I5-25I: Great Ideas in Theoretical Computer Science

Lecture 1.5: On proofs + How to succeed in 251

Proof. Define
$$f_{ij}$$
 as in (5). As f is symmetric, we only need to consider f_{12} .

$$\mathbf{E} \left[f_{12}^2 \right] = \mathbf{E}_{x_3...x_n} \left[\frac{1}{4} \cdot \left(f_{12}^2(00x_3...x_n) + f_{12}^2(01x_3...x_n) + f_{12}^2(10x_3...x_n) + f_{12}^2(11x_3...x_n) \right) \right] \\
= \frac{1}{4} \mathbf{E}_{x_3...x_n} \left[(f(00x_3...x_n) - f(11x_3...x_n))^2 + (f(11x_3...x_n) - f(00x_3...x_n))^2 \right] \\
\ge \frac{1}{2} \left(\binom{n-2}{r_0-1} \cdot 2^{-(n-2)} \cdot 4 + \binom{n-2}{n-r_1-1} \cdot 2^{-(n-2)} \cdot 4 \right) \\
= 8 \cdot \left(\frac{(n-r_0+1)(n-r_0)}{n(n-1)} \cdot \binom{n}{r_0-1} + \frac{(n-r_1+1)(n-r_1)}{n(n-1)} \cdot \binom{n}{r_1-1} \right) 2^{-n}.$$

Inequality (6) follows by applying Lemma 2.2.

In order to establish inequality (7), we show a lower bound on the principal Fourier coefficient of *f*:

$$\widehat{f}(\emptyset) \ge 1 - 2\left(\sum_{s < r_0} \binom{n}{s} + \sum_{s > n - r_1} \binom{n}{s}\right) 2^{-n},$$

which implies that

$$\widehat{f}(\emptyset)^2 \geq 1 - 4 \cdot \left(\sum_{s < r_0} \binom{n}{s} + \sum_{s < r_1} \binom{n}{s}\right) 2^{-n}.$$



August 29th, 2018

Poll

What is your favorite TV show? (go to Diderot to see the link)



"It's possible to succeed in 251, be a part of student orgs, and date, but hands off the phone!"

- Gabriela Brik (CS junior, RA)

PART I

On proofs

Proof. Define f_{ij} as in (5). As f is symmetric, we only need to consider f_{12} .

$$\begin{split} \mathbf{E}\left[f_{12}^{2}\right] &= \mathbf{E}_{x_{3}\dots x_{n}}\left[\frac{1}{4}\cdot\left(f_{12}^{2}(00x_{3}\dots x_{n})+f_{12}^{2}(01x_{3}\dots x_{n})+f_{12}^{2}(10x_{3}\dots x_{n})+f_{12}^{2}(11x_{3}\dots x_{n})\right)\right] \\ &= \frac{1}{4}\mathbf{E}_{x_{3}\dots x_{n}}\left[\left(f(00x_{3}\dots x_{n})-f(11x_{3}\dots x_{n})\right)^{2}+\left(f(11x_{3}\dots x_{n})-f(00x_{3}\dots x_{n})\right)^{2}\right] \\ &\geq \frac{1}{2}\left(\binom{n-2}{r_{0}-1}\cdot 2^{-(n-2)}\cdot 4+\binom{n-2}{n-r_{1}-1}\cdot 2^{-(n-2)}\cdot 4\right) \\ &= 8\cdot\left(\frac{(n-r_{0}+1)(n-r_{0})}{n(n-1)}\cdot\binom{n}{r_{0}-1}+\frac{(n-r_{1}+1)(n-r_{1})}{n(n-1)}\cdot\binom{n}{r_{1}-1}\right)2^{-n}. \end{split}$$

Inequality (6) follows by applying Lemma 2.2.

In order to establish inequality (7), we show a lower bound on the principal Fourier coefficient of *f*:

$$\widehat{f}(\emptyset) \ge 1 - 2\left(\sum_{s < r_0} \binom{n}{s} + \sum_{s > n - r_1} \binom{n}{s}\right) 2^{-n},$$

which implies that

$$\widehat{f}(\emptyset)^2 \ge 1 - 4 \cdot \left(\sum_{s < r_0} \binom{n}{s} + \sum_{s < r_1} \binom{n}{s} \right) 2^{-n}.$$

I. What is a proof?

- 2. How do you find a proof?
- 3. How do you write a proof?

