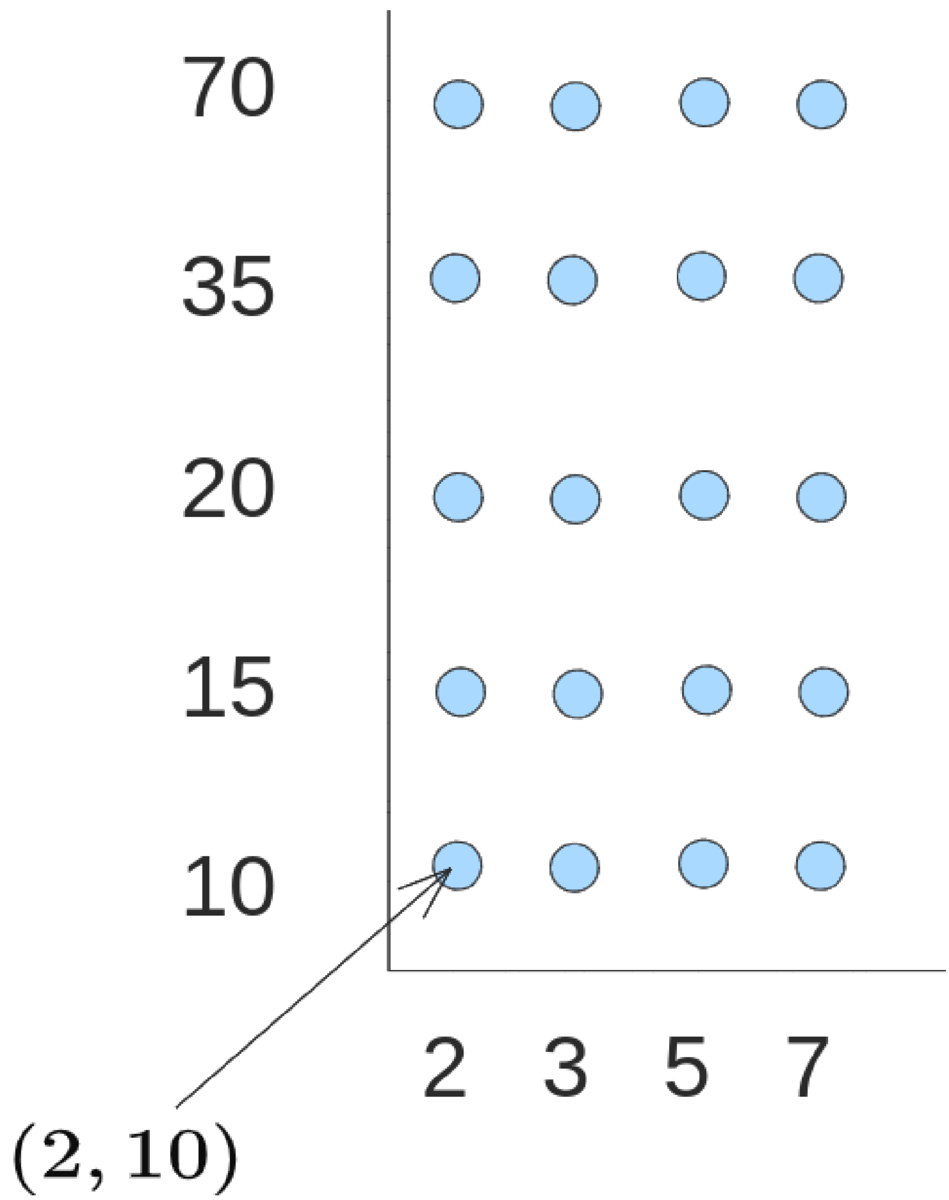
For finite sets A, B

$$|A \times B| = |A| \cdot |B|.$$

proof



Visual Representation



Subsets of $A \times B$:

$C = \{(a, b) \in A \times B : a \mid b\}$

$D = \{(a, b) \in A \times B : a < b\} = A \times B$

Binary Relations

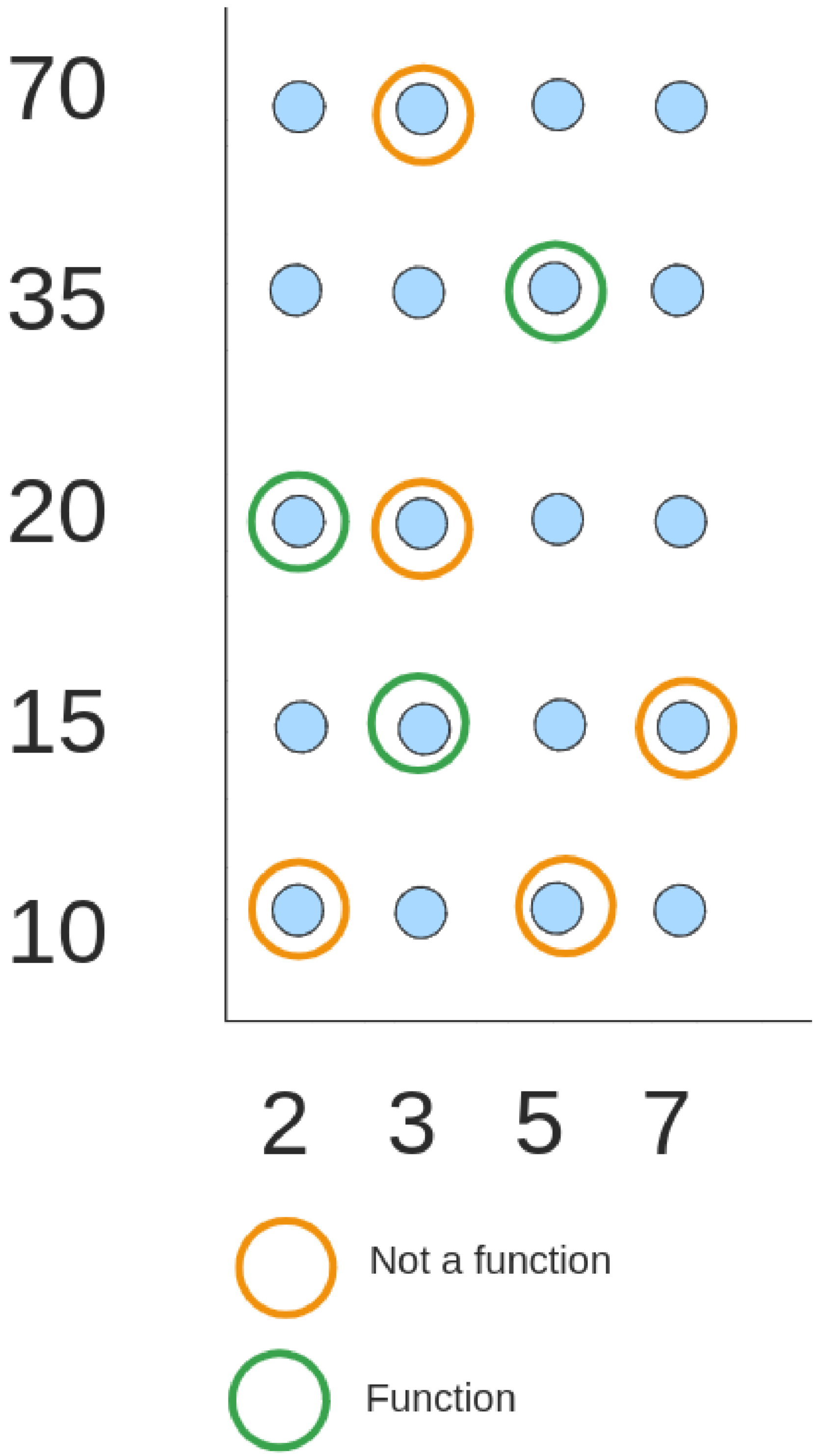
A subset of $A \times B$ is said to be a *binary relation* between A and B.

Definition

A subset $F \subseteq A \times B$ is said to be a *function* if for each $a \in A$,

$$|\{b \in B : (a, b) \in F\}| \leq 1$$

Example



Definition

Let $F \subseteq A \times B$, be a function

1. $\text{Domain}(F) = \{a \in A : \text{There is a } b \in B \text{ with } ($
$= \{a \in A : (\exists b)(b \in B \text{ and } (a, b) \in F)\}$
2. $\text{Range(F)} = \{b \in B : (\exists a)(a \in A \text{ and } (a, b) \in I$

We say F is a function from $\text{Domain}(F) \mapsto \text{Range}(F)$.

The domain of our green function is $\{2, 3, 5\}$ with a range of $\{10, 20, 35\}$.

Additional Concepts Correlated with Functions

1. One-to-one: F is said to be a one-to-one function, if for each $b \in \textbf{range}$ there is exactly one $a \in \textbf{domain}$ with respect to F.
2. Onto: Consider a function, $F \subseteq A \times B$, with a $C = \textbf{domain}(F)$. We say, $F : C \to B$. Note that $\textbf{range}(F) \subseteq B$. If $\textbf{range}(F) = B$, we say 'F is a function from C onto B.'
   > - It is always the case that F is a function from $\textbf{domain}(F)$ onto $\textbf{range(F)}$.
3. Into: F is a function from A into B if $A = \textbf{domain}(F)$ and $\textbf{range(F)} \subseteq B$.
4. Many-to-one: A function is many-to-one if it is not one-to-one.

Cardinality

Let A, B be sets. We say "A and B have the same number of elements" if there is a function, $f : A \to B$ such that f is one-to-one and onto. Alternatively, we say "A and B have the same cardinality."

Lecture 8

Brennan Becerra

2023-09-14

one-to-one function

Let A, B be sets. We say that B has at least as many elements as A if there is a *one-to-one function* from A to B.

$$|A| \leq |B|$$

" A has no more elements than B. "

<u>Examples:</u>

$\mathbb{N} = \{n : n \text{ is a positive integer}\}.$
$\mathbb{Z} = \{n : n \text{ is an integer}\}$ $\mathbb{E} = \{\text{set of even integers}\}$
$\mathbb{Q} = \{\text{Set of Rational numbers}\}$ $\mathbb{R} = \{\text{Real numbers.}\}$

1. Do $\mathbb{N}$ and $\mathbb{Z}$ have the same number of elements?

$\mathbb{Z}$	$\mathbb{N}$
...	...
4	10
3	8
2	6
1	4
0	2
-1	1
-2	3
-3	5
-4	7
...	...

$$f(m) = \begin{cases} 2 \text{ if} & m = 0 \\ 2(m+1) \text{ if} & m > 0 \\ 2|m| - 1 \text{ if} & m < 0 \end{cases}$$

This function is one-to-one and onto.

2. Do $\mathbb{R}$ and $(-1,1)$ have the same number of elements? Define a function, f, such that, $f:\mathbb{R}\to(-2,1)$. Consider the function

$$g(x) = \frac{x}{x^2+1}$$

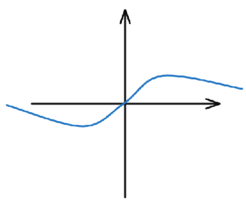
a. Is g a function from $\mathbb{R}\to(-1,1)$?

Yes!

b. Is g one-to-one?

$$g'(g) = \frac{(x^2+1)-x(2x)}{(x^2+1)^2} = \frac{1-x^2}{(x^2+1)^2}$$

$g'(x)$ is 0 at $-1, 1$, it is not one to one.



c. Is g onto?

Define $h:(1,\infty)\to(0,1/2)$ by

$$h(x) = \frac{x}{x^2+1}$$

$$h'(x) = -\frac{x^2}{(1+x^2)^2} < 0 \text{ on } (1,\infty),$$

so $h(x)$ is one-to-one. We can infer that $|(1,\infty)| \leq |\left(0, \frac{1}{2}\right)|$.

