Class starts after this song

Yiruma – River Flows in You (2001) requested by Yiyang Shao (Backend head TA)

I like playing basketball, volleyball and archery. I have a cat named Lizi(Chestnut).

Machine learning mood



Submitted at: January 23, 1:08 PM

Question Outline

Title

11

1.1 a

1.2 b

1.3 c

2.1 a

2.2 b

2.3 C

3.1 a

3.2 b

4 Recitation part (skip if attended recitation)

22

33

Select a question or a page.

Select questions and pages to indicate where your responses are located. Use esc to desele

Points

0.0 pts

×

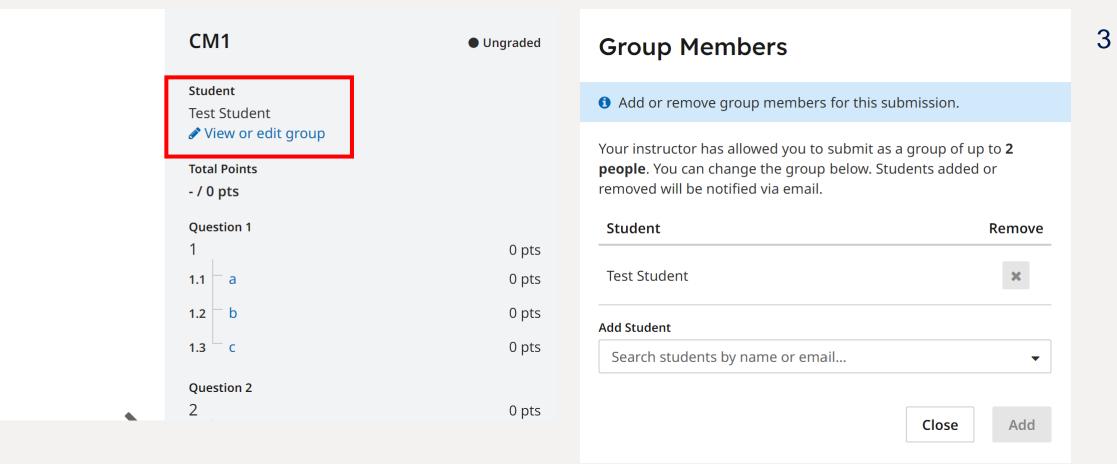
1 Recitation

•

Jse esc to deselect al		use the arrow keys on the keyboard.
CS230 Recitation/Assignmen	Unmatched Pages & Questions	ns) menution are satisfied. Specify the sense is the consequence provided.
Recitation 01/22, Assign Recitation (Usgradel articly) feedenshing and getting to know each of Continued from class metring: Let C(x) represent 'x' can be	You haven't matched all pages and questions.	a Process and Marke Talasce
DS(c) inpresent "x drive solw" and PO(x) inpresent "x given (a) Translate the following senses of the mon English to a popul "Share-Heng can have cale or ice crossit, but not both" (b) What does the materices "Drive solver, or get pulled over," profilente.	Page 1 doesn't have associated questions.	gives about two periods: $P(r)$ as: $(0 \frac{V(r)(r)}{V(r)} = Q(r)$ $(0 \frac{V(r)(r)}{V(r)} = Q(r)$
3. (Ungraded whole-section activity) Let P be the proposition proposition T have get 80% of the quotients in the proposite T have actuated lineticities, for models T^* . Derive the texth 1 module P , according to the information in Carcas. You will b $P = Q_{-}$.	Question 4 doesn't have associated pages.	0 (100) 1000 100
4. (Ungraded articly) Finding emigranesis partner. 5. (De Mergan's here for three variables) We have already seen $(-q(x,y)) = -\sqrt{-q_0}$.	You can still submit your assignment without this page associated, however we recommend matching all pages so that graders can	if is useful for this many number of $Q(x)$, since we have a single state of the domain is as in two, which the constant is non- $W(x)$ and $Q(x)$, along with mean dynamic is true, which the Benchminn matrix (3). From Add
We will derive the non-for three variables $\label{eq:constraint} \begin{split} & (c,b,p,t,t) = - \\ & -(c,b,p,t,t) = - \\ & -($	easily find your work. Submit Assignment Continue Matching	b) (2007) and requestries small T in the ** of the hand in the truth <i>EAE for * a domainstation for two</i> why have it in the table from the Q <i>e</i> expension between it (CSF: CC