Proof. Define f_{ij} as in (5). As f is symmetric, we only need to consider f_{12} .

$$\begin{split} \mathbf{E}\left[f_{12}^{2}\right] &= \mathbf{E}_{x_{3}\dots x_{n}}\left[\frac{1}{4}\cdot\left(f_{12}^{2}(00x_{3}\dots x_{n})+f_{12}^{2}(01x_{3}\dots x_{n})+f_{12}^{2}(10x_{3}\dots x_{n})+f_{12}^{2}(11x_{3}\dots x_{n})\right)\right] \\ &= \frac{1}{4}\mathbf{E}_{x_{3}\dots x_{n}}\left[\left(f(00x_{3}\dots x_{n})-f(11x_{3}\dots x_{n})\right)^{2}+\left(f(11x_{3}\dots x_{n})-f(00x_{3}\dots x_{n})\right)^{2}\right] \\ &\geq \frac{1}{2}\left(\binom{n-2}{r_{0}-1}\cdot 2^{-(n-2)}\cdot 4+\binom{n-2}{n-r_{1}-1}\cdot 2^{-(n-2)}\cdot 4\right) \\ &= 8\cdot\left(\frac{(n-r_{0}+1)(n-r_{0})}{n(n-1)}\cdot\binom{n}{r_{0}-1}+\frac{(n-r_{1}+1)(n-r_{1})}{n(n-1)}\cdot\binom{n}{r_{1}-1}\right)2^{-n}. \end{split}$$

Inequality (6) follows by applying Lemma 2.2.

In order to establish inequality (7), we show a lower bound on the principal Fourier coefficient of *f*:

$$\widehat{f}(\emptyset) \ge 1 - 2\left(\sum_{s < r_0} \binom{n}{s} + \sum_{s > n - r_1} \binom{n}{s}\right) 2^{-n},$$

which implies that

$$\widehat{f}(\emptyset)^2 \ge 1 - 4 \cdot \left(\sum_{s < r_0} \binom{n}{s} + \sum_{s < r_1} \binom{n}{s} \right) 2^{-n}.$$

- 2. How do you find a proof ?
- 3. How do you write a proof?

Proposition:

Start with any number. If the number is even, divide it by 2. If it is odd, multiply it by 3 and add 1. If you repeat this process, it will lead you to 4, 2, 1.

Proof:

Many people have tried this, and no one came up with a counter-example.

Prepetition: Collatz Conjecture:

Start with any number. If the number is even, divide it by 2. If it is odd, multiply it by 3 and add 1. If you repeat this process, it will lead you to 4, 2, 1.

Proof:

Many people have tried this, and no one came up with a counter-example.

Proposition:

 $313(x^3 + y^3) = z^3$ has no solution for $x, y, z \in \mathbb{Z}^+$.

Proof:

Using a computer, we verified that there is no solution for numbers with < 500 digits.



$313(x^3 + y^3) = z^3$ has no solution for $x, y, z \in \mathbb{Z}^+$.



Proposition:

Given a solid ball in 3 dimensional space, there is no way to decompose it into a finite number of disjoint subsets, which can be put together to form two identical copies of the original ball.



Proof:

Obvious.

Banach-Tarski Theorem:

Given a solid ball in 3 dimensional space,

there **is a** way to decompose it into a finite number of disjoint subsets, which can be put together to form two identical copies of the original ball.

Proof:

Uses group theory... The pieces are such weird scatterings of points that they have no meaningful "volume"...

Proposition:

| + | = 2

Proof:

This is obvious???

Proposition:

| + | = 2

Proof:

This is obvious!!!

The story of 4 color theorem

1852 Conjecture:

Any 2-d map of regions can be colored with 4 colors so that no adjacent regions get the same color.





The story of 4 color theorem

- **1879:** Proved by Kempe in American Journal of Mathematics (was widely acclaimed)
- **1880:** Alternate proof by Tait in Trans. Roy. Soc. Edinburgh
- 1890: Heawood finds a bug in Kempe's proof
- **1891:** Petersen finds a bug in Tait's proof
- **1969:** Heesch showed the theorem could in principle be reduced to checking a large number of cases.