We can define our function as follows

$\mathbb{R}$	Function	$(-1,1)$
$(1,\infty)$		$\left(0, \frac{1}{2}\right)$
$(-\infty,-1)$	$h_2(x) = \frac{x}{1+x^2}$	$\left(-\frac{1}{2}, 0\right)$
$(-1,0]$	$h_3(x) = \frac{1}{2}x - \frac{1}{2}$	$\left(-1, -\frac{1}{2}\right]$
$(0,1]$	$h_4(x) = -\frac{1}{2}x + 1$	$\left[\frac{1}{2}, 1\right)$

Lecture 8

Brennan Becerra

2023-09-19

1. Followup on $\mathbb{R}$ and $(-1, 1)$
2. $\mathbb{N}$ and $\mathbb{R}$
3. $\mathbb{N}$ and the rational numbers between 0 and 1
4. $P(\{1, 2, 3, \ldots, m\})$ and $\{(i_1, i_2, \ldots, i_n) \mathbf{i}_j \in \{0, 1\} \text{ for } 1 \leq j \leq n\}$

2.

a) Is there a one to one function from one of $\mathbb{N}, \mathbb{R}$ to the other?

Yes $f : \mathbb{N} \to \mathbb{R} : n \mapsto f(n) = n$ is one-to-one.

b. Is there a one-to-one function from $\mathbb{N}$ to $\mathbb{R}$ that is onto?

(Cantor) No.

proof

Let g be any one-to-one natural function, such that $g : \mathbb{N} \to \mathbb{R}$. List the values of g in decimal form as follows:

$$\begin{aligned} g(1) &= n_1.\, \underline{a_{11}} a_{12} a_{13} \dots a_{1k} \dots \\ g(2) &= n_2.\, a_{21} \underline{a_{22}} a_{23} \dots a_{2k} \dots \\ g(3) &= n_3.\, a_{31} a_{32} \underline{a_{33}} \dots a_{3k} \dots \\ &\vdots \\ g(m) &= n_m.\, a_{m1} a_{m2} a_{m3} \dots a_{mk} \dots \\ &\vdots \end{aligned}$$

Note that $a_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for any i, j. Define decimal number

$$r = 0.r_1 r_2 r_3 \dots r_m \dots$$

as follows:

for $1 \leq j < \infty$,

$$r_j = \begin{cases} 1 & \text{if } a_{ij} \neq 1 \\ 2 & \text{otherwise.} \end{cases}$$

Claim: $r \neq g(n)$ for all $n \in \mathbb{N}$.

Proof of the claim: We rely on the induction Axiom.

$$S = \{n \in \mathbb{N} : r_{nn} \neq a_{nn}\}$$

Claim: $S = \mathbb{N}$.

1. $1 \in S$ is true by definition of r_{11}.
2. We must check the statement "If $n \in S$, then $n+1 \in S$"

P	Q	$P \implies Q$
T	T	T
T	F	F $\leftarrow$
F	T	T
F	F	T

Again, we are only concerned with the second line. But by definition, $r_{n+1\,n+1} \neq a_{n+1\,n+1}$ So by the $\implies$ truth table,

"If $n \in S$ then $n+1 \in S$ is true."

Since S satisfies 1. and 2. the induction Axiom gives that $S = \mathbb{N}$. It follows that g is not onto. Thus, $|\mathbb{N}| < |\mathbb{R}|$.

Claim: $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$

Proof: First note that there are one-to-one functions from $\mathbb{N} \to \mathcal{P}(\mathbb{N})$ for example,

$$g : \mathbb{N} \to \mathcal{P}(\mathbb{N}) : n \mapsto g(n) = \{n\}.$$

Thus, $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$. So now consider any one-to-one function,

$$h : \mathbb{N} \to \mathcal{P}(\mathbb{N}).$$

Define a set $S \subset \mathbb{N}$ as follows: $n \in S$ if and only if $n \notin h(n)$. Then, $S \neq h(n)$ for all n allowing us to conclude that h is not onto. Thus,

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$$

- How about $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$?
- Is there a set, S such that $|\mathbb{N}| < |S| < |\mathcal{P}(\mathbb{N})|$
- $|\mathbb{N}| < |S| < \mathbb{R}$?

Lecture 10

Brennan Becerra

2023-09-21

✎ Schroeder-Bernstein Theorem

Let A, B be sets. The following are equivalent:

1. There is a one-to-one and onto function:

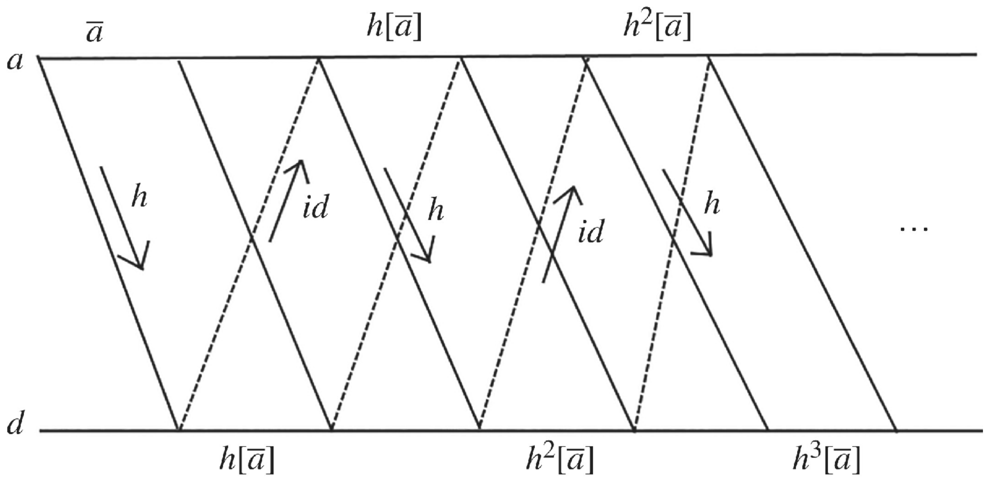
$$f : A \to B$$

2. (a.) There is a one-to-one function:

$$g : A \to B$$

(b.) There is a one-to-one function:

$$h : B \to A$$



First Some Examples

Example 1.

Recall: For sets A, B $A \times B = \{(a, b) : a \in A, b \in B\}$.

Claim: $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ have the same number of elements. That is, there is a one-to-one and onto function,

$$f : \mathbb{N} \to \underbrace{\mathbb{N} \times \mathbb{N}}_{\mathbb{N}^2}.$$

proof:

1. $h : \mathbb{N} \to \mathbb{N}^2 : n \mapsto h(n) = (n, n)$ is one-to-one.
2. We define a function $g : \mathbb{N}^2 \to \mathbb{N}$ by $g(m, n) = 2^m \cdot 3^n$.

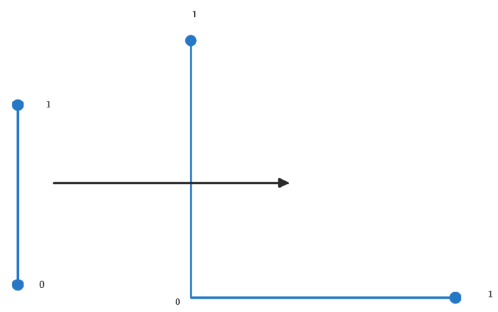
   <u>Claim:</u> g is one-to-one.

   proof: Suppose we have two pairs, $(m_1, n_1), (m_2, n_2)$ such that $g(m_1, n_1) = g(m_2, n_2)$. Thus, $2^{m_1} \cdot 3^{n_1} = 2^{m_2} \cdot 3^{n_2}$. Notice that if we continue to divide by 2 on both sides, we must 'run-out' of twos at the same time. The same thing could be said about 3. By unique prime factorization, $m_1 = m_2$ and $n_1 = n_2$, so $(m_1, n_1) = (m_2, n_2)$, therefore, g is one-to-one.

By *Schroeder-Bernstein Theorem,* there is a one-to-one and onto function from $\mathbb{N} \to \mathbb{N}^k$ for any $k \in \mathbb{N}$.

Example 2.

Is there a one-to-one and onto function from $(0,1) = \{x \in \mathbb{R} : 0 < x, 1\}$ to $(0,1)^2$?



proof of Schroeder-Bernstein Theorem

First some facts:

If $f : A \to B$ is one-to-one and $g : B \to C$ is one-to-one, then $g \circ f : A \to C$ is one-to-one. Here, $g \circ f : A \to C$ is defined by $g \circ f(x) = g(f(x))$.

<u>Verification:</u> Suppose $x_1, x_2 \in A$ are such that $g \circ f(x_1) = g \circ f(x_2)$. That is to say, $g(f(x_1)) = g(f(x_2))$. Since g is one-to-one, $f(x_1) = f(x_2)$. Since f is one-to-one, $x_1 = x_2$. We can conclude that $g \circ f$ is one-to-one.

We first work on **2.** $\implies$ **1.** This will happen in two steps.

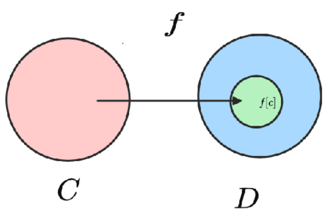
1. Restrict to the case when $B \subseteq A$.
2. No restriction on the relation between A and B beyond the assumptions of 2.

Notation

1. For a function $f : C \to D$, $f[c]$ denotes $\{f(x) : x \in C\}$
2. If f is a function from $C \to C$,

$$f^{n+1} : C \to C,$$

is $f \circ f^n : C \to C$, where $f' = f$. 3 $f^0(x) = x$, all $x \in C$.



Now the Step 1 Version:

Given sets, A, B with $B \subseteq A$ and $f : A \to B$ one-to-one. We must show there is a one-to-one and onto function from A to $B:$

$$A_0 = A = f^0[A]$$

Where $B \subseteq f^0[A]$,

$$B = f^0[B] = B_0$$

and $f^1[A] \subseteq B_0$,

$$f^1[A] = A_1$$

and $f^1[B] \subseteq A_1$

$$f^1[B] = B_1$$

...

