Indirect Proofs

Outline for Today

- **Preliminaries**
  - Disproving statements
  - Mathematical implications
- **Proof by Contrapositive**
  - The basic method.
  - An interesting application.
- **Proof by Contradiction**
  - The basic method.
  - Contradictions and implication.
  - Contradictions and quantifiers.

Disproving Statements

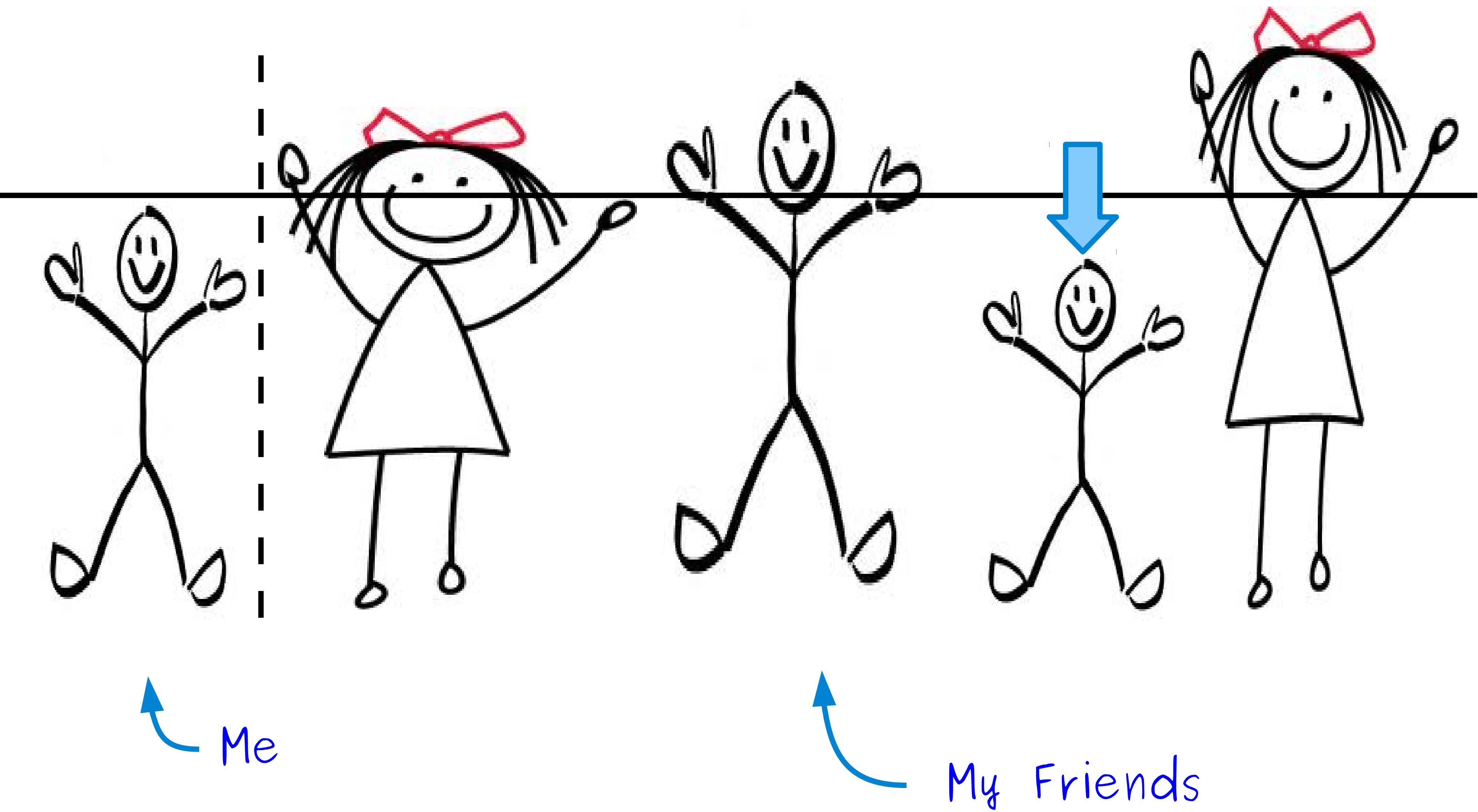
Proofs and Disproofs

- A proof is an argument establishing why a statement is true.
- A ***disproof*** is an argument establishing why a statement is *false*.
- Although proofs generally are more famous than disproofs, mathematics heavily relies on disproofs of conjectures that have turned out to be false.