1976: Appel and Haken wrote a massive amount of code to compute and then check 1936 cases. (1200 hours of computer time)

The story of 4 color theorem

Much controversy at the time. Is this a proof?

What do you think?

Arguments against:

- no human could ever hand-check the cases
- maybe there is a bug in the code
- maybe there is a bug in the compiler
- maybe there is a bug in the hardware
- no "insight" is derived
- **1997**: Simpler computer proof by Robertson, Sanders, Seymour, Thomas

What is a mathematical proof?



a statement that is true or false

Euclidian geometry

5 AXIOMS

- I. Any two points can be joined by exactly one line segment.
- **2**. Any line segment can be extended into one line.
- **3**. Given any point P and length r, there is a circle of radius r and center P.

4. Any two right angles are congruent.

5. If a line L intersects two lines M and N, and if the interior angles on one side of L add up to less than two right angles, then M and N intersect on that side of L.

Euclidian geometry

Triangle Angle Sum Theorem

Pythagorean Theorem

Thales' Theorem







 $a^2 + b^2 = c^2$

Euclidian geometry

Pythagorean Theorem



Proof:



$$c^2 = (a+b)^2 - 2ab$$
$$= a^2 + b^2.$$



- I. Suppose $\sqrt{2}$ is rational. Then we can find $a, b \in \mathbb{N}$ such that $\sqrt{2} = a/b$.
- 2. If $\sqrt{2} = a/b$ then $\sqrt{2} = r/s$, where r and s are not both even. 3. If $\sqrt{2} = r/s$ then $2 = r^2/s^2$. 4. If $2 = r^2/s^2$ then $2s^2 = r^2$. 5. If $2s^2 = r^2$ then r^2 is even, which means r is even. 6. If r is even, r = 2t for some $t \in \mathbb{N}$. 7. If $2s^2 = r^2$ and r = 2t then $2s^2 = 4t^2$ and so $s^2 = 2t^2$. 8. If $s^2 = 2t^2$ then s^2 is even, and so s is even.

- I. Suppose $\sqrt{2}$ is rational. Then we can find $a, b \in \mathbb{N}$ such that $\sqrt{2} = a/b$.
- 2. If $\sqrt{2} = a/b$ then $\sqrt{2} = r/s$, where r and s are not both even. 3. If $\sqrt{2} = r/s$ then $2 = r^2/s^2$. 4. If $2 = r^2/s^2$ then $2s^2 = r^2$. 5. If $2s^2 = r^2$ then r^2 is even, which means r is even. 6. If r is even, r = 2t for some $t \in \mathbb{N}$. 7. If $2s^2 = r^2$ and r = 2t then $2s^2 = 4t^2$ and so $s^2 = 2t^2$. 8. If $s^2 = 2t^2$ then s^2 is even, and so s is even. 9. Contradiction is reached.

- I. Suppose $\sqrt{2}$ is rational. Then we can find $a, b \in \mathbb{N}$ such that $\sqrt{2} = a/b$.
- 2. If $\sqrt{2} = a/b$ then $\sqrt{2} = r/s$, where r and s are not both even. 3. If $\sqrt{2} = r/s$ then $2 = r^2/s^2$. 4. If $2 = r^2/s^2$ then $2s^2 = r^2$. 5. If $2s^2 = r^2$ then r^2 is even, which means r is even. 6. If r is even, r = 2t for some $t \in \mathbb{N}$. 7. If $2s^2 = r^2$ and r = 2t then $2s^2 = 4t^2$ and so $s^2 = 2t^2$. 8. If $s^2 = 2t^2$ then s^2 is even, and so s is even.
- 9. Contradiction is reached.

5a.
$$r^2$$
 is even. Suppose r is odd.
5b. So there is a number t such that $r = 2t + 1$.
5c. So $r^2 = (2t + 1)^2 = 4t^2 + 4t + 1$.
5d. $4t^2 + 4t + 1 = 2(2t^2 + 2t) + 1$, which is odd.
5e. So r^2 is odd.

5f. Contradiction is reached.

Odd number means not a multiple of 2.

Is every number a multiple of 2 or one more than a multiple of 2?

5b1. Call a number $r \mod if r = 2t$ or r = 2t + 1 for some t.

If
$$r = 2t$$
, $r + 1 = 2t + 1$.

If
$$r = 2t + 1$$
, $r + 1 = 2t + 2 = 2(t + 1)$.

Either way, r+1 is also good.

5b2. 1 is good since $1 = 0 + 1 = (0 \cdot 2) + 1$.

5b3. Applying 5b1 repeatedly, $2, 3, 4, \ldots$ are all good.

Axiom of induction:

Suppose for every positive integer n, there is a statement S(n).

If S(1) is true, and $S(n) \implies S(n+1)$ for any n, then S(n) is true for every n.

Can every mathematical theorem be derived from a set of agreed upon axioms?

A dream from late 19th and early 20th century.



After playing around, people realized you could seemingly do 100% of math using just the notions from set theory.

(Define natural numbers in terms of sets, ordered pairs in terms of sets, functions in terms of sets, sequences in terms of sets, real numbers, graphs, strings, automata, **everything** in terms of sets...)



Frege, 1893:

Proposes axioms for set theory. Spends 10 years writing two thick books about the system.

Russell, 1903:

"Your axioms allow me to define D = {x : x∉x}. Now if D∈D then D∉D. And if D∉D then D∈D. Inconsistency, boom!"





Frege, 1893:

Proposes axioms for set theory. Spends 10 years writing two thick books about the system.

Russell, 1903:

"Your axioms allow me to define D = {x : x∉x}. Now if D∈D then D∉D. And if D∉D then D∈D. Inconsistency, boom!"



Principia Mathematica Volume 2





Russell

Whitehead

Writing a proof like this is like writing a computer program in machine language.



AN EPIC SEARCH FOR TRUTH

APOSTOLOS DOXIADIS AND CHRISTOS H. PAPADIMITRIOU ART BY ALECOS PAPADATOS AND ANNIE DI DONNA

It became generally agreed that you **could** rigorously formalize mathematical proofs.

But nobody wants to. (by hand, at least)
Interesting consequence:

Proofs can be verified mechanically.

One last story



Lord Wacker von Wackenfels (1550 - 1619)



I6II:

Kepler as a New Year's present (!) for his patron, Lord Wacker von Wackenfels, wrote a paper with the following conjecture.

The densest way to pack oranges is like this:





Kepler as a New Year's present (!) for his patron, Lord Wacker von Wackenfels, wrote a paper with the following conjecture.

The densest way to pack spheres is like this:



2005: Pittsburgher Tom Hales submits a 120 page proof in Annals of Mathematics.

Plus code to solve 100,000 distinct optimization problems, taking 2000 hours computer time.



Annals recruited a team of 20 refs.They worked for 4 years.Some quit. Some retired. One died.In the end, they gave up.

They said they were "99% sure" it was a proof.



Hales: "I will code up a completely formal axiomatic deductive proof, <u>checkable by a computer</u>."

2004 - 2014: Open source "Project Flyspeck":

2015: Hales and 21 collaborators publish "A formal proof of the Kepler conjecture".

Formally proved theorems

- Fundamental Theorem of Calculus (Harrison)
- Fundamental Theorem of Algebra (Milewski)
- Prime Number Theorem (Avigad @ CMU, et al.)
- Gödel's Incompleteness Theorem (Shankar)
- Jordan Curve Theorem (Hales)
- Brouwer Fixed Point Theorem (Harrison)
- Four Color Theorem (Gonthier)
- Feit-Thompson Theorem (Gonthier)
- Kepler Conjecture (Hales++)

Summary / Bottom Line

In math, there are agreed upon rigorous rules for deduction. Proofs are either right or wrong.

Nevertheless, what constitutes an acceptable proof is a social construction.

(But computer science can help.)

What does this all mean for 15-251?

A proof is an argument that can withstand all criticisms from a highly caffeinated adversary (your TA).