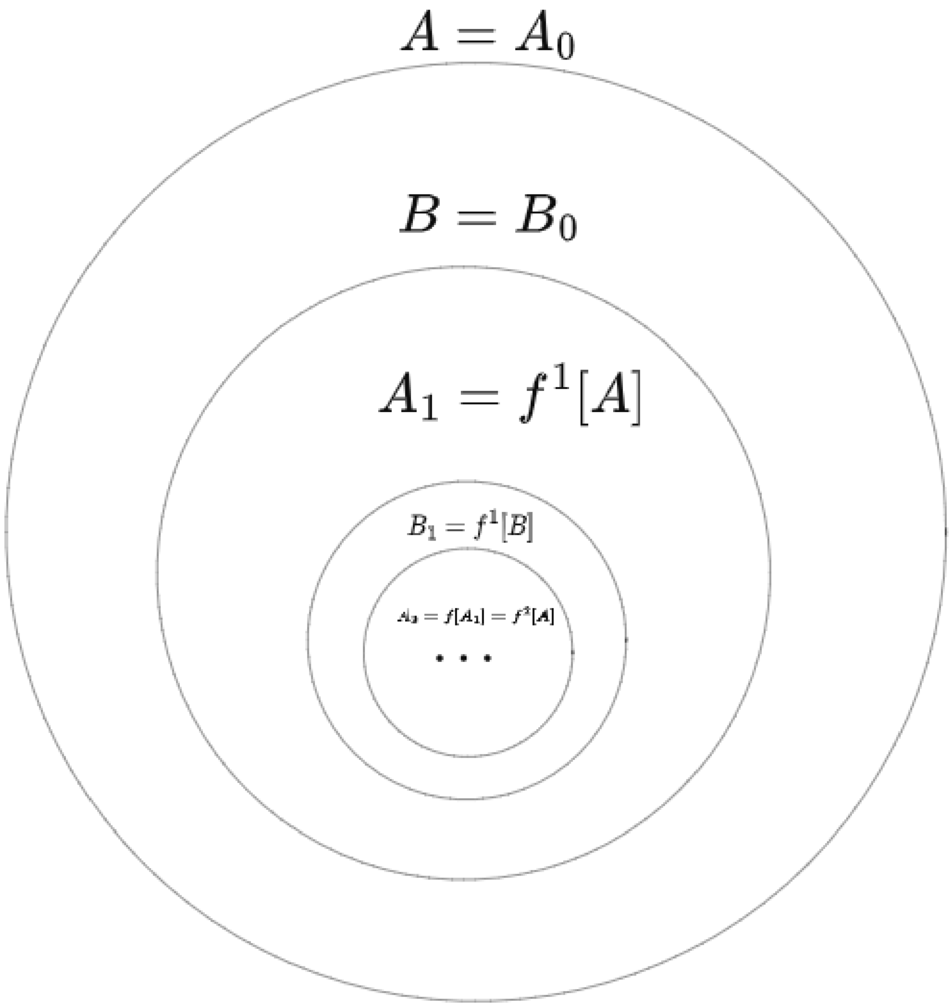
To be continued I guess.

Lecture 11

Brennan Becerra

2023-09-26

Step 1 Version Continued



Next, define the following sets:

- $H_0 = A_0 \setminus B_0$
- $H_1 = A_1 \setminus B_1$
- $H_2 = A_2 \setminus B_2$
- ...
- $H_n = A_n \setminus B_n$
- ...
- $K_0 = B_0 \setminus A_1$
- $K_1 = B_1 \setminus A_2$

- $K_2 = B_2 \setminus A_3$
- ...
- $B_n = B_n \setminus A_{n+1}$
- ...

Define some P, such that

$$P = \bigcap_{n=0}^{\infty} A_n = \bigcap_{n=0}^{\infty} B_n$$

$$A_0 \supseteq B_0 \supseteq A_1 \supseteq B_1 \supseteq \cdots \supseteq A_n \supseteq B_n \supseteq A_{n+1}$$

Note that

1. $(\forall_{n,j})(n \neq j)$ (a.) $H_n \cap H_j = \emptyset$ (b.) $K_n \cap K_j = \emptyset$ (c.) $H_n \cap K_j = \emptyset$ (d.) $H_n \cap P = \emptyset$ (e.) $K_n \cap P = \emptyset$
    - $H_n \cap H_{n+1} \equiv H_n \cap P$ more or less
2. $A = P \cup (\bigcup_{n=0}^{\infty} H_n) \cup (\bigcup_{n=0}^{\infty} K_n)$
3. $B = P \cup (\bigcup_{n=1}^{\infty} H_n) \cup (\bigcup_{n=0}^{\infty} K_n)$

Define $g : A \to B$ by the following:

Consider some $x \in A$.

$$g(x) = \begin{cases} x \text{ if } x \in P \cup (\bigcup_{n=0}^{\infty} K_n) \\ f(x) \text{ if } x \in \bigcup_{n=0}^{\infty} H_n. \end{cases}$$

- f maps an H_n 1-1 and onto H_{n+1}.
    - Recall $H = f^n[A] \setminus f^n[B]$

We claim g is 1-to-1 and onto.

1. g is 1-to-one.

Consider $x_1, x_2 \in A$. $x_1 \neq x_2$.

Case 1: $x_1, x_2 \in P \cup (\bigcup_{n=0}^{\infty} K_n)$, then $g(x_1) = x_1 \neq x_2 = g(x_2)$. Case 2: $x_1, x_2 \in \bigcup_{n=0}^{\infty} H_n$, then $g(x_1) = f(x_1) \neq f(x_2) = g(x_2)$ Case 3: $x_1 \in P \cup (\bigcup_{n=0}^{\infty} K_n)$ and $x_2 \in \bigcup_{n=0}^{\infty} H_n$. Then $g(x_1) = x_1 \in P \cup (\bigcup_{n=0}^{\infty} K_n)$ and $g(x_2) = f(x_2) \in \bigcup_{n=0}^{\infty} H_n$.

Thus $g(x_1) \neq g(x_2)$, so x_1, x_2 were arbitrary distinct elements of A, $g : A \to B$ is 1-to-1.

2. g is onto (connected)

   We consider any $y \in B$. We must now show that there is an $x \in A$ with $g(x) = y$. Case 1: $y \in P$, then $g(y) = y$ by definition of g, and so $x = y$ is an element of A with $g(x) = g(y) = y$.

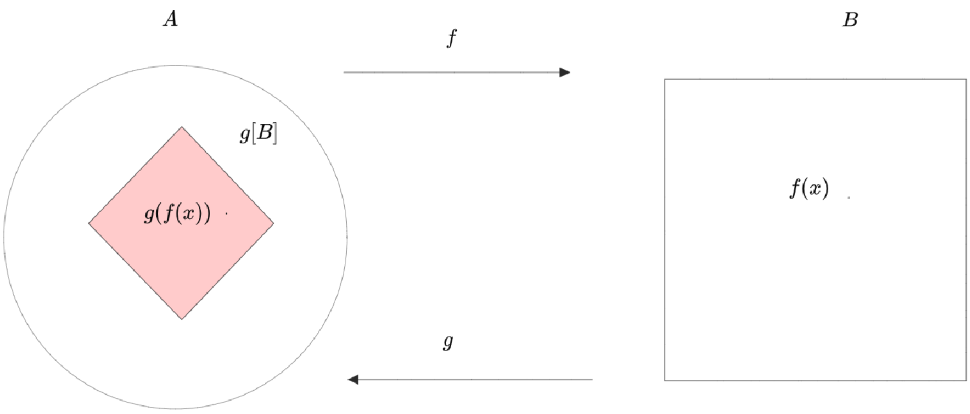
   Case 2: $y \in \bigcup_{n=1}^{\infty} H_n$: Fix an n with $y \in H_n$. Note that $n > 0$. By definition, of g, $y = f(x) = g(x)$ for an $x \in H_{n-1}$ (Check this... f maps H_{n-1} 1-1 and onto H_n, all n).

   Case 3: $y \in \bigcup_{n=0}^{\infty} K_n$. In this case, take x to be y. We find from definition of g, $g(x) = g(y) = y$.

Thus, for any $y \in B$, there is an $x \in A$ with $g(x) = y$. So g is onto! We can conclude that g is 1-to-1 and onto. $\square$

General Case:

Given Sets A, B and 1-to-1 functions, $f : A \to B$ and $g : B \to A$. We must now show that there is a 1-to-1 and onto function $h : A \to B$.



- $g : B \to g[B]$ is 1-to-1
- $g \circ f : A \to g[B]$ is 1-to-1

Proof:

Note that:

1. $f \circ g$ is one-to-one as f, g are one-to-one.
2. $\overline{B} = g[B] \subseteq A$ and $\ell : A \to \overline{B}$ given by $\ell = f \circ g$ is one-to-one. By step 1, we have a one-to-one and onto function, $m : A \to \overline{B}$.
3. $g : B \to \overline{B} = g[B]$ is one-to-one and onto, thus its inverse, g^{-1} on $\overline{B}$ and $g^{-1} : \overline{B} \to B$ is also one-to-one and onto. Thus $h = g^{-1} \circ m : A \to B$ is one-to-one and onto.

This is the completes the proof of the Schroeder-Bernstein theorem. $\square$

Lecture 12

Brennan Becerra

2023-09-28

Items of Consideration

1. $|\mathcal{P}(S)| = 2^{|S|}$ (S is finite)
2. If A, B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$
3. For finite sets, A, B $|A \times B| = |B| \cdot |A|$
4. $\mathbb{N}$ and the rational numbers between 0 and 1.
5. $\mathcal{P}(\{1, 2, \ldots, n\})$ and $\{(i_1, i_2, \ldots, i_n) : i_j \in \{0, 1\}, 1 \leq j \leq n\}$

5. $\mathcal{P}(\{1, 2, \ldots, n\})$ and $\{(i_1, i_2, \ldots, i_n) : i_j \in \{0, 1\}, 1 \leq j \leq n\}$

<u>Claim:</u>

Put $A = \mathcal{P}(\{1, 2, \ldots, n\})$ and $B = \{(i_1, i_2, \ldots, i_n) : i_j \in \{0, 1\}, 1 \leq j \leq n\}$.

We claim that $|A| = |B|$.

Proof

We wish to exhibit a one-to-one and onto function from A to B or B to A.

Define $F : B \to A$ so that $f((i_1, i_2, \ldots, i_n)) = \{j : 1 \leq j \leq n \text{ and } i_j = 1\}$

<u>Example:</u> $n = 4$

$$f((1, 0, 0, 1)) = \{1, 4\}$$
$$f((1, 1, 0, 0)) = \{1, 2\}$$
$$f((1, 1, 0, 1)) = \{1, 2, 4\}$$

<u>Claim 1:</u> f is one-to-one.

Proof

$x = (i_1, i_2, \ldots, i_n)$ and $y = (j_1, j_2, \ldots, j_n)$ are both elements of B where $x \neq y$. Since $x \neq y$, we could say that if we pick some $1 \leq \ell \leq n$, then, $i_\ell \neq j_\ell$.

$$(i_1, i_2, \ldots, i_\ell, \ldots, i_n)$$
$$(j_1, j_2, \ldots, j_\ell, \ldots, j_n)$$

Subcase 1: $i_\ell = 1, j_\ell = 0$, then $\ell \in f(i_1, \ldots, i_n)$ and $\ell \notin f(j_1, \ldots, j_n)$. So $f(i_1, \ldots, i_n) \neq f(j_1, \ldots, j_n)$ i.e. $f(x) \neq f(y)$.

Subcase 2: $i_\ell = 0, j_\ell = 1$. By the same reasoning, $f(x) \neq f(y)$.

Since $x \neq y$ in the domain of f were arbitrary, f is one-to-one.

<u>Claim 2:</u> f is onto. If you give me anything in the range, A, there is something in B that assigns to A. Let $y \in A$ be given. Recall that $A = \mathcal{P}(\{1, 2, \ldots, n\})$ so $y \subseteq \{1, 2, \ldots, n\}$.

Let $x \in B$ be the sequence, $(i_1, i_2, \ldots, i_\ell, \ldots, i_n)$, where

$$i_j = \begin{cases} 0 \text{ if } j \notin y \\ 0 \text{ if } j \in y. \end{cases}$$

$B = \{(i_1, i_2, \ldots, i_4) : i_j \in \{0, 1\}, 1 \leq j \leq 4\}$ and $A = \{s : s \subseteq \{1, 2, 3, 4\}\}$. $y = \{1, 3\}$. Put $x = (1, 0, 1, 0)$. By the definition of f and x, we have that $f(x) = y$. Clearly, we can see that f is onto, as $y \in A$ and was arbitrary.

1. $|\mathcal{P}(S)| = 2^{|S|}$.

Claim: $|\mathcal{P}(A)| = 2^{|A|}$.

