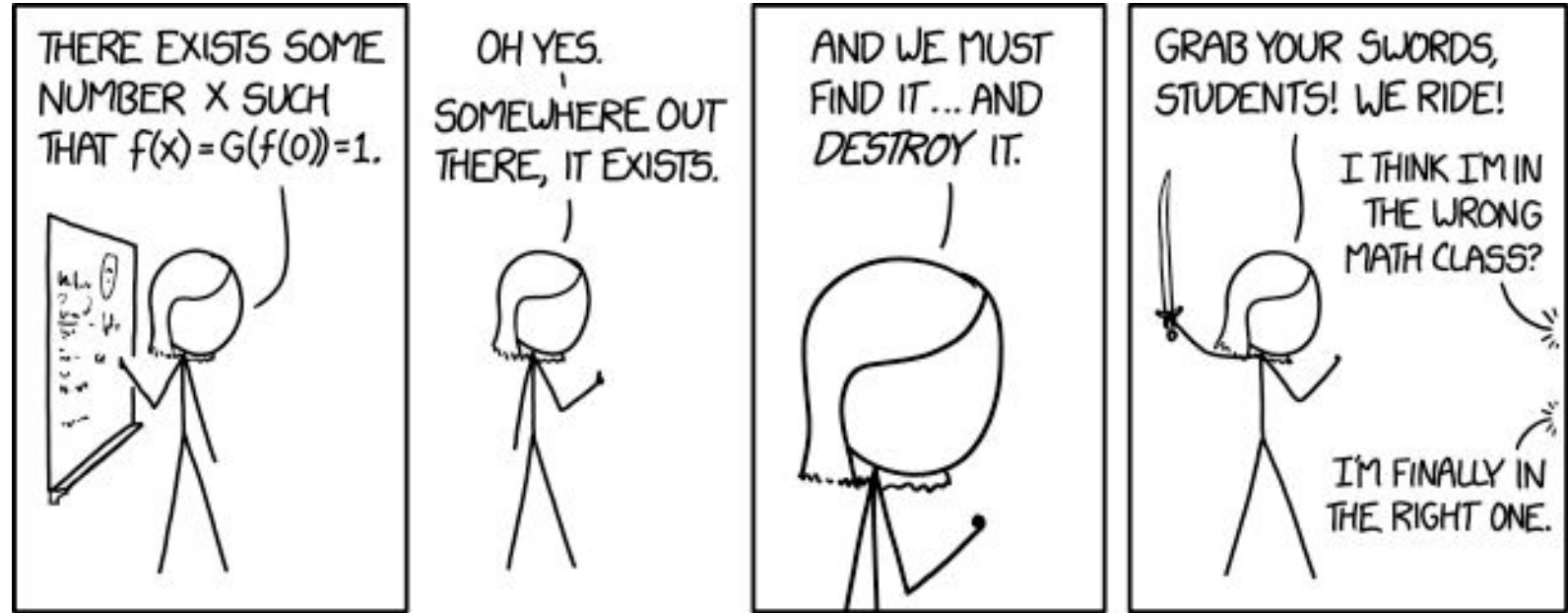


# Warm Up: Shaking Hands

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?

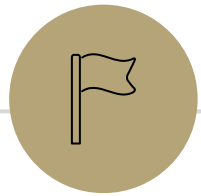


# Proof by Cases, Existence Proof

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

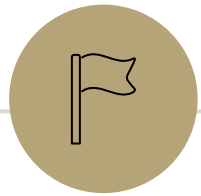
To show  $\forall x(P(x) \rightarrow Q(x))$ , assume  $P(x)$  and prove  $Q(x)$ .

- Proof by Contrapositive

To show  $\forall x(P(x) \rightarrow Q(x))$ , assume  $\neg Q(x)$  and prove  $\neg P(x)$ .

- Proof of Biconditional

To show  $\forall x(P(x) \leftrightarrow Q(x))$ , 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:

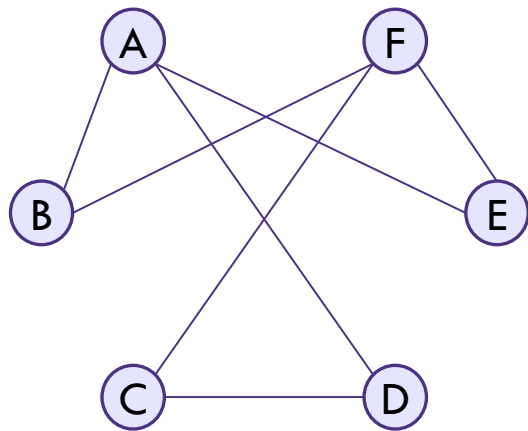
There are at least three people who **all** shook each other's hands, or three people such that **no pair** of them shook hands.

Is it true?

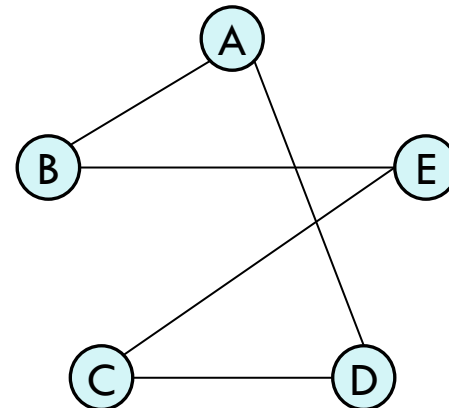
# Warm Up: Shaking Hands

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.

# 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.

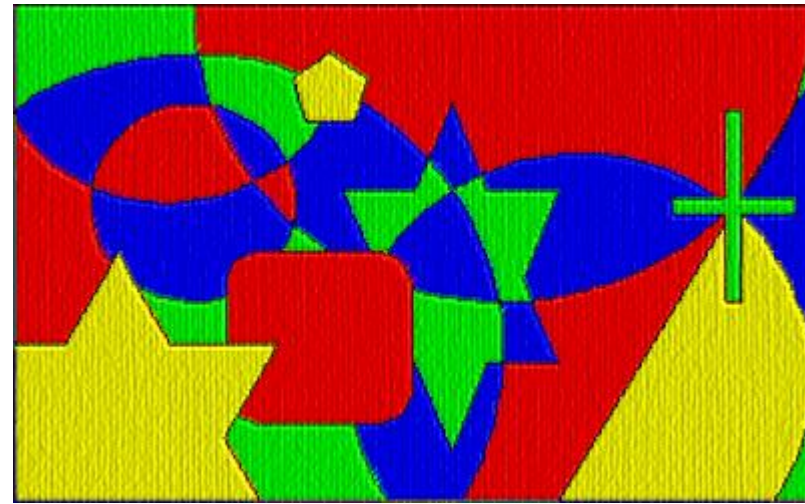
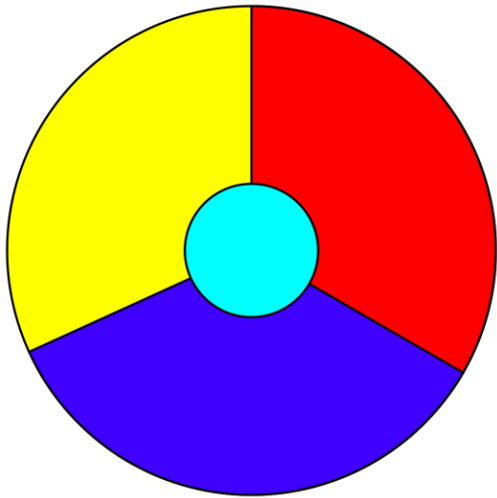
Formally:  $(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$ .

# 5 numbers: Proof by Cases

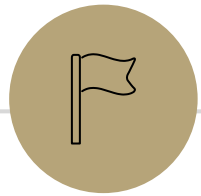
Suppose that  $x_1, \dots, x_5$  are real numbers such that  $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$  and  $x_1 + x_2 + x_3 + x_4 + x_5 = 50$ . Prove that  $x_1 + x_2 \leq 20$ .

# 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  $\exists x P(x)$ , we \_\_\_\_\_.

# Existence Proof

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

# When are Existence Proofs often helpful?

To **disprove** a claim, we \_\_\_\_\_.

Existence proofs are often helpful to \_\_\_\_\_.

Another term for this is \_\_\_\_\_.

# Counterexamples

A single example can't *prove* a  $\forall$  statement.

A single counterexample can *disprove* a  $\forall$  statement.

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

In formal logic:

$$\begin{aligned}\neg\forall x(P(x) \rightarrow Q(x)) &\equiv \neg\forall x(\neg P(x) \vee Q(x)) && \text{Law of Implication} \\ &\equiv \exists x\neg(\neg P(x) \vee Q(x)) && \text{DeMorgan's Law for Quantifiers} \\ &\equiv \exists x(P(x) \wedge \neg Q(x)) && \text{DeMorgan's Law}\end{aligned}$$

# Counterexamples

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

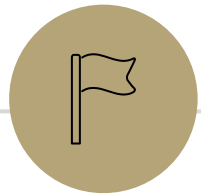
This claim is false. Disprove!

# 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.



**Prove or Disprove**

---

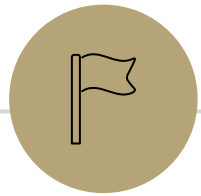
# Prove or Disprove

- 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.
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.



# Computer-Verifiable Proofs

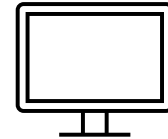
---

# 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]