Proof. Define f_{ij} as in (5). As f is symmetric, we only need to consider f_{12} .

$$\begin{split} \mathbf{E}\left[f_{12}^{2}\right] &= \mathbf{E}_{x_{3}\dots x_{n}}\left[\frac{1}{4}\cdot\left(f_{12}^{2}(00x_{3}\dots x_{n})+f_{12}^{2}(01x_{3}\dots x_{n})+f_{12}^{2}(10x_{3}\dots x_{n})+f_{12}^{2}(11x_{3}\dots x_{n})\right)\right] \\ &= \frac{1}{4}\mathbf{E}_{x_{3}\dots x_{n}}\left[\left(f(00x_{3}\dots x_{n})-f(11x_{3}\dots x_{n})\right)^{2}+\left(f(11x_{3}\dots x_{n})-f(00x_{3}\dots x_{n})\right)^{2}\right] \\ &\geq \frac{1}{2}\left(\binom{n-2}{r_{0}-1}\cdot 2^{-(n-2)}\cdot 4+\binom{n-2}{n-r_{1}-1}\cdot 2^{-(n-2)}\cdot 4\right) \\ &= 8\cdot\left(\frac{(n-r_{0}+1)(n-r_{0})}{n(n-1)}\cdot\binom{n}{r_{0}-1}+\frac{(n-r_{1}+1)(n-r_{1})}{n(n-1)}\cdot\binom{n}{r_{1}-1}\right)2^{-n}. \end{split}$$

Inequality (6) follows by applying Lemma 2.2.

In order to establish inequality (7), we show a lower bound on the principal Fourier coefficient of *f*:

$$\widehat{f}(\emptyset) \ge 1 - 2\left(\sum_{s < r_0} \binom{n}{s} + \sum_{s > n - r_1} \binom{n}{s}\right) 2^{-n},$$

which implies that

$$\widehat{f}(\emptyset)^2 \ge 1 - 4 \cdot \left(\sum_{s < r_0} \binom{n}{s} + \sum_{s < r_1} \binom{n}{s} \right) 2^{-n}.$$

I. What is a proof?

- 2. How do you find a proof ?
- 3. How do you write a proof?



No Eureka effect



Terence Tao

Fields Medalist, "MacArthur Genius",

I don't have any magical ability. ... When I was a kid, I had a romanticized notion of mathematics, that hard problems were solved in 'Eureka' moments of inspiration. [But] with me, it's always, 'Let's try this. That gets me part of the way, or that doesn't work. Now let's try this. Oh, there's a little shortcut here.' You work on it long enough and you happen to make progress towards a hard problem by a back door at some point. At the end, it's usually, 'Oh, I've solved the problem.'

Suggestions

Make 1% progress for 100 days. (Make 17% progress for 6 days.)

Understand the problem. (List what is given to you. Write down what you need to derive. Unpack definitions.)

Figure out some meaningful special cases (e.g. n = 1, n = 2).

Simplify the problem.

Put yourself in the mind of the adversary. (What are the worst-case examples/scenarios?)

Suggestions

Look at proofs from notes, recitations.

Give breaks, let the unconscious brain do some work.

Develop good notation.

Use paper, draw pictures.

Suggestions

Try different proof techniques.

- contrapositive $P \implies Q \iff \neg Q \implies \neg P$
- contradiction
- induction
- case analysis

Proof. Define f_{ij} as in (5). As f is symmetric, we only need to consider f_{12} .

$$\begin{split} \mathbf{E}\left[f_{12}^{2}\right] &= \mathbf{E}_{x_{3}\dots x_{n}}\left[\frac{1}{4}\cdot\left(f_{12}^{2}(00x_{3}\dots x_{n})+f_{12}^{2}(01x_{3}\dots x_{n})+f_{12}^{2}(10x_{3}\dots x_{n})+f_{12}^{2}(11x_{3}\dots x_{n})\right)\right] \\ &= \frac{1}{4}\mathbf{E}_{x_{3}\dots x_{n}}\left[\left(f(00x_{3}\dots x_{n})-f(11x_{3}\dots x_{n})\right)^{2}+\left(f(11x_{3}\dots x_{n})-f(00x_{3}\dots x_{n})\right)^{2}\right] \\ &\geq \frac{1}{2}\left(\binom{n-2}{r_{0}-1}\cdot 2^{-(n-2)}\cdot 4+\binom{n-2}{n-r_{1}-1}\cdot 2^{-(n-2)}\cdot 4\right) \\ &= 8\cdot\left(\frac{(n-r_{0}+1)(n-r_{0})}{n(n-1)}\cdot\binom{n}{r_{0}-1}+\frac{(n-r_{1}+1)(n-r_{1})}{n(n-1)}\cdot\binom{n}{r_{1}-1}\right)2^{-n}. \end{split}$$

Inequality (6) follows by applying Lemma 2.2.

In order to establish inequality (7), we show a lower bound on the principal Fourier coefficient of *f*:

$$\widehat{f}(\emptyset) \ge 1 - 2\left(\sum_{s < r_0} \binom{n}{s} + \sum_{s > n - r_1} \binom{n}{s}\right) 2^{-n},$$

which implies that

$$\widehat{f}(\emptyset)^2 \ge 1 - 4 \cdot \left(\sum_{s < r_0} \binom{n}{s} + \sum_{s < r_1} \binom{n}{s} \right) 2^{-n}.$$

I. What is a proof?

- 2. How do you find a proof?
- 3. How do you write a proof?

How do you write a proof?

http://www.cs.cmu.edu/~15251/docs/proof-checklist.pdf

<u>PART 2</u>

Course structure and how to succeed in 15-251

http://www.cs.cmu.edu/~I525I/docs/how-to-succeed.pdf

I. Lecture



3. Recitation



2. Course notes



4. Homework



I. Lecture

- provides background, motivation, insights, high-level picture.
- does **not** provide all the details.
- focus in lecture. take notes.

2. Course notes

- does **not** provide background and motivation.

- provides the details at the level you need to know them.

- fully understanding concepts and definitions is crucial!!

3. Recitation

- basically a small group review session.

- you'll be assigned a 50-minute time slot.

- you'll choose a spiciness level.







- come prepared.

4. Homework

- engagement with the material \rightarrow real learning

4. Homework

4 types of questions: SOLO, GROUP, OPEN COLLABORATION, PROGRAMMING

SOLO - work by yourself

GROUP - work in groups of 3 or 4

OPEN - work with anyone you would like from class

PROG - same rules as SOLO. submit to Autolab.

4. Homework

Homework comes out Thu night and contains:

SOLO + PROG problems from current week +

GROUP + OPEN problems from previous week

4. Homework

Homework writing sessions:

Wednesdays 6:30pm to 7:50pm at DH 2315

Write the solutions to a random subset of the problems. (usually 3 problems)

Practice writing the solutions beforehand!!!

Style matters!!!

4. Homework

Homework writing sessions:

You get 20% of the credit for the question if you write:

- nothing
- "I don't know", or
- "WTF!"

4. Homework

Homework Grading:



We are very happy even though there might be some minor errors.



General idea is correct, overall structure is good. But an non-trivial piece missing/incorrect



Good progress, but there are major gaps.

Needs to be redone.

4. Homework

Homework Grading:



4. Homework

Homework Grading:

Submit corrections or rewrites to receive back 50% of the lost credit.



Find the right group

Your group is going to be one of the most important parts of the course!

ADVICE FROM PREVIOUS 15-251 STUDENTS

If you leave enough time for 251 work, it won't be stressful, it'll just be fun. But you have to leave yourself a good amount of time.

Be proactive and don't procrastinate! Take advantage of office hours!

Go to office hours. They are helpful.

get ur shit together and don't be afraid to ask for help.

GO TO THE PROF'S OFFICE HOURS AT THE BEGINNING OF THE SEMESTER.

Read the notes and slides until you completely understand them, then understand the questions on the homework completely before trying to come up with an answer.

Understand course material before starting doing homework. Definitions are really really important for this class Pay attention in class, go to recitation, review the material every week, and go to office hours.
Choose your group carefully; make sure that you feel comfortable calling your group members lazy bums if necessary.

Find a good group, and expect to be spending a lot of time with them. A lot of the success or failure in the class will come from how well you can work together with your group so that during homework sessions you can all learn something. There will absolutely be problems or concepts which you don't understand as well as someone else in your group, and vice versa. That way you can teach each other, which is ideal. Also, if you get stumped, absolutely attend office hours. The TA's are generally quite helpful.

Think of it as a course that will give you a fantastic overview of CS theory — the ride will be tough, but try to focus less on the grades and more on enjoying understanding the material.