Proof (by induction)

Suppose $|A| = 1$ such that $A = \{a_1\}$, thus $\mathcal{P}(A) = \{\{a\}, \emptyset\}$. So it can be concluded that $|A| = 2^1 = 2$. Our Inductive hypothesis is that $|S| = n$ and $|\mathcal{P}(A)| = 2^n$. Consider some set A', where A' is A with a new element added, call it a_{n+1}. We could say that $A' = \{a_1, \ldots, a_n, a_{n+1}\}$. Considering $\mathcal{P}(A')$, two types of sets arise, those containing a_{n+1} and those that do not. Allow B_i to represent any particular member of $\mathcal{P}(A)$ and notice that $|\mathcal{P}(A')| = |\mathcal{P}(A)| + |B_k \cup \{a_{n+1}\}|$ for all $k \in \mathbb{N}$, satisfying $1 \leq k \leq 2^n$. We can therefore conclude that $\mathcal{P}(A') = 2^n + 2^n = 2 \cdot_2^n = 2^{n+1}$. $\square$

Lecture 13

Brennan Becerra

2023-10-03

Claim: There is a one-to-one ant onto function between $\mathbb{N}$ and

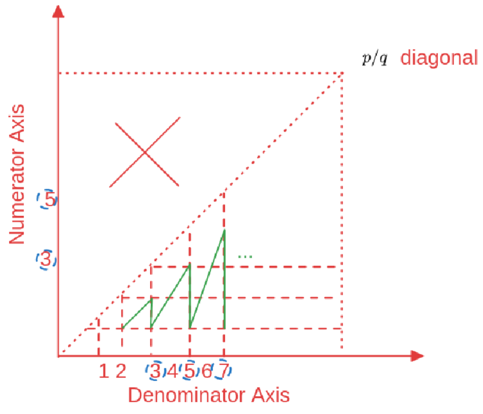
$\mathbb{Q} \cap (0,1) = \left\{ \frac{p}{q} : \gcd(p,q) = 1, 0 < p < q, \text{ and } p, q \in \mathbb{N}\right.$

Proof:

We can use the *Schroeder Bernstein Theorem.*

1. There is a 1-to-1 function from $\mathbb{N}$ to $\mathbb{Q} \cap (0,1)$. We will define some function $f : \mathbb{N} \to \mathbb{Q} \cap (0,1) : n \mapsto f(n) = \frac{1}{n+1}$. We claim that f is one-to-one: Suppose $m \neq n$ and $m, n \in \mathbb{N}$. We may assume that $m < n$. Now, $f(m) - f(n) = \frac{1}{m+1} - \frac{1}{n+1} = \frac{n-m}{(m+1)(n+1)}$. Since $m < n$, we can say that $\frac{n-m}{(m+1)(n+1)} > 0$, so $f(m) > f(n)$, so $f(m) \neq f(n)$.
2. There is a one-to-one function from $\mathbb{Q} \cap (0,1) \to \mathbb{N}$. We will define some function, $g : \mathbb{Q} \cap (0,1) \to \mathbb{N}$ by $g\left(\frac{p}{q}\right) = 7^p 11^q$. We claim that this function, g is one-to-one. Suppose $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q} \cap (0,1)$ and $g\left(\frac{p_1}{q_1}\right) = g\left(\frac{p_2}{q_2}\right)$, then $7^{p_1} 11^{q_1} = 7^{p_2} 11^{q_2}$. It must be the case that $p_1 = p_2$ and $q_1 = q_2$ for this to be true, therefore, $\frac{p_1}{q_1} = \frac{p_2}{q_2}$, so g is one-to-one.

   By the Schroeder-Bernstein Theorem, there is a one-to-one and onto function that exists between $\mathbb{N}$ and $\mathbb{Q} \cap (0,1)$.



- We call this Cantors Zig-zag Argument

More one-to-one and onto function stuff

One-to-one and onto functions from a set to itself.

Let M be a set. We wish to look at all the one-to-one and onto functions from the set to itself. We denote this

$$\text{Sym}\ (M) = \{f : f \text{ is a one-to-one and onto function fr}$$

We'll note that $f \in \text{Sym}(M)$ is also called a permutation of M, or a bijection of M.

<u>Examples:</u>

1. Say $M = \{1, 2, 3, 4\}$. We would like to look at the one-to-one and onto functions from $M \to M$.

These functions take the form $f : M \to M$

$$f(n) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ f(1) & f(2) & f(3) & f(4) & f(5) \end{pmatrix}$$

We will call the function h,

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

the *Identity function.*

Now consider

$$k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$$

$k \circ g$ could be defined by

$$k \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

What about $g \circ g$?

$$g \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

We can see that g defines its own inverse, such that $g = g^{-1}$.

Lecture 14

Brennan Becerra

2023-10-05

1. $(a)(\mathrm{sym}(\{1,2,3\}),\circ)_j$
   (2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ f(1) & f(2) & f(3) & f(4) & f(5) & f(6) \end{pmatrix} = f$
2. Groups - Identify inverses.
3.

1. $\text{sym}(\{1,2,3\}) = S_3$

We'll note that $|S_3| = 3 \cdot 2 \cdot 1 = 3!$

Can take the form:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$$

Our cases are:

$$\begin{aligned}
\text{id} &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\
f_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\
f_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\
f_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\
f_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\
f_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
\end{aligned}$$

$S_n = \text{sym}(\{1,2,3,\dots,n\})$ so $|S_n| = n!$

We'll note that $S_n = \{f : \{1,\dots,n\} \to \{1,\dots,n\} \mid \text{f is one-to-one and}$

$\circ$	Id	f_1	f_2	f_3	f_4	f_5
Id	Id	f_1	f_2	f_3	f_4	f_5
f_1	f_1	Id	f_3	f_2	f_5	f_4
f_2	f_2	f_5	Id	f_4	$f_4 \circ f_2 = f_3$	f_1
f_3	f_3	f_4	f_1	f_5	f_2	Id
f_4	f_4	f_3	f_5	f_1	Id	f_2
f_5	f_5	f_2	f_4	Id	f_1	f_3

Note that

$$f_5 = f_3 \circ f_3$$

and

$$(f_3 \circ f_3) \circ (f_3 \circ f_3) = f_5 \circ f_5 = f_3$$
$$f_3 \circ (f_3 \circ f_3) = f_5$$

(*Latin Squares*)

Example

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 2 & 4 \end{pmatrix}$$

- This function maps from a set of 6 elements and maps back to the same set

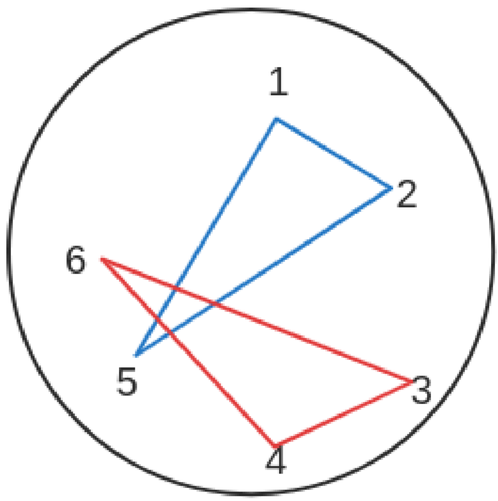
$$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$$

$$f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = id.$$

Disjoint Cycle Decomposition of f :

$$\begin{aligned} f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 2 & 4 \end{pmatrix} \\ &= (1 \quad 5 \quad 2) \circ (3 \quad 6 \quad 4) \\ &= (2 \quad 1 \quad 5) \circ (4 \quad 3 \quad 6) \end{aligned}$$

2 *Cycles*, each of length 3.



$$
\begin{aligned}
g &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 5 & 7 & 2 & 10 & 4 & 8 & 3 & 1 & 6 \end{pmatrix} \\
&= \underbrace{\begin{pmatrix} 1 & 9 \end{pmatrix}}_{2} \circ \underbrace{\begin{pmatrix} 2 & 5 & 10 & 6 & 4 \end{pmatrix}}_{5} \circ \underbrace{\begin{pmatrix} 3 & 7 & 8 \end{pmatrix}}_{3}
\end{aligned}
$$

so we can say that $\textbf{Order}(g) = \mathbf{30}$.

Lecture 15

Brennan Becerra

2023-10-10

1. Groups (G, Δ)
2. Order of an element.
3. Disjoint cycle decomposition and order.
4. Two cycle decomposition.

Group

A *group* is a pair, (G, Δ) where G is a set and Δ denotes a binary operation on G such that

1. For all $a, b \in G$, $A\Delta b \in G$. (G is closed under Δ)
2. There is an element $e \in G$ such that for any $a \in G$,

$$a\Delta e = a = e\Delta a$$

$$3 - 0 = 3 \neq 0 - 3$$

$$3 + 0 = 3 = 0 + 3$$

   (There is an identity element in G for Δ)
3. For every $a \in G$, there is a $b \in G$, such that

$$a\Delta b = id_g = b\Delta a.$$

4. For all $a, b, c \in G$, $(a\Delta b)\Delta c = a\Delta(b\Delta c)$, (i.e. Δ is associative)

Definition

An element, e of G, satisfying the requirement in G_2 is said to be an identity element for this operation, Δ on the set G.

Theorem

There can be only one identity element.

Proof.

Let $e, f \in G$ be such that for any $a \in G$, $e\Delta a = a = a\Delta e$ and $f\Delta a = a = a\Delta f$. In particular, $e\Delta f = f = f\Delta e$. ($e$ is an identity element). But f has the same operation as e. So we can say $f\Delta e = e$. This implies that $f = e$, such that there is only 1 element that can be classified as the identity element.

- Note that $G \neq \emptyset$
- Denote the *Identity Element* by id_G.

Definition

b is said to be an *inverse* of a if

$$a\Delta b = id_G = b\Delta a.$$

Theorem

For each a there is a unique b such that

$$a\Delta b = id_g = b\Delta a.$$

Proof

Fix $a \in G$. Suppose $b, c \in G$, such that $a \Delta b = id_G = b \Delta a$, and $a \Delta c = id_G = c \Delta a$. Now $b = b \Delta id_G = b \Delta (a \Delta c)$. $(b \Delta a) \Delta c = id_G \Delta c = c$.

<u>Example:</u> 2 - (3 - 4) = 3 but this is not the same as (2 - 3) -4 = -5.

Examples:

1. $\mathbb{Z}$ is the set of integers. $(\mathbb{Z}, +)$ is a group with identity element 0.
2. $(\mathbb{N}, +)$ is not a group as it does not have an identity element. G_1 holds and G_4 holds, but G_2 and G_3 fail.
3. $(S_3, \circ)$ is a group.

In general, for any n, $(S_n, \circ)$ is a group. More generally, $(\mathrm{Sym}(S), \circ)$ is a group.

<u>Next:</u> Cycle decomposition of elements of S_n.