Writing a Disproof

- The easiest way to disprove a statement is to write a proof of the opposite of that statement.
  - The opposite of a statement X is called the ***negation*** of statement X.
- A typical disproof is structured as follows:
  - Start by stating that you're going to disprove some statement X.
  - Write out the negation of statement X.
  - Write a normal proof that statement X is false.

"All My Friends Are Taller Than Me"



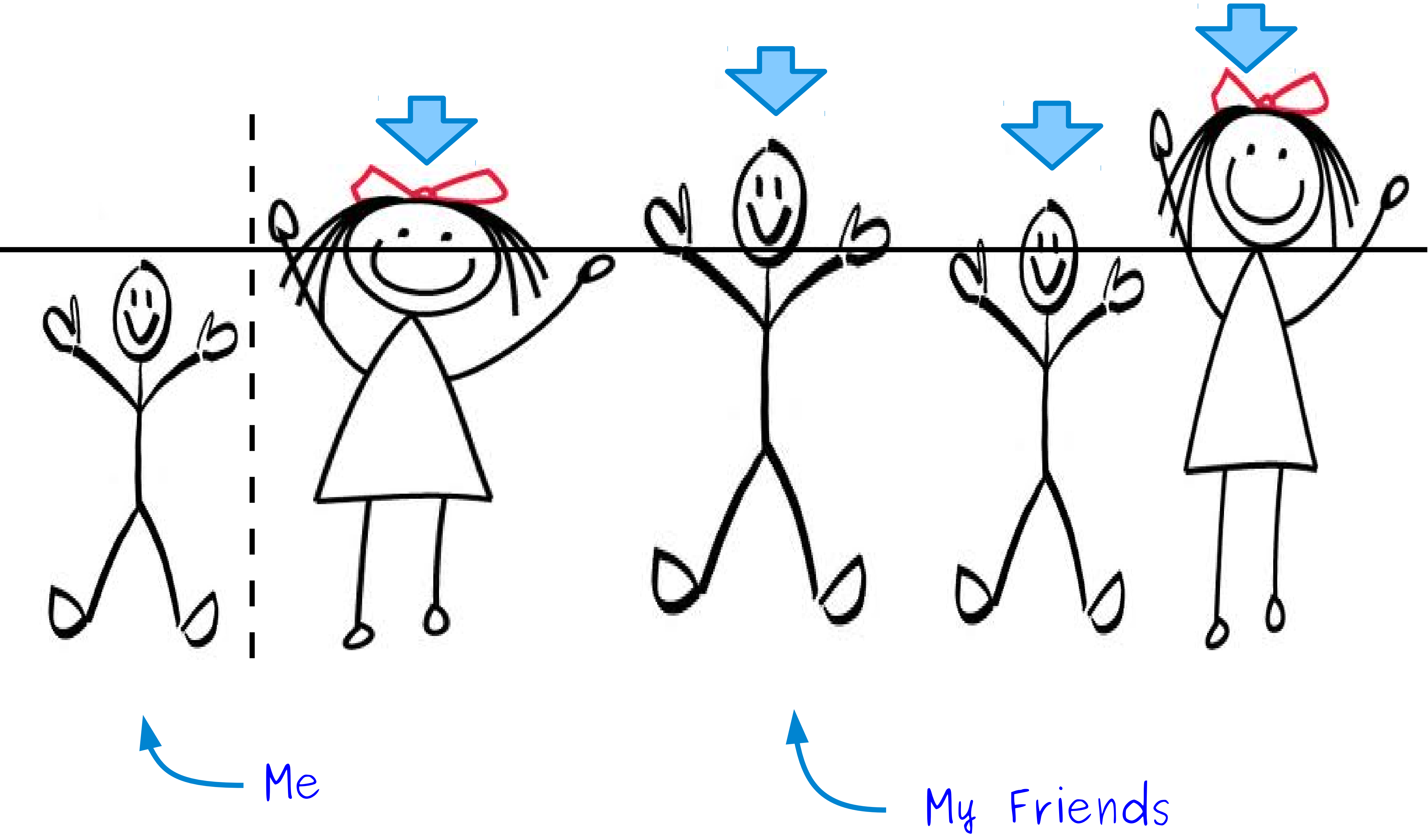
The negation of the *universal* statement

For all x, $P(x)$ is true.

is the *existential* statement

There exists an x where $P(x)$ is false.

“Some Friend Is Shorter Than Me”



The negation of the *existential* statement

There exists an *x* where *P*(*x*) is true.

is the *universal* statement

For all *x*, *P*(*x*) is false.

What would we have to show to disprove the following statