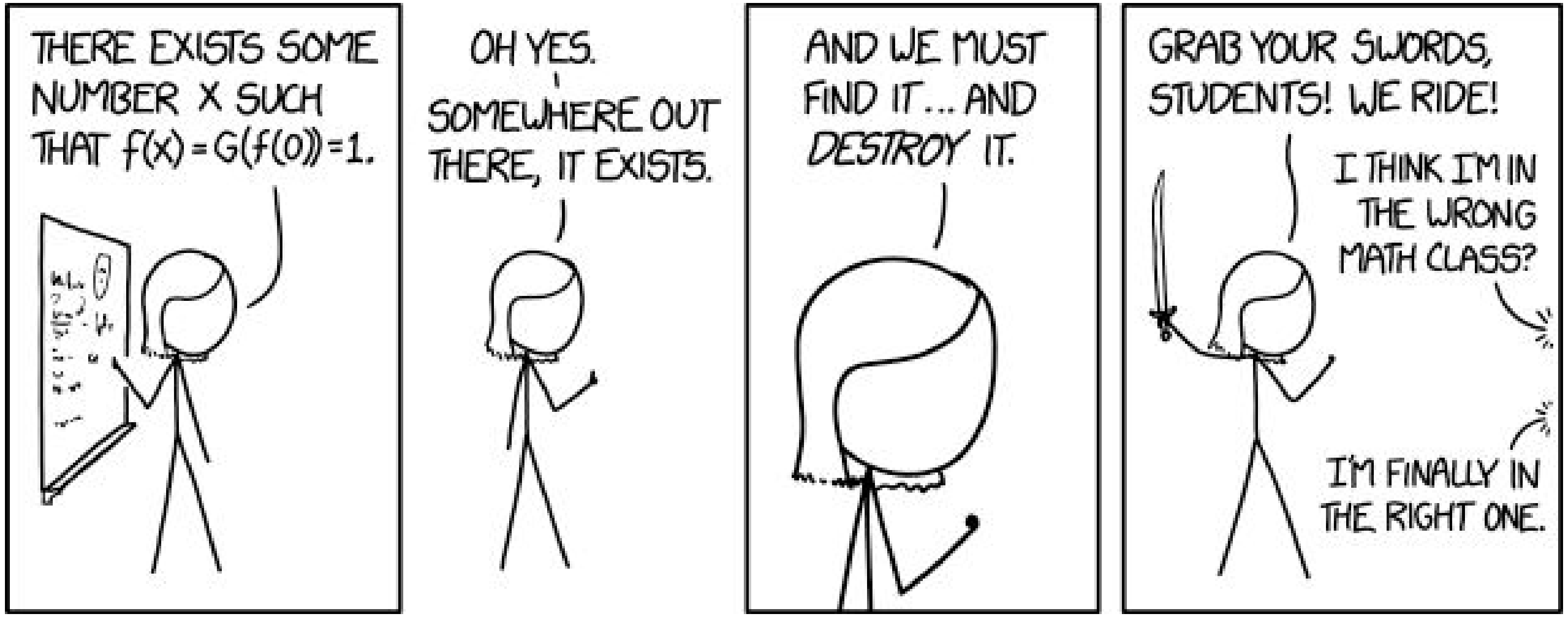
Warm Up: Shaking Hands

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?



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 $\forall x\big(P(x) \rightarrow Q(x)\big)$, assume $P(x)$ and prove $Q(x)$.

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

- Proof of Biconditional
  To show $\forall x\big(P(x) \leftrightarrow Q(x)\big)$, 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:

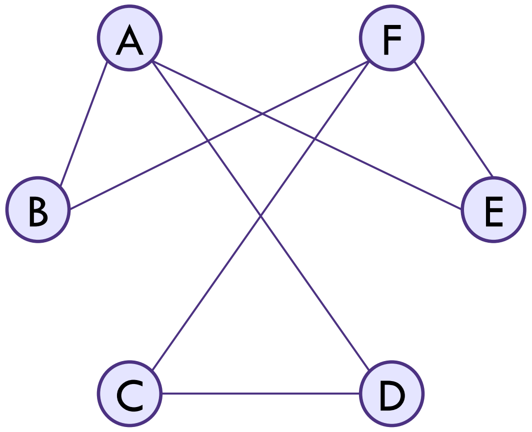
There are at least three people who **all** shook each other's hands, or three people such that **no pair** of them shook hands.

Is it true?

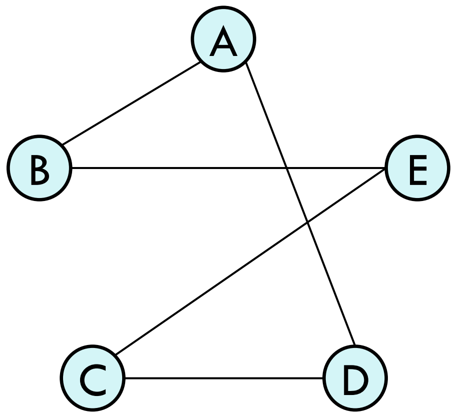
Warm Up: Shaking Hands

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.



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 in the room.