- Double check you label the correct pages to each question •
 - If you don't submit recitation work, Gradescope will warn you that you haven't labeled pages for it (which is normal)

2



Then add your teammate here; DO NOT SUBMIT SEPARATELY



 $\exists L \in \mathbb{R} \quad \forall \varepsilon > 0 \quad \exists \delta > 0 \qquad \left[(0 < |x - a| < \delta) \rightarrow (|f(x) - L| < \varepsilon) \right]$

- We made a mistake in CM1 recitation material here; we forgot to quantify x
- The predicate with this part missing was not "false"; it is still true when the limit exists, but it's this version with *x* quantified that semantically translates the limit definition
- In hindsight, this problem still relies on knowing what a limit is; don't worry about that part and we were/are just using it for practice on predicate logic



CS230 Spring 2024 Module 02: Proof Methods



Why proof?

- You need to make arguments on how things work as a future computer scientist
- Can you always base your arguments on evidence?
 - "The last 1,000 times I used it, this sorting algorithm actually gives me a sorted list"
- If not, then you sometimes need to base them on logic
 - Proofs are nothing beyond that (but more formal, and more stylistic)

7

What can be proved?

- Nothing can be proved without assumptions/axioms/facts given
 - Very very strictly speaking, a mathematical proof is incomplete without specifying what axioms are used
 - Practical compromise: state all nontrivial assumptions/axioms
- Only propositions can be proved/disproved
 - This is how we "defined" propositions!
 - Not all propositions can be proved/disproved within propositional logic

How are \rightarrow and \Rightarrow different?

- \rightarrow (conditional operator): $p \rightarrow q$ can be either true or false
- \Rightarrow (implication): $p \Rightarrow q$ means " $p \rightarrow q$ is a tautology"

8

Modus Ponens, revisited

 $\frac{p \to q}{\frac{p}{\therefore q}}$

 $((p \to q) \land p) \Rightarrow q$



Similarly:

- \leftrightarrow (biconditional operator): $p \leftrightarrow q$ means $(p \rightarrow q) \land (q \rightarrow p)$
- \Leftrightarrow , =, \equiv (equivalence): $p \Leftrightarrow q$ means $(p \Rightarrow q) \land (q \Rightarrow p)$
- When we prove $p \leftrightarrow q$ is true, we proved $p \Leftrightarrow q$ (read: p is equivalent to q)
- "We prove *p* if and only if *q* (is true)"

PD: Proof Example 1

- Read this proof individually
- Then turn to your neighbor, discuss where exactly is the proof wrong



Proof:

n and q need to be integers

Let a = 2n + 1 and b = 2q + 1 be two odd integers.

Then (2n+1)(2q+1) = 4nq + 2n + 1 = 2(2nq + n) + 1.

missing a 2q (algebraic error)

Since (2nq + n) is an integer, 2(2nq + n) + 1 is an odd integer.

questionable choices of variables (not wrong)

Duke

PD: Proof Example 2

• What about this proof?



states more than what is needed (not wrong, but bad practice)

If n is an integer, $n^3 - n = (n - 1)n(n + 1)$ is the product of three consecutive integers (n - 1), n, and (n + 1).

Among these three integers, at least one is a multiple of 2 and exactly one is a multiple of 3.

Since 2 and 3 are both primes, $n^3 - n = (n-1)n(n+1)$ is a multiple of 2 imes 3 = 6.

Duke

Proof by construction [Existential Generalization]

• To prove a theorem of the form

 $\exists x[P(x)]$

we merely need to find ("construct") ONE c and show P(c).

 $P(c) \Rightarrow \exists x [P(x)]$



Proof by construction [Existential Generalization]

- Theorem: There exist integers *a*, *b*, *c* such that $a^2 + b^2 = c^2$.
- Proof: let a = 3, b = 4, c = 5.

14



Proof by (complicated) construction

- Theorem: Given two strings $x_1x_2 \cdots x_n$ and $y_1y_2 \cdots y_m$, there is an algorithm that runs in O(mn)-time that finds the length of their longest common substring, i.e., the largest k for which there exist indices i, j with $x_i x_{(i+1)} \cdots x_{(i+k-1)} = y_j y_{j+1} \cdots y_{(j+k-1)}$.
- Proof:
 - Describe the algorithm
 - Prove the algorithm runs in O(mn)-time
 - Prove the algorithm finds the largest such k for all possible input strings

Proof by construction [Existential Generalization]

• To prove a theorem of the form

 $\exists x[P(x)]$

we merely need to find ("construct") ONE c and show P(c).

 $P(c) \Rightarrow \exists x [P(x)]$





Disproof by counterexample

- A disproof by counterexample is itself a proof by construction of the negation of the initial proposition.
- Disproving $\forall x[P(x)]$ is just proving $\neg(\forall x[P(x)])$, which is equivalent to $\exists x[\neg P(x)]$.
- The counterexample is some c that makes $\neg P(c)$ true.



Class starts after this song

Paramore – Proof (2013) requested by Luke Lorentzatos (TA-of-CM2)

I'm half Greek and can speak a little bit. I am a huge Houston Astros fan.



Duke

Visiting Class Today: TAs-of-CM2



Anirudh Jain

I'm always down for poker and table tennis. And I respond to at least 8 pronunciations of my name.

> Hi, I like taekwondo and reading. I also like skiing and baking but those are harder to do at Duke.





Reminders on Gradescope assignment

- Type your work; no handwriting accepted
- The best way to use the provided LaTeX source code is to directly modify it (as it's meant to be the skeleton/template)
 - Put macros.tex in your project folder as a separate file
 - Use \mathbb{R} to typeset blackboard bold \mathbb{R}
- Label pages after uploading PDF
- Submit just once per group, then add your teammate
- No names necessary in PDF

Prove a proposition/theorem/statement

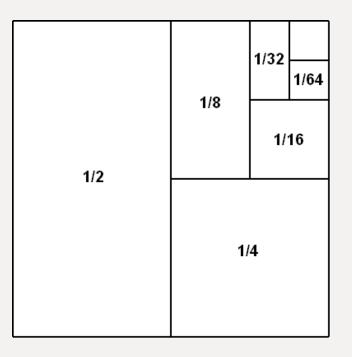
- Direct proof
- Proof by contrapositive
- Proof by contradiction
- Proof by cases
- Proof by construction
- Proof by induction [big topic itself CM5]
- What else?



Proof by picture...?

•
$$\sum_{i=1}^{\infty} \frac{1}{2^i} = 1$$

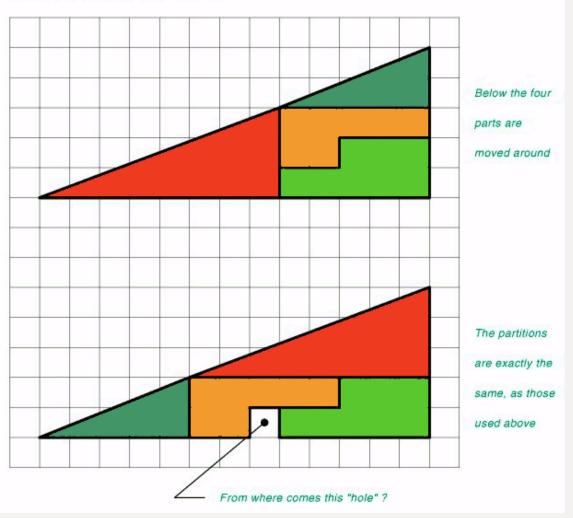
• A picture alone is not a proof





HOW CAN THIS BE TRUE ?

Proof by picture





23

PI: Biconditional







An abstracted version of the question

- Want to prove: $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \land (q \rightarrow p)$
- a) $p \rightarrow q$ b) $q \rightarrow p$ c) $\neg q \rightarrow \neg p$

 $d) \neg p \rightarrow \neg q$



In case you did not notice

- The theorem is false
- If exactly two of a, b, c are even and the other is odd, $a^2 + b^2 + c^2$ is also odd (check this yourself)
- That should not matter
 - We were identifying what conditional statements or their contrapositives, that we should prove
 - We were not actually trying to prove them (we would fail)



26

Proving more than what is needed

- is technically correct
- is usually unnecessary
- sometimes makes the proof easier
 - more examples about this in CM5 (Inductions)



Write good proofs, not just correct proofs

- Correctness of the proof is the *first* priority, not the *only* priority
- Correct proofs are just correct. Good proofs can be understood.
 - You want your proofs to be correct and understood
 - What is obvious to yourself, may not be obvious to others

Peer Review (Proof-by-cases)

Navigate to the Canvas quiz



- Complete two simple proof-by-cases
 - Don't share accounts; complete the proofs on your own
 - Don't discuss with anyone else



Peer Review (Proof-by-cases)

- Navigate to Canvas quiz again
- You are now assigned two anonymous assignments by your classmates
- Read their work, then give feedback
 - Evaluate the technical correctness, readability, and conciseness of the proofs via the rubric provided



30

Proof. "For every positive integer n, if \sqrt{n} is rational, then \sqrt{n} is an integer.".

