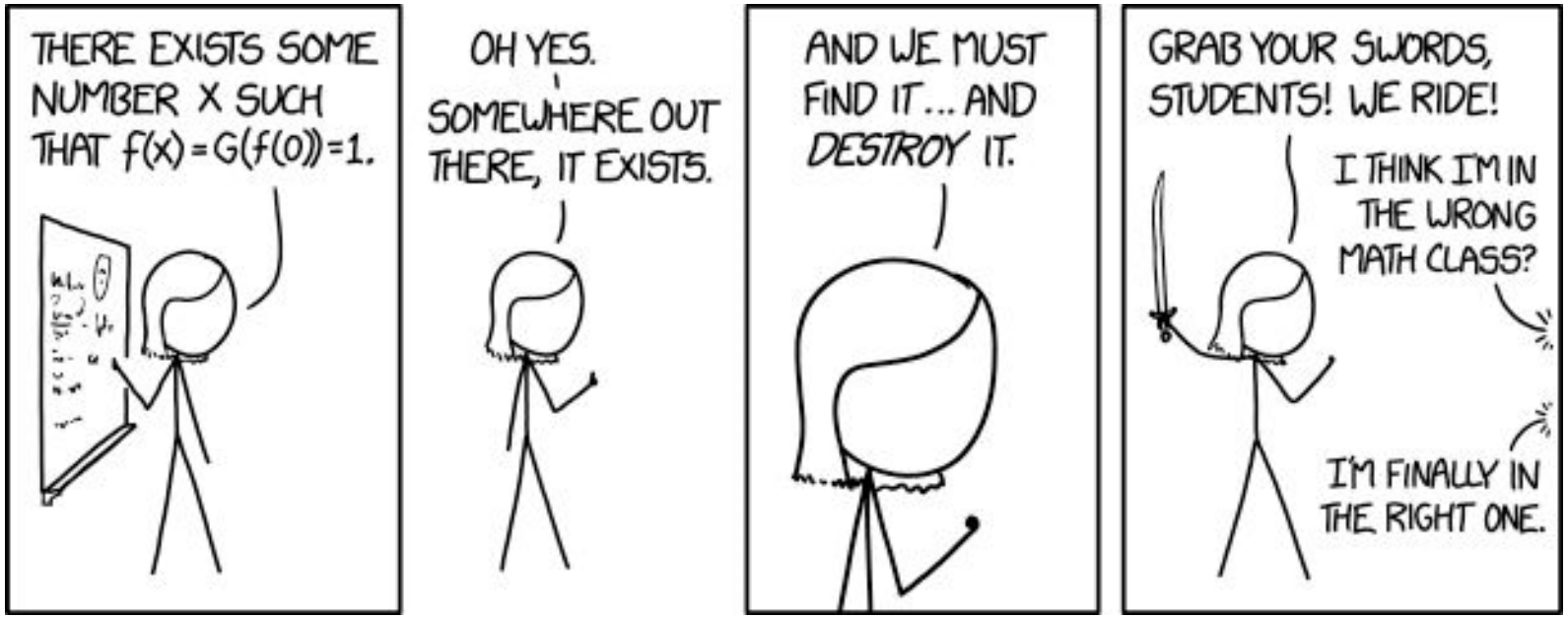
Warm Up: Shaking Hands

Suppose there are six people in a room. Some of them shake hands. Consider the claim:

There are at least three people who **all** shook each other's hands, or three people such that **no pair** of them shook hands.

Is it true? Can you prove or disprove it?

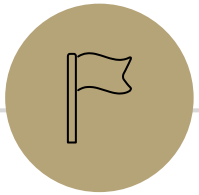


Proof by Cases, Existence Proof

CSE 311: Foundations of Computing I
Lecture 8

Announcements

- HW2 late deadline Friday at 11:59 pm
- HW3 posted, due next Wednesday at 11:59 pm



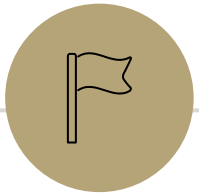
Review: Proof Strategies so Far

Proof Strategies So Far

- Direct Proof
  To show $\forall x\big(\mathrm{P}(x) \to \mathrm{Q}(x)\big)$, assume $\mathrm{P}(x)$ and prove $\mathrm{Q}(x)$.

- Proof by Contrapositive
  To show $\forall x\big(\mathrm{P}(x) \to \mathrm{Q}(x)\big)$, assume $\neg\mathrm{Q}(x)$ and prove $\neg\mathrm{P}(x)$.

- Proof of Biconditional
  To show $\forall x\big(\mathrm{P}(x) \leftrightarrow \mathrm{Q}(x)\big)$, write a proof in each direction.



Proof by Cases

Warm Up: Shaking Hands

Suppose there are six people in a room. Some of them shake hands. Consider the claim:

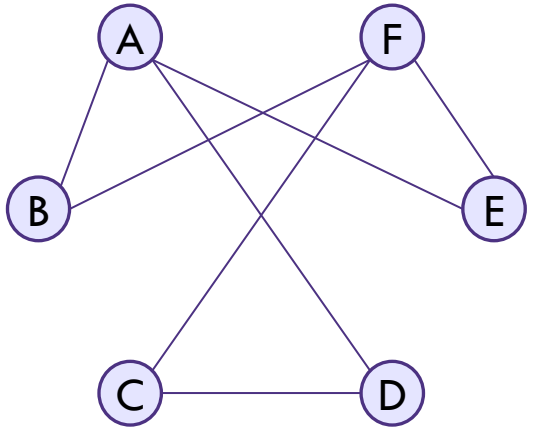
There are at least three people who **all** shook each other's hands, or three people such that **no pair** of them shook hands.

Is it true?

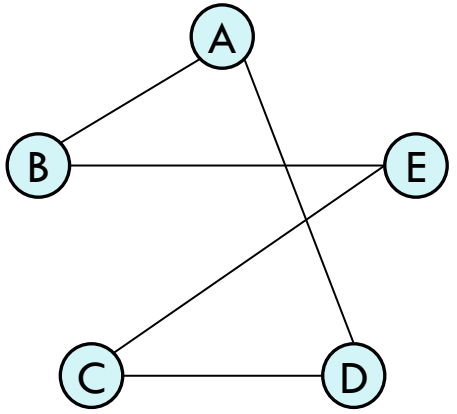
Warm Up: Shaking Hands

Suppose there are six people in a room. Some of them shake hands. Consider the claim:

There are at least three people who **all** shook each other's hands, or three people such that **no pair** of them shook hands.



Not obvious! Doesn't work with 5 people.



False

There are six people in a room. Prove that there are at least three people who **all** shook each other's hands, or three people such that **no pair** of them shook hands.

Choose one person, call them A. Note that A has 5 people around them.

Case 1: A shakes hands with 3+ people. Pick 3 of them, label them B, C, and D. If any of B, C, or D shake hands, we have a trio (including A) of 3 people who have all shaken. If none of them shake, we have a trio (B, C, D) who have all not shaken.

Case 2: A shakes hands with 2 or fewer people. Pick three of the people A did not shake with, call them X, Y, and Z. If any of X, Y, and Z did not shake, we have a trio (including A) who did not shake. If all of them shook, we have a trio that did shake.

In any case, the claim is true.

Proof by Cases

Proof by cases is the strategy of:

1. Breaking your assumption(s) into smaller cases.

   Be careful to make sure that your cases cover all of the possible scenarios. It's ok if they have overlap though.

2. Proving that the claim holds in **all** of these cases.

   Formally: $(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$.

5 numbers: Proof by Cases

$a+b=50$ $b>30$ $a<20$

Suppose that $x_1, \ldots, x_5$ are real numbers such that $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ and $x_1 + x_2 + x_3 + x_4 + x_5 = 50$. Prove that $x_1 + x_2 \leq 20$.

Let $x_1, \ldots, x_5$ be arbitrary real numbers. Suppose that $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ and $x_1 + \ldots + x_5 = 50$.

case 1: $x_2 \leq 10$. Since $x_1 \leq x_2$, then $x_1 \leq 10$. Adding:

$$x_1 + x_2 \leq 10+10 = 20$$

* case 2: $x_2 > 10$. Since $x_3, x_4, x_5 \geq x_2$ then $x_3 > 10$, $x_4 > 10$, $x_5 > 10$.

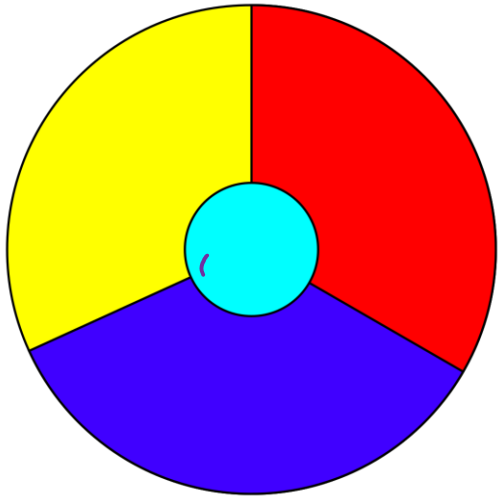
$$x_3 + x_4 + x_5 > 30$$

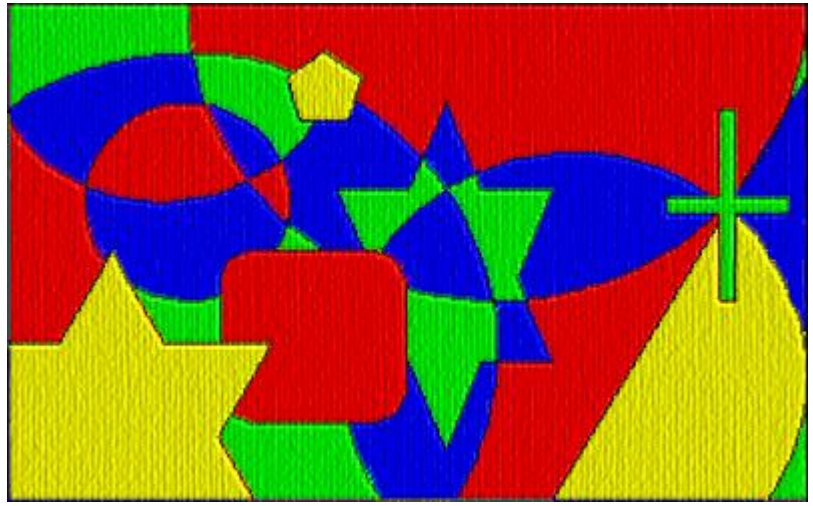
Since $x_3 + x_4 + x_5 > 30$ and $x_1 + \ldots + x_5 = 50$, $x_1 + x_2 < 20$.

The claim holds in all cases. Since $x_1, \ldots, x_5$ were arbitrary claim holds.

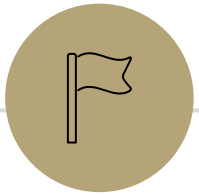
Four Color Theorem: Proof by Cases

Theorem (Four Color): Any plane surface with regions in it can be colored in four colors or less. Two regions that have a common border must not get the same color.





The first proof had 1,936 cases. The shortest known proof today has over 600 cases.



Existence Proof

Existence Proof

To prove $\exists x\, \mathrm{P}(x)$, we give one example of an x that makes P(x) true.

Existence Proof

There is some prime number p such that $p + 6$ and $p + 8$ are also prime.

Proof

Consider p=5. This is prime. p+6=11 which is also prime. And p+8=13 which is also prime.

When are Existence Proofs often helpful?

To **disprove** a claim, we prove the negation of the claim.

$\neg \forall x (P(x)) \equiv \exists x \neg P(x)$

Existence proofs are often helpful to disprove "for all" claims.

Another term for this is giving a counterexample.

Counterexamples

A single example can't *prove* a ∀ statement.

A single counterexample can *disprove* a ∀ statement.

For example, to disprove "all professors like pizza", you must find a professor who does not like pizza.

In formal logic:

$$\neg\forall x\big(\mathrm{P}(x)\to\mathrm{Q}(x)\big)$$

$$\equiv \neg\forall x\big(\neg\mathrm{P}(x)\vee\mathrm{Q}(x)\big) \quad \text{Law of Implication}$$

$$\equiv \exists x\neg\big(\neg\mathrm{P}(x)\vee\mathrm{Q}(x)\big) \quad \text{De Morgan's Law for Quantifiers}$$

$$\equiv \exists x\big(\mathrm{P}(x)\wedge\neg\mathrm{Q}(x)\big) \quad \text{De Morgan's law}$$

Counterexamples

$|a+1| = |b+1|$ (−6 ↙, 4 ↘)

For all real numbers a, b, c, if $|a + c| = |b + c|$, then $|a| = |b|$.

This claim is false. Disprove!