<u>Example:</u>

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 7 & 1 & 6 & 11 & 5 & 2 & 9 & 4 & 3 & 9 \end{pmatrix} \in S_{11}$$

<u>Cycle decomposition:</u>

$$f = (1 \quad 10 \quad 3) \circ (2 \quad 7) \circ (4 \quad 6 \quad 5 \quad 11 \quad 8 \quad 9)$$

<u>Notes:</u>

1. The cycles are "disjoint" meaning that none moves items appearing in another cycle.
2. $\underbrace{f \circ f \circ \cdots \circ f}_{\text{How many?}} = id.$ $\qquad f^6 = id.$ $\qquad$ Note: $6 = \text{l.c.m.}\{2, 3, 6\}$

<u>Examples Continued:</u>

$$f = (1 \quad 10 \quad 3) \circ (2 \quad 7) \circ (4 \quad 6 \quad 5 \quad 11 \quad 8 \quad 9)$$

Just consider

$$(4 \quad 6 \quad 5 \quad 11 \quad 8 \quad 9).$$

$$(4 \quad 9) \circ (4 \quad 8) \circ (4 \quad 11) \circ (4 \quad 5) \circ (4 \quad 6)$$

Lecture 16

Brennan Becerra

2023-10-12

- Groups
- Order of an elements
- $(S_n, \circ)$ and disjoint cycle decomposition
- $(S_n, \circ)$ and 2-cycle representation
- A_n.
- Futurama...?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 2 & 3 & 4 & \dots & n \end{pmatrix}$$

$$\begin{aligned} (1 \quad 2) &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \\ (1 \quad 3) &\circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 6 & \dots & n \end{pmatrix} \end{aligned}$$

$$f = (a_1 \quad a_2) \circ (a_3 \quad a_4) \circ \dots \circ (a_{k-1} \quad a_k)(x)$$

Where for $i \neq j$, $(a_i, a_{i+1}) \neq (a_j, a_{j+1})$

<u>Example 1:</u>

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 5 & 2 & 1 & 4 & 3 & 7 \end{pmatrix}$$

$$= (1 \quad 6 \quad 4 \quad 2 \quad 8 \quad 7 \quad 3 \quad 5)$$

- Single cycle of length 8

$= (1 \quad 5) \circ (1 \quad 3) \circ (1 \quad 7) \circ (1 \quad 8) \circ (1 \quad 2) \circ (1 \quad 4) \circ$

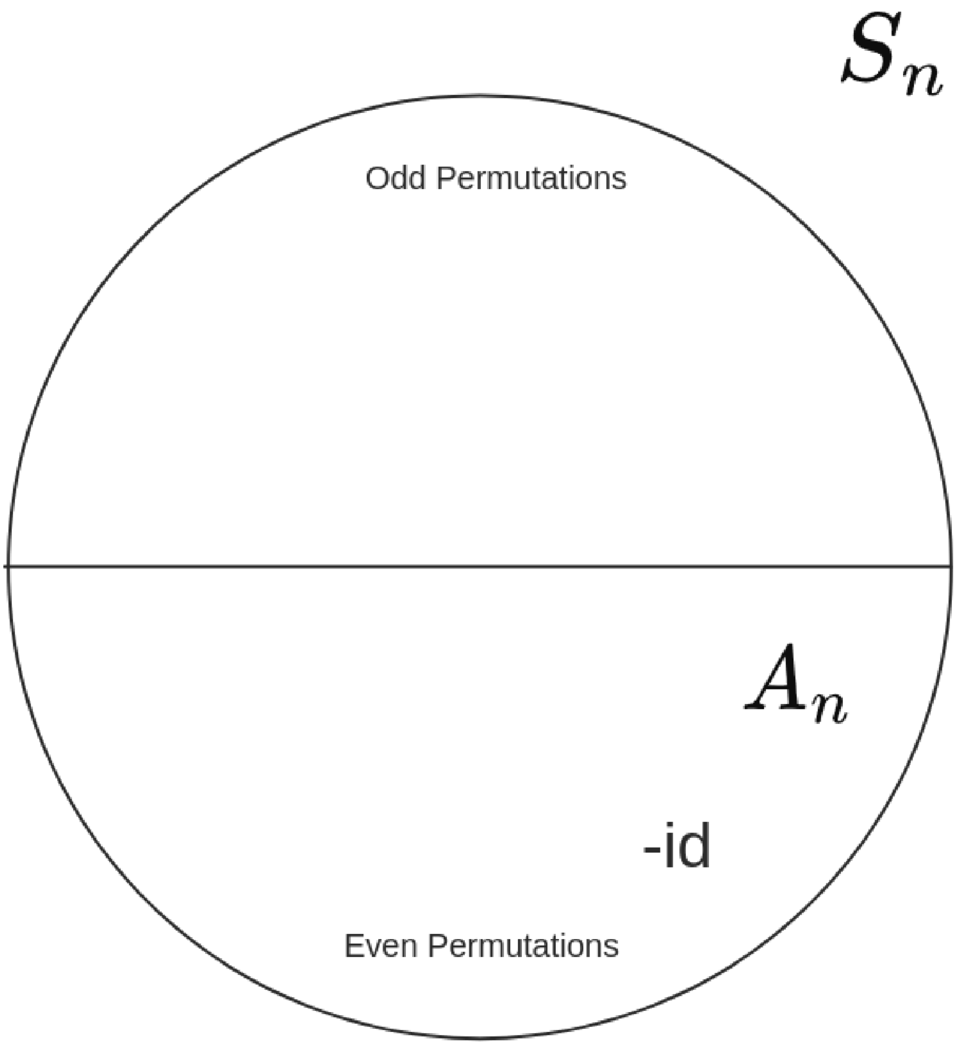
- We can plug some x into our composition, and get the same output as in g

Example 2:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 9 & 2 & 5 & 1 & 7 & 3 & 6 & 10 & 8 \end{pmatrix}$$
$$= (1 \quad 4 \quad 5) \circ (2 \quad 9 \quad 10 \quad 8 \quad 6 \quad 7 \quad 3)$$
$$= (1 \quad 5) \circ (1 \quad 4) \circ (2 \quad 3) \circ (2 \quad 7) \circ (2 \quad 6) \circ (2 \quad 8) \circ$$

- 8 2-cycles.

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = (\quad) \circ (\quad) \circ \cdots \circ (\quad)$$



$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 8 & 5 & 2 & 1 & 4 & 3 & 7 & 9 & 10 \end{pmatrix}}_{\text{7 2 - cycles}} \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 9 & 2 & 5 \end{pmatrix}}$$

- Even and odd composition $\implies$ odd composition
- Even and Even Composition $\implies$ even composition
- Odd and Odd Composition $\implies$ even composition

Emerging Facts:

1. Every permutation has a "unique" disjoint cycle decomposition.
2. We can write every cycle as a composition of 2-cycles. The parity of the number of 2-cycles in the compositions is invariant for each permutation.
3. The Identity permutation is a composition of zero 2-cycles - convention.
4. The set $A_n (\subseteq S_n)$ of even permutations is a group under composition.

Questions:

1. Given cycles

$(a_1 \quad \dots \quad a_n)$ and $(b_1 \quad \dots \quad b_m)$
when is
$(a_1 \quad \dots \quad a_n) \circ (b_1 \quad \dots \quad b_m) = (b_1 \quad \dots \quad b_m) \circ (a_1$

- Disjointedness

2. Prisoner of Benda Problem - When is it sufficient to use only the initial n parties to succeed in everyone recovering their own mind?

Lecture 17

Brennan Becerra

2023-10-17

Cycles and Cycle decomposition

Permutations: Fix a positive $n \in \mathbb{Z}^+$ and a container $S_n = \{f \mid f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is one-to-one and S_n has the operation, $\circ$ (composition of functions).

Special notation:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

$$= (1 \quad f(1) \quad f^2(1) \quad \ldots) \circ (i_i \quad f(i_1) \quad \ldots) \circ \cdots \circ ($$

Cycles

An element, $f \in S_n$ is said to by a cycle, if it has the following properties:

1. There is some x, for which $x \in \{1, \ldots, n\}$, for which $x \neq f(x)$.
2. Fix an x_0 as in (1.) For any $y \in \{1, \ldots, n\}$, such that $y \neq f(y)$, there is an m, such that $y = f^m(x_0)$.

Example:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 2 & 3 & 4 & 8 & 7 \end{pmatrix}$$

$$= \underbrace{(1 \quad 5 \quad 3)}_{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 4 & 3 & 6 & 7 & 8 \end{pmatrix}} \circ \underbrace{(2 \quad 6 \quad 4)}_{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 3 & 2 & 5 & 4 & 7 & 8 \end{pmatrix}} \circ (7$$

Theorem

For each $n \in \mathbb{N}$, each $f \in S_n$ can be written as a composition of disjoint cycles.

Disjoint

Let $f, g \in S_n$ both be cycles. f and g are disjoint if:

1. For each x such that $x \neq f(x)$, it is true that $x = g(x)$
2. For each x such that $x \neq g(x)$, it is true that $x = f(x)$.

If $n = 1$, each element of S_n is declared a cycle.

Equivalent Versions of the Induction Axiom

Induction Axiom

For a set, $S \subseteq \mathbb{N}$, if

1. $1 \in S$ is true and,
2. $n \in S \implies (n+1) \in S$, then, $S = \mathbb{N}$.

Strong Induction Axiom

For a set, $S \subseteq \mathbb{N}$, if

1. $1 \in S$, and
2. $1, 2, \ldots, n \in S \implies n+1 \in S$, then, $S = \mathbb{N}$.

Well Ordering Principle

For a set, $S \subseteq \mathbb{N}$, if $S \neq \emptyset$, then S has a smallest element.

Lecture 18

Brennan Becerra

2023-10-19

Topics Covered for The Exam

Lecture 19

Brennan Becerra

2023-10-26

Exam

Section	Values	Total	Averages
Individual	4 x 13	52	42.1
Collaborative	6 x 8	48	42.3

Question	c1	c2	c3	c4	c5	c6	I1	I2	
Correct	20	21	7	21	21	21	18	21	1

Topic 4: $\mathbb{R}$

Final:

10 questions 6-7 options.

Lecture 20

Brennan Becerra

2023-10-31

On the notion of symmetric groups

Cayley's Theorem

Let (G, Δ) and $(H, \square)$ be groups. A function $f : G \to H$ such that

1. f is one-to-one and onto
2. for all $a, b \in G,\ f(a\Delta b) = f(a)\square f(b)$ is said to be an *isomorphism.*

Consider a function

$$f = \underbrace{(\ )}_{3-\text{cycle}} \circ \underbrace{(\quad)}_{7-\text{cycle}}$$

$$\langle f \rangle = \{f, f^2, f^3, \ldots, f^{20}, e\}$$

Lecture 21

Brennan Becerra

2023-11-02

Topic 4: Real numbers, Sequences and Topology

1. Distance

- Metric/metric space

2. Order

- Bounds
- Least upper bound
- Greatest lower bounds
- Completeness Axiom

3. Sequences

- $f : \mathbb{N} \to \mathbb{R}$
- Limits
- Convergence

1. $F : S \to \mathbb{R}$, $S \subseteq \mathbb{R}$
    - Limits
    - Continuity

Distance

Metric

Let S be a given nonempty set. A function $d : S \times S \to [0, \infty)$ is said to be a *metric* (distance function) if:

1. $(\forall x \in S)(d(x, x) = 0)$
2. $(\forall_{x,y} \in S)(d(x, y) = d(y, x))$
3. $(\forall_{x,y,z} \in S)(d(x, z) \leq d(x, y) + d(y, z))$ (Triangle inequality)
4. $(\forall_{x,y} \in S)(d(x, y) \geq 0)$

For $S = \mathbb{R}$:

For $x \in \mathbb{R}$,

$$|x| = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0 \end{cases}$$

$|x|$ is said to be the "absolute value of x."

For $x, y \in \mathbb{R}$, define:

$$d(x, y) = |x - y|.$$

Claim

$d : \mathbb{R} \times \mathbb{R} \to [0, \infty)$ is a *metric* on $\mathbb{R}$.

Other Examples of Metrics

$$D(x, y) = \begin{cases} 1 \text{ if } x \neq y \\ 0 \text{ if } x = y. \end{cases}$$

Other Topics

- $S \subseteq \mathbb{R}$ and $<$, the order on the real line.

Boundedness

1. $u \in \mathbb{R}$ is an *upper bound* for S if $(\forall x \in S)(x \leq u)$.
2. $\ell \in \mathbb{R}$ is a *lower bound* for S if $(\forall x \in S)(\ell \leq x)$.
3. $m \in \mathbb{R}$ is a *maximum* for S if,

- m is an upper bound for S
- $m \in S$.