Case 1: A shook 3 or more of the others' hands. Pick three of them, call them B,C,D. Then if **any** of B, C or D shook hands with each other, we have 3 people who have all shaken hands. If none of B, C, or D shook hands with each other, then we have 3 people who have not shaken any hands.

Case 2: A shook 2 or fewer of the others' hands. Pick three of the people A did not shake hands with, and call them X, Y, Z. Then if any of X, Y, Z also did not shake with each other, we have 3 people who have all not shaken hands. If all of X, Y, or Z shook hands with each other, then we have 3 people who have all shaken hands.

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

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

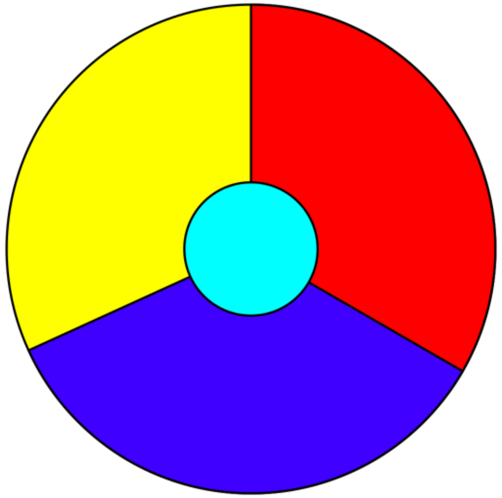
Case 1: $x_2 \leq 10$. Then since $x_1 \leq x_2, x_1 \leq 10$. So $x_1 + x_2 \leq 20$, as desired.

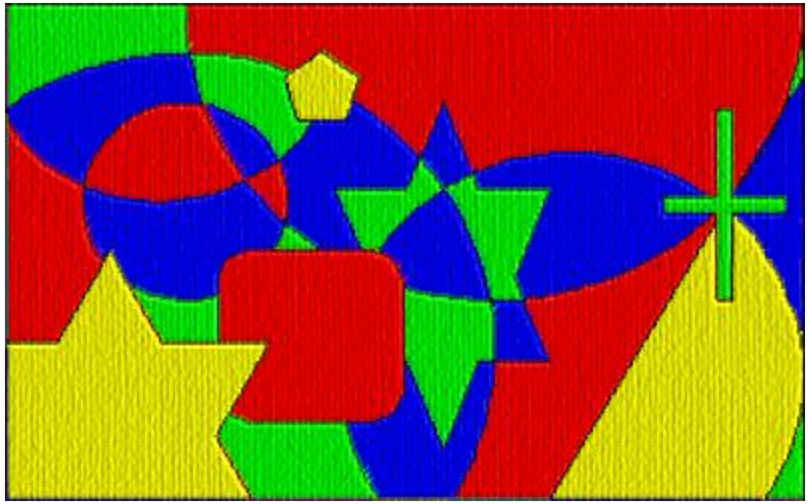
Case 2: $x_2 > 10$. Then since $x_3, x_4, x_5 \geq x_2$, we have that $x_3 > 10, x_4 > 10, x_5 > 10$. So $x_3 + x_4 + x_5 > 30$. Thus $x_1 + x_2 < 20$, as desired.

Since $x_1, \ldots, x_5$ were arbitrary, the 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 x in the domain that makes $\mathrm{P}(x)$ true.

Existence Proof

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

$\exists p \left(\text{Prime}(p) \land \text{Prime}(p + 6) \land \text{Prime}(p + 8) \right)$

Consider $p = 5$. Then $p + 6 = 11$ is also prime, as is $p + 8 = 13$.

When are Existence Proofs often helpful?

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

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:

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

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

$$\equiv \exists x\big(P(x) \wedge \neg Q(x)\big) \quad \text{DeMorgan's Law}$$

Counterexamples

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

This claim is false. Disprove!

Consider $a = -6, b = 4, c = 1$. Certainly $|a| \neq |b|$. Observe that:
$|a + c| = |-6 + 1| = |-5| = 5$

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

So this is a counterexample to the claim.

Counterexamples

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

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.

Disprove this with a counterexample.

Consider making $21¢$ of change. Your boss's strategy would involve using $12¢$, $5¢$, $1¢$, $1¢$, $1¢$, $1¢$ coins, i.e. 6 coins. However you can make this much change using only 3 coins: $10¢$, $10¢$, $1¢$.

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.
   False: e.g. $n = 6$ gives $36 + 18 + 1 = 55$.

2. For all positive integers n, the sum $1 + 2 + \cdots + n$ is equal to $\frac{n(n+1)}{2}$.
   True. Hint to prove: regroup $1 + 2 + \cdots + n - 1 + n$ into pairs $(1 + n) + (2 + (n - 1)) + \cdots$

3. For every real number n, $n^2 \geq n$.
   False: e.g. $n = \frac{1}{2}$, since $\frac{1}{4} < \frac{1}{2}$.

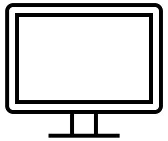
4. For an integer n, $3n^2 + n + 10$ is always even.
   True. Hint to prove: break into the cases that n is even and n is false.

Computer-Verifiable Proofs

Recall: Proofs are written for an audience

Computer Science Theorist

"The proof is clear ☺"



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 $p \rightarrow q$ and p are known, then q is known
3. Continue until we reach what we want to show.

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]