Disproof:

Consider $a = -6, b = 4, c = 1$. Certainly $|a| \neq |b|$ since $6 \neq 4$. Observe:

$$|a+c| = |-6+1| = |-5| = 5$$

$$|b+c| = |4+1| = |5| = 5$$

So, $|a+c| = |b+c|$ but $|a| \neq |b|$. This is a counterexample to the claim.

Counterexamples

U21
U31

canonical

32¢

You are given 1¢, 5¢, 10¢, 12¢ and 25¢ coins.

(4) 25¢, 5¢, 1¢, 1¢
(3) 12¢, 10¢, 10¢

Your boss says to make change with the least amount of coins, first use as many 25¢ coins that will fit, then 12¢ coins, then 10¢, then 5¢, then 1¢ cent.

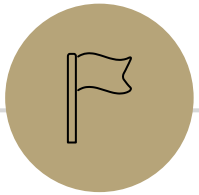
31¢: 25¢, 5¢, 1¢

Disprove this with a counterexample.

Consider 32¢. Then the boss's strategy would require:

25¢, 5¢, 1¢, 1¢ (4 coins)

But you can make 32¢ with 12¢, 10¢, 10¢ (3 coins).
So this strategy is not optimal.



Prove or Disprove

Prove or Disprove

- In practice, we don't usually know if a claim is true or false beforehand
- We want to prove the statement if it's true, and disprove it if it's false.
- Strategy:
  - Play around with many examples in an attempt to show that the claim is false
  - If the claim is false, hopefully you'll find a counterexample
  - If the claim is true, you'll gain intuition for why from the examples

Prove or Disprove

Identify if the following claims are true or false, and then prove or disprove.

1. For all positive integers n, $n^2 + 3n + 1$ is always prime.

1, 2, 3, 4, 5, 6 odd & even prime & composite

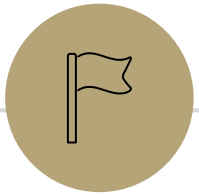
2. For all positive integers n, the sum $1 + 2 + \cdots + n$ is equal to $\frac{n(n+1)}{2}$.

3. For every real number n, $n^2 \geq n$.

4. For an integer n, $3n^2 + n + 10$ is always even.

n odd
n even

n pos
n neg
n 0



Computer-Verifiable Proofs

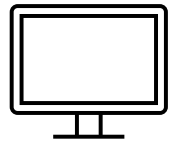
Recall: Proofs are written for an audience

Computer Science Theorist

"The proof is clear ☺"

English proofs

us!



Computer

Possibly many steps to show $1 + 1 = 2$

Computer-Verifiable Proofs

How do they work?

1. Write down all the facts that we know.
2. Combine facts into new facts using a set of known rules.

   Example Rule: Modus Ponens

   If $p \to q$ and p are known, then q is known

3. Continue until we reach what we want to show.

$P \wedge Q$

P

Computer-Verifiable Proofs

If n and m are odd, then $n + m$ is even.

1.	Let x be an arbitrary integer.		
2.	Let y be an arbitrary integer.		
	3.1.	$\text{Odd}(x) \wedge \text{Odd}(y)$	[Assumption]
	3.2.	$\text{Odd}(x)$	[Elim $\wedge$: 3.1]
	3.3.	$\exists k\ (x = 2k + 1)$	[Definition of Odd, 3.2]
	3.4.	$x = 2k + 1$	[Elim $\exists$: 3.3]
	3.5.	$\text{Odd}(y)$	[Elim $\wedge$: 3.1]
	3.6.	$\exists k\ (y = 2k + 1)$	[Definition of Odd, 3.5]
	3.7.	$y = 2j + 1$	[Elim $\exists$: 3.7]
	3.8.	$x + y = 2k + 1 + 2j + 1$	[Algebra: 3.4, 3.7]
	3.9.	$x + y = 2(k + j + 1)$	[Algebra: 3.8]
	3.10.	$\exists r\ (x + y = 2r)$	[Intro $\exists$: 3.9]
	3.11.	$\text{Even}(x + y)$	[Definition of Even, 3.10]
3.	$\text{Odd}(x) \wedge \text{Odd}(y) \rightarrow \text{Even}(x + y)$		[Direct Proof Rule]
4.	$\forall m(\text{Odd}(x) \wedge \text{Odd}(m) \rightarrow \text{Even}(x + m))$		[Intro $\forall$: 2,3]
5.	$\forall n \forall m(\text{Odd}(n) \wedge \text{Odd}(m) \rightarrow \text{Even}(n + m))$		[Intro $\forall$: 1,4]