4. m is a *minimum* for the set S if

- m is a lower bound for S,
- $m \in S$.

5. u is a *least upper bound* for the set S if

- u is an upper bound for S
- For any upper bound, U of S, $u \leq U$.
  (Least upper bound = supremum) $u = \sup(S)$

6. ℓ is a *greatest lower bound* for S if

- ℓ is a lower bound

- For any lower bound, L of S, $L \leq \ell$. (Greatest lower bound = infimum) $\ell = \inf(S)$

Examples

1. $S = (0, 2)$

- Open interval from $(0, 2)$
- 2 is an upper bound, but not a maximum for S

2. $S = \{1, 1 + \frac{1}{4}, 1 + \frac{1}{4} + \frac{1}{16}, 1 + \frac{1}{4} + \frac{1}{16} + \frac{1}{64}, \ldots, 1$

- S has a lower bound
- How about an upper bound?

For each n define $v_n = \sum_{i=0}^{n} \left(\frac{1}{4}\right)^n$. To determine v_n, consider the following:

Put $m_n = \sum_{i=0}^{n} x^i$. $x \cdot m_n = \sum_{i=0}^{n} (x^2)^i$.

$m_n - x m_n = x^0 - x^{n+1}$. So,

$$m_n = \frac{x^0 - x^{n+1}}{1 - x}.$$

Applied to our example S,

$$\begin{aligned} v_n &= \frac{\left(\left(\frac{1}{4}\right)^0 - \left(\frac{1}{4}\right)^{n+1}\right)}{1 - \left(\frac{1}{4}\right)} \\ &= \frac{4}{3}\left(1 - \left(\frac{1}{4}\right)^{n+1}\right). \end{aligned}$$

Note that for $m < n$, $\left(\frac{1}{4}\right)^{m+1} > \left(\frac{1}{4}\right)^{n+1}$, so v_m compared with v_n yields $v_m < v_n$.

But note that for all n, $\left(\frac{1}{4}\right)^{n+1} > 0$. Thus, $1 - \left(\frac{1}{4}\right)^{n+1} < 1 - 0$, so $v_n = \frac{4}{3}\left(1 - \left(\frac{1}{4}\right)^{n+1}\right) < \frac{4}{3}$.

Is $\frac{4}{3}$ the least upper bound?

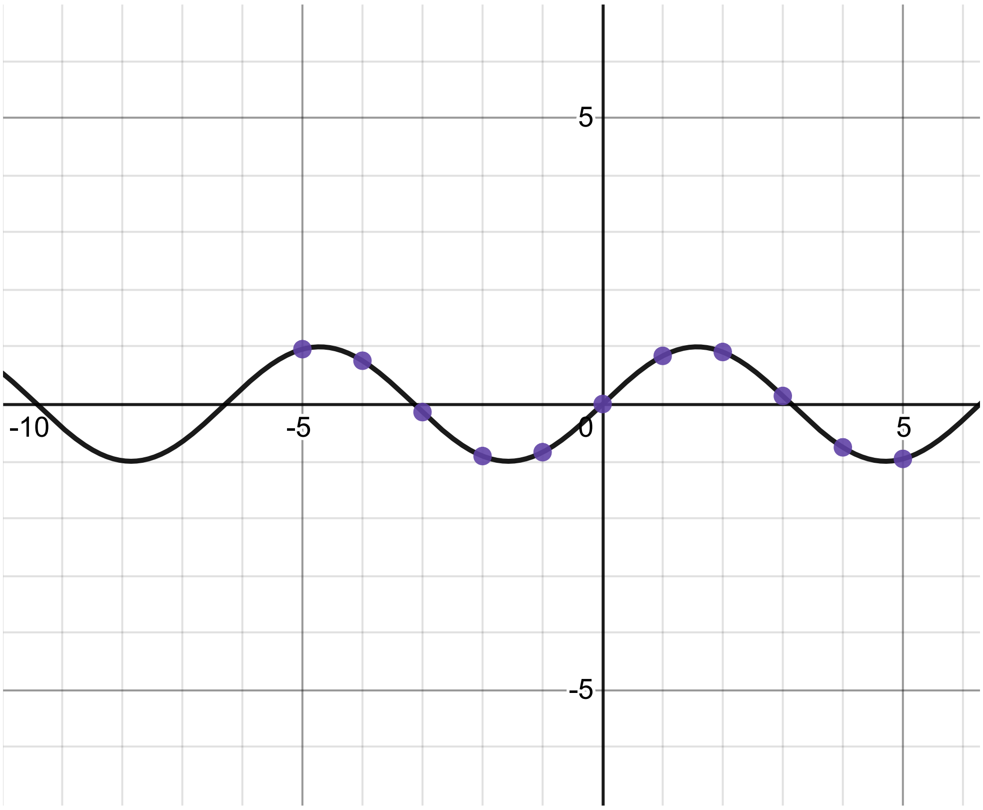
3. $S = (1, 1) \cup (3, 5)$

Bounds	Set
Lower Bounds	$(-\infty, 0]$
Upper Bounds	$[5, +\infty)$
Greatest Lower Bound	0
Least Upper Bound	5

4. $S = \{\sin(n) : n \in \mathbb{N}\}$

Bounds	Set
Lower Bounds	$(-\infty, -]$
Upper Bounds	$[1, +\infty)$
Greatest Lower Bound	0
Least Upper Bound	5

- Note that we know when considering $f : \mathbb{R} \to \mathbb{R}$, $\sin(x) = 1$ when $x = \frac{\pi}{2} + 2\pi n$, where $n \in \mathbb{Z}$.



$\sin(x) = -1$ if $x = -\frac{\pi}{2} + 2\pi n$, $n \in \mathbb{Z}$.

Conjecture: $1 = \sup(S)$ and $-2 = \inf(S)$.

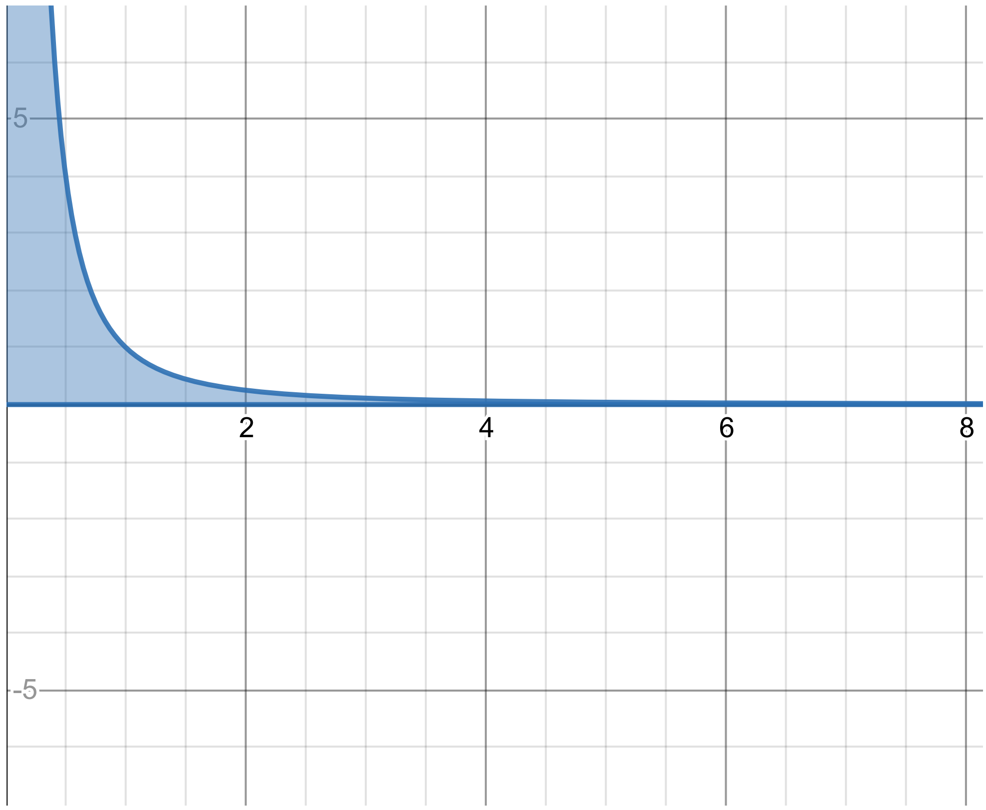
Idea: How 'close' can the quantities $\frac{\pi}{2} + 2\pi n$ and m, where $m, n \in \mathbb{N}$ be?

5. $f(n) = \sum_{n=0}^{\infty} \frac{1}{n}$ and we say $S = \{f(n) : n \in \mathbb{N}\} = \{f(1), f(2), f(3), \ldots, f(n), .$

- $(m < n) \implies (f(m) < f(n))$

Clearly $f(1) \in S$ and $f(1) = \min(S)$. S has no *maximum* element.

6. Consider the function $f(x) = \frac{1}{x^2}$



as we know

$$\int_1^\infty \frac{1}{x^2}\,dx = \left[-\frac{1}{x}\right]_1^\infty = \lim_{n\to\infty} -\frac{1}{c} - \left(-\frac{1}{1}\right)$$
$$= \lim_{n\to\infty} 1 - \frac{1}{c} = 1.$$

Lecture 24

Brennan Becerra

2023-11-14

Example

$$f(n) = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \dots \frac{1}{n^2}$$

$$S = \{f(n) : n \in \mathbb{N}\}$$

We showed S is bounded above and 2 is an upper bound.

> Completeness Axiom
>
> Every nonempty set of real numbers that has an upper bound, has a least upper bound.

Euler found that the least upper bound to S was in fact $\frac{\pi^2}{6}$. $\sup(S) = \frac{\pi^2}{6}$

Now consider the following:

$$f_2(n) = \sum_{i=1}^{n} \frac{1}{i^4}$$

$$S_2 = \{f_2(n) : n \in \mathbb{N}\}, S = \{f(n) : n \in \mathbb{N}\}.$$

$$(\forall x \in S_2)(\exists y \in S)(x \leq y).$$

Thus, as S has an upper bound, so does S_2. Thus as S has a least upper-bound so does S_2 and $\sup(S_2) \leq \sup(S)$.

What about 6th powers?

$$
\begin{aligned}
f_3(n) &= \sum_{i=1}^{n} \frac{1}{i^6} \\
S_3 &= \{f_3(n) : n \in \mathbb{N}\} \\
\sup(s_3) &= \frac{\pi^6}{945}
\end{aligned}
$$

8th powers?

$$
\begin{aligned}
f_4(n) &= \sum_{i=1}^{n} \frac{1}{i^8} \\
S_4 &= \{f_4(n) : n \in \mathbb{N}\} \\
\sup(S_4) &= \frac{\pi^8}{9450}
\end{aligned}
$$

Considering the reciprocals of the fractions, we observe the following pattern:

Denominators of $\zeta\left(\frac{2n}{\pi^{2n}}\right)$:

https://oeis.org/search?q=6%2C+90%2C+945%2C+9450&language=english&go=Search

For a sequence of the form $f : \mathbb{N} \to \mathbb{R}$

$$
f(n) = g(1) + g(2) + \cdots + g(n)
$$

where $g : \mathbb{N} \to \mathbb{R}$ is a sequence with $g(n) \geq 0$ for all n, if the set $S = \{f(n) : n \in \mathbb{N}\}$ has an upper bound, then we write the following:

$$
\sup(S) = \sum_{n=1}^{\infty} g(n).
$$

$f(n)$ is said to be a partial sum of $\sum_{n=1}^{\infty} f(n)$.