- We use proof by contradiction: assume $\neg (\forall n \in \mathbb{N} [\sqrt{n} \in \mathbb{Q} \to \sqrt{n} \in \mathbb{Z}])$
- $\therefore \exists n \in \mathbb{N}[\neg(\sqrt{n} \in \mathbb{Q} \to \sqrt{n} \in \mathbb{Z})]$
- $\therefore \exists n \in \mathbb{N}[(\sqrt{n} \in \mathbb{Q}) \land (\sqrt{n} \notin \mathbb{Z})]$
- $\therefore \exists a \in \mathbb{N} \, \exists b \in \mathbb{N}[(\sqrt{n} = \frac{a}{b}) \land (b \nmid a)]$
- Let $c \ge 1 = \operatorname{GCD}(a, b)$.
- $\therefore \exists x \in \mathbb{N} \, \exists y \in \mathbb{N}[(a = cx) \land (b = cy) \land (y \nmid x)]$

$$-: n = \frac{a^2}{b^2} = \frac{c^2 x^2}{c^2 y^2} = \frac{x^2}{y^2}.$$

- Since $(y \nmid x) \to (y^2 \nmid x^2), n = \frac{x^2}{y^2} \notin \mathbb{Z}$.

Excessive symbolism

)11ke

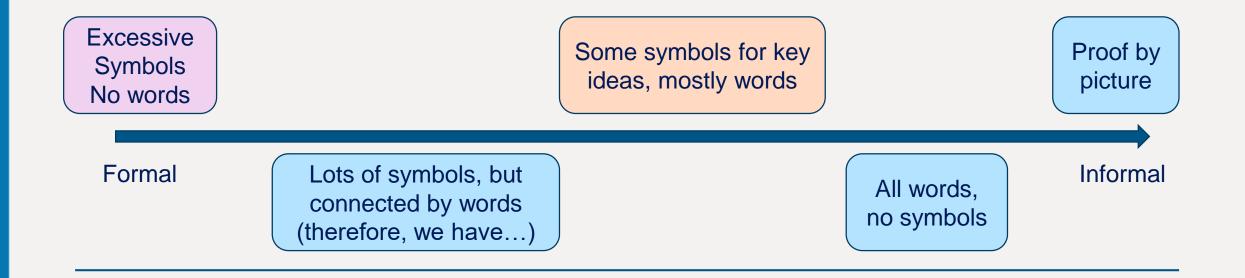
Proof. "For every positive integer n, if \sqrt{n} is rational, then \sqrt{n} is an integer."

- We use proof by contradiction: assume the theorem is not true.
- Then there exists a positive integer n such that \sqrt{n} is rational but not an integer.
- Then there exist positive integers a, b such that $\sqrt{n} = \frac{a}{b}$ and $b \nmid a$ (i.e., b does not divide a).
- Let $c \ge 1$ be the greatest common divisor of a and b.
- Then there exist positive integers x, y such that a = cx, b = cy, and $y \nmid x$. (otherwise b = cy would divide a = cx). Less
- Then $n = \frac{a^2}{b^2} = \frac{c^2 x^2}{c^2 y^2} = \frac{x^2}{y^2}$.
- Since $y \nmid x$ implies $y^2 \nmid x^2$, $n = \frac{x^2}{y^2}$ is not an integer.
- Since we reached a contradiction, the theorem is proved.

Duke

symbolistic

Level of formality





How to come up with the proof steps?

- Reading proofs (especially simple and beautiful ones) make you feel proofs come "naturally" as if all steps just magically fall into place
 - For most of sufficiently complicated theorems, this is usually not the case
 - A lot of trial-and-error (you don't have a compiler to tell you there's an error)
 - Messy thoughts, dead-ends, useful but out-of-order ideas...
- No one expects you to be perfect on the first try
 - Like no one expects you to write 100 lines of code that work immediately