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

The series $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is convergent, and converges to $\frac{\pi^2}{6}$.

Say $g(n) = (-1)^{n+1}$ and $f(n) = \sum_{i=1}^{n} g(i)$. Is there an upper bound for the set $\{f(n) : n \in \mathbb{N}\}$

n	$f(n)$
1	1
2	0
3	1
4	0
5	1
6	0

1 in fact is the upper bound for $\{f(n) : n \in \mathbb{N}\}$, with a lower bound of 0. This series does not converge. In order to make this precise, we must discuss limits and convergence. We must make precise that $\sum_{n=1}^{\infty}(-1)^n$ does not have a limit.

What is a limit for a sequence?

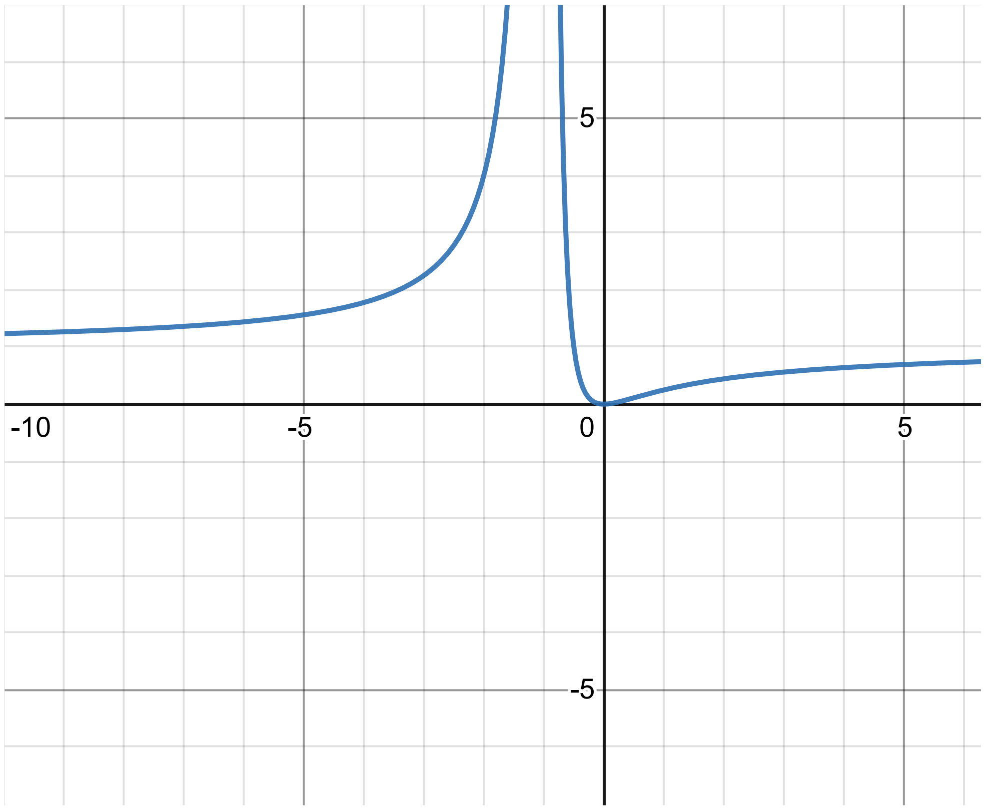
Limit of a Sequence

Let $h : \mathbb{N} \to \mathbb{R}$ be a sequence, with $L \in \mathbb{R}$ as a limit for h if: for each $\epsilon \in \mathbb{R}^+$ there is an $N \in \mathbb{N}$ such that for all $n \geq N$,

$$L - \epsilon < h(n) < L + \epsilon$$

I.E. $h(n) \in (L - \epsilon, L + \epsilon)$.

$$h_3(n) = \frac{n^2}{n^2 + 2n + 1}$$



Lecture 25

Brennan Becerra

2023-11-16

Limit Definition

Definition

Given a sequence $f : \mathbb{N} \to \mathbb{R}$ and a real number L, we call L the *limit* of the sequence if:

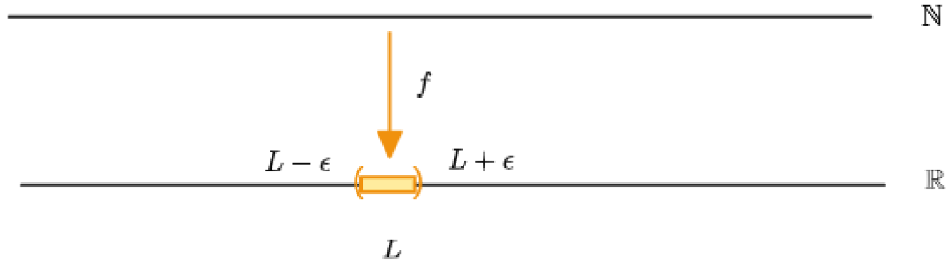
For each $\epsilon > 0$, there exists a $N \in \mathbb{N}$, such that

$$(\forall n \geq N)(L - \epsilon < f(n) < L + \epsilon).$$

More stuff

L is a limit of $f : \mathbb{N} \to \mathbb{R}$. How does one verify/disprove a statement like this?

One	Two
$\epsilon > 0$	$N \in \mathbb{N}$
$\epsilon_2 > 0$	$N_2 > N$



Concrete Examples

Recall: $f(n) = \sum_{i=1}^{n} \frac{1}{i^2}$ and $\lim_{n\to\infty} f(n) = \frac{\pi^2}{6}$.

New example:

$$f_2(n) = \sum_{i=1}^{n} \frac{1}{i^2 + i}$$

1. Does $f_2(n)$ have an upper bound?

Note that

$$(\forall n)(f_2(n) \leq f(n))$$

Proof

Define

$$T = \{m \in M : f_2(m) \leq f(m)\} = \mathbb{N}.$$

Let us verify the truth of each of the following two statements

(A) $1 \in T$

$$f_2(1) = \frac{1}{2} < 1 = f(1).$$

Thus $1 \in T$ is true.

(B) If $\underbrace{n \in T,}_{p_1}$ then $\underbrace{n + 1 \in T.}_{p_2}$

p_1	p_2	$p_1 \implies p_2$
T	T	T
T	F	F
F	T	T
F	F	T

Thus, $f_2(n) \leq f(n)$.

But

$$
\begin{aligned}
f_2(n+1) = f_2(n) + \frac{1}{(n+1)^2 + (n+1)} &\leq f(n) + \frac{\quad}{(n \cdots} \\
&< f(n) + \frac{1}{(n + \cdots}
\end{aligned}
$$

thus, $n+1 \in T$ is true. It follows that If $n \in T$, then $n+1 \in T$ is true. By the induction axiom, $T = \mathbb{N}$. So, $(\forall n \in \mathbb{N},)(f_2(n) \leq f(n))$. Since $\{f(n : n \in \mathbb{N})\}$ has an upper bound, say U, we find that U is also an upper-bound of $f_2(n)$. The completeness axiom tells us that a least upper bound, L also exists for $\{f_2(n) : n \in \mathbb{N}\}$.

Recall that for $\{f(n) : n \in \mathbb{N}\}$, the least upper bound is $\frac{\pi^2}{6}$. So, $L \leq \frac{\pi^2}{6}$.

What s L?

$$
\frac{1}{n^2+n} = \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}
$$

so,

$$
\begin{aligned}
f_2(1) &= \frac{1}{2} - \frac{1}{1+1} \\
f_2(2) &= \frac{1}{1^2+1} + \frac{1}{2^2+2} \\
&= \left(\frac{1}{1} - \frac{1}{1+1}\right) + \left(\frac{1}{2} - \frac{1}{2+1}\right) \\
&= \frac{1}{1} - \frac{1}{2+1} \\
f_2(3) &= \frac{1}{1^2+1} + \frac{1}{2^2+2} + \frac{1}{3^2+3} \\
&= \left(\frac{1}{1} - \frac{1}{1+1}\right) + \left(\frac{1}{2} - \frac{1}{2+1}\right) + \left(\frac{1}{3} - \frac{1}{3+}\right.
\end{aligned}
$$

And we cans see that this *telescoping series* will go to

$f_2(n) = \frac{1}{1} - \frac{1}{n+1} < 1.$

Hypothesis: $L = 1$ is a limit for the following set:

$$\{f_2(n) : n \in \mathbb{N}\}.$$

One	Two
$\epsilon_1 = \frac{1}{10}$	

$$f_2(n) = 1 - \frac{1}{n+1} = \frac{n}{n+1}$$

Lecture 26

Brennan Becerra

2023-11-28

Metrics

Metric

Let S be a given nonempty set. A function $d : S \times S \to [0, \infty)$ is said to be a *metric* (distance function) if:

1. $(\forall x \in S)(d(x, x) = 0)$
2. $(\forall_{x,y} \in S)(d(x, y) = d(y, x))$
3. $(\forall_{x,y,z} \in S)(d(x, z) \leq d(x, y) + d(y, z))$ (Triangle inequality)
4. $(\forall_{x,y} \in S)(x \neq y) \implies (d(x, y) \geq 0)$

- Metrics measure distances between elements of sets

Consider $\mathbb{R} = \mathbb{X}$.

Definition

1. $d(x, y) = |x - y|$.
2. $$|x| = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0. \end{cases}$$

Show that this d is a metric. Catalog properties of $|\cdot|$ and its interaction with the algebraic properties of $\mathbb{R}$.

(a) $|-x| = |x|$, for all $x \in \mathbb{R}$.

Proof

Case 1:

$x < 0$. Then $-x > 0$, and by definition, $|x| = -x = |-x|$ (as $-x > 0$)

Case 2:

$x = 0 \implies -x = x$, so $|-x| = x$.

Case 3: $x > 0 \implies -x < 0$, so by Case 1, $|-x| = |-(-x)| = |x|$.

(b) $|x \cdot y| = |x| \cdot |y|$.

Proof

$((x = 0) \vee (y = 0)) \implies (|x \cdot y| = |0| = |x| \cdot |y|)$, so assume $x \neq 0$, and $y \neq 0$.

x	y
+	+
+	-
-	+
-	-

<u>Case 1:</u> $x, y > 0$.

Then, $x \cdot y > 0$. By definition, $|x \cdot y| = xy = |x| \cdot |y|$.

<u>Case 2:</u> $x > 0$ and $y < 0$. Then we get $x \cdot y < 0$, and

$$\underbrace{|x \cdot y| = -(x \cdot y)}_{\text{Definition}} = \underbrace{(-1 \cdot x) \cdot y = (x \cdot -1) \cdot y = x \cdot (-y)}_{\text{Algebraic Properties}}$$

<u>Case 3:</u> $x < 0$ and $y > 0$.

Analogue to Case 2.

<u>Case 4:</u> $x, y < 0$

Then we can say $x \cdot y > 0$, and so,

$$
\begin{aligned}
|x \cdot y| &= x \cdot y \\
&\left.\begin{aligned}
&= (-1)^2 \cdot (x \cdot y) \\
&= ((-1) \cdot (-1) \cdot x) \cdot y \\
&= ((-1) \cdot ((-1) \cdot x)) \cdot y \\
&= ((-1) \cdot (x \cdot (-1))) \cdot y. \\
&= (-1) \cdot ((x \cdot (-1)) \cdot y) \\
&= (-1) \cdot (x \cdot ((-1) \cdot y)) \\
&= ((-1) \cdot x) \cdot ((-1) \cdot y) \\
&= -x \cdot -y
\end{aligned}\right\}\text{Algebra} \\
&= |x| \cdot |y|.
\end{aligned}
$$

(c) $|x+y| \leq |x| + |y|$.

Proof

If $x = 0$ then $x + y = y$, and $|x| + |y| = |y|$. This implies that $|x+y| = |y| = |x| + |y| \leq |x| + |y|$. Similarly, $(y = 0) \implies (|x+y| \leq |x| + |y|)$.

Assume $x, y \neq 0$.

Case 1: $x, y > 0$, then

$$\begin{aligned} x + y &> 0 \text{ and} \\ |x+y| &= x + y \\ &= |x| + |y| \\ &\leq |x| + |y|. \end{aligned}$$

Case 2: $x > 0$, and $y < 0$, then,

$$|x| + |y| = x + (-y)$$

Subcase (a). $0 < -y < x$, so

$$y < 0 < x + y < x$$

but by definition of $|\cdot|$,

$$\begin{aligned} 0 < |x+y| &< |x| \\ &< |x| + |y|. \end{aligned}$$

Case 3: $x < 0$ and $y > 0$,

apply the same argument as in Case 2.

Case 4: $x, y < 0$, then

$$\begin{aligned} x + y &< 0 \text{ so,} \\ |x + y| &= -(x + y) \\ &= (-1) \cdot x + (-1) \cdot y \\ &= -x + -y \\ &= |x| + |y|. \end{aligned}$$

This completes all cases. $\square$

(d) $|x - y| \leq |x| + |y|$

We wish to compare $|x + y|$ to $|x - y|$.

Lecture 27

Brennan Becerra

2023-11-30

Metrics

Metric

Let S be a nonempty set. A function $d : S \times S \to [0, \infty)$ is said to be a *metric* (distance function) if:

1. $(\forall x \in S)(d(x, x) = 0)$
2. $(\forall_{x,y} \in S)(d(x, y) = d(y, x))$ (Symmetry)
3. $(\forall_{x,y,z} \in S)(d(x, z) \leq d(x, y) + d(y, z))$ (Triangle inequality)
4. $(\forall_{x,y} \in S)(x \neq y) \implies (d(x, y) \geq 0)$

Metrics in $\mathbb{R}$

Definition

For $x, y \in \mathbb{R}$, $d(x,y) := |x-y|$.

Recall:

For $x, y \in \mathbb{R}$,

1. $d(x,y) = |x-y|$.
2. $$|x| = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0. \end{cases}$$

Properties of $|\cdot|$

1. $|-x| = |x|$
2. $|x \cdot y| = |x| \cdot |y|$.
3. $|x \cdot y| = |x| \cdot |y|$
4. $|x+y| \leq |x| + |y|$

Proof of (4)

$$\begin{aligned} |x-y| &= |x+(-y)| \\ &\leq |x| + |-y| \qquad \text{[By (3)]} \\ &= |x| + |y| \qquad \text{[By (1)]} \qquad \square \end{aligned}$$

- Direct proof

Verifying that $d : \mathbb{R}^2 \to [0, \infty)$ is a Metric

Proof

1. Let $x \in \mathbb{R}$, be given. Then, $d(x, x) = |x - x| = |0| = 0.$✓
2. Let $x, y \in \mathbb{R}$ be given. Then, $d(x, y) = |x - y|$. (Definition)

$$\begin{aligned} d(x,y) &= |x-y| \\ &= |-(x-y)| && \text{[By} \\ &= |-x+y| && \text{[Distributiv} \\ &= |y+(-x)| && \text{[Commutativity of addit} \\ &= d(y,x). && \text{[Definit} \end{aligned}$$

Since $x, y \in \mathbb{R}$ were arbitrary, (2) is confirmed. ✓

3. Let $x, y, z \in \mathbb{R}$, be given. Then,

$$\begin{aligned} d(x,y) &= |x-y| && \text{[Defin} \\ &= |x-0-y| \\ &= |x-(z-z)-y \\ &= |(x-z)+(z-y)| \\ &\le |x-z|+|z-y| && \text{[B} \\ &= |x-z|+1\cdot|z-y| \\ &= |x-z|+|-1|\cdot|z-y| \\ &= |x-z|+|(-1)\cdot(z-y)| \\ &= |x-z|+|-z+y| && \text{[Distribut} \\ &= |x-z|+|y-z| && \text{[Commutat} \\ &= d(x,z)+d(y,z). \end{aligned}$$

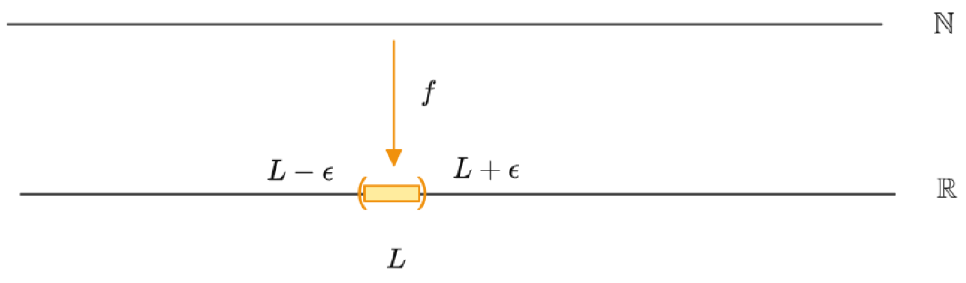
4. Let $x, y \in \mathbb{R}$, such that $x \neq y$. Then, by definition, $d(x, y) = |x - y|$. Since $x \neq y$, $x - y \neq 0$, therefore

$$|x-y| = \begin{cases} x-y \text{ if } x-y \ge 0 \\ y-x \text{ if } x-y < 0. \end{cases}$$

In either case, $|x - y| \neq 0$, and furthermore, must be positive. Thus, $d(x, y) > 0$ is true. Consequently, $x \neq y \implies d(x, y) > 0$ is true. ✓

Since all 4 properties of a metric have been satisfied, $d : \mathbb{R}^2 \to d(x, y)$ is in fact a metric. $\square$

Quick Sketch Of Limits



Lecture 28

Brennan Becerra

2023-12-05

Review

Topic 1: The Mathematical Method

$P = \{p_1, p_2, \ldots, p_n\}$ denote *statements.*

Connectives:

- $\wedge$ ("and")
- $\vee$ ("or")
- $\neg$ ("not")
- $\implies$ "if, then"

Parentheses: (,)

Language:

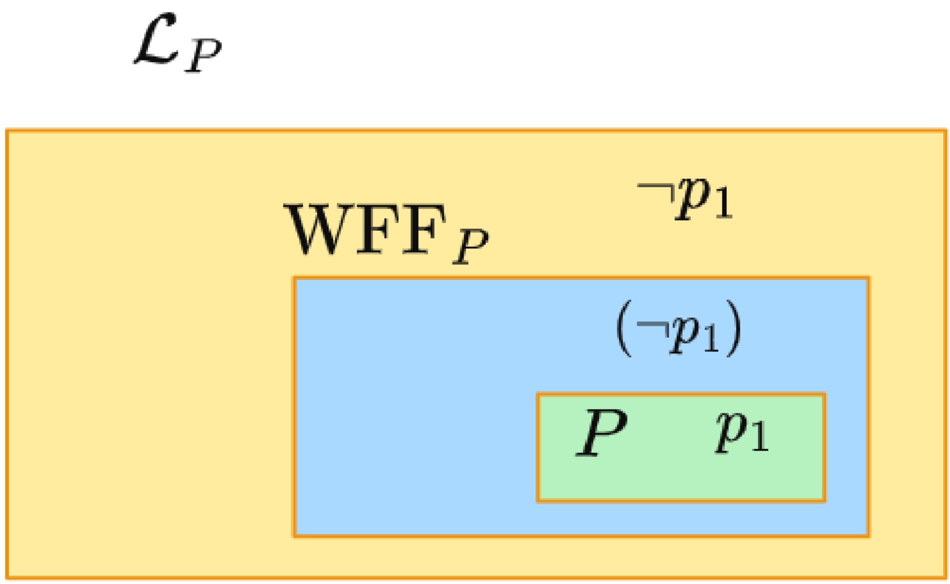
Propositional logic language $\mathcal{L}_P$ denotes all finite sequences that can be built from the alphabet consisting of all the propositional, and connective symbols

$$\mathcal{L}_p := P \cup \{\wedge, \vee, \neg, \implies, (,)\}.$$

> Well-Formed Formula
>
> Let Ψ be an element of $\mathcal{L}_p$. Ψ is a well formed formula, if
>
> 1. $\Psi \in P$
> 2. Ψ is $\neg\Phi$ where Φ is a well-formed formula.
> 3. Ψ is $\Phi \wedge \Gamma$ where Φ, Γ are well-formed formula.
> 4. Ψ is $(\Phi \vee \Gamma)$ where Φ, Γ are well formed-formula.

5. Ψ is $(\Phi \implies \Gamma)$ where Φ, Γ are well-formed formula

$$\text{WFF}_P = \{\Phi \in \mathcal{L}_p : \Phi \text{ is a well formed formula.}\}$$



Example

$$((\underbrace{\neg p_1}_{\checkmark}) \vee (\underbrace{p_2 \wedge p_3 \wedge p_4}_{\times}))$$

<u>Not</u> well-formed. We could fix this by changing $(p_2 \wedge p_3 \wedge p_4)$ to $(p_2 \wedge (p_3 \wedge p_4))$ or $((p_2 \wedge p_3) \wedge p_4)$.

Truth Values

The set of truth values is $\{\mathrm{T}, \mathrm{F}\}$. Consider the <u>assignment of truth values</u> to proposition symbols $p_1, p_2, \ldots$

$$A : P \to \{\mathrm{T}, \mathrm{F}\}$$

(A is a function)

Extension of A to $\mathbf{WWF}_P$ is as follows:

Let Φ and Ψ be well formed formulae, for which the values of A are known.

Consider the following:

$A(\neg\Phi)$

Φ	$\neg\Phi$
T	F
F	T

$A(\Phi \wedge \Psi)$

Φ	Ψ	$\Phi \wedge \Psi$
T	T	T
T	F	F
F	T	F
F	F	F

$A(\Phi \vee \Psi)$

Φ	Ψ	$\Phi \vee \Psi$
T	T	T
T	F	T
F	T	T
F	F	F

$A(\Phi \implies \Psi)$

Φ	Ψ	$\Phi \implies \Psi$
T	T	T
T	F	F
F	T	T
F	F	T

These represent the functional values of A as truth tables.

Contradictions and Tautologies

Contradiction

A contradiction is a well-formed formula with truth value F for all truth assignments.

- $(p_1 \wedge (\neg p_1))$

Tautology

A tautology is a well-formed formula with truth value T for all truth assignments.

- $(p_1 \vee (\neg p_1))$
- Note that propositions can NOT be a tautology
- Tautologies, propositions and contradictions are disjoint "sets" in $\mathbf{WWF}_P$

Sets and Functions

Set

We can define a *set* as a collection of objects.

$$S = \{s_1, \ldots, s_n\}$$

- Order doesn't matter
- No repetitions of objects allowed

- $\mathcal{P}(A)$
- $A \cup B$
- $A \cap B$
- $A \setminus B$
- $A \Delta B$

one-to-one function

Let A, B be sets. We say that B has at least as many elements as A if there is a *one-to-one function* from A to B.

$$|A| \leq |B|$$

" A has no more elements than B. "

Schroeder-Bernstein Theorem

Let A, B be sets. The following are equivalent:

1. There is a one-to-one and onto function:

$$f : A \to B$$

2. (a.) There is a one-to-one function:

$$g : A \to B$$

   (b.) There is a one-to-one function:

$$h : B \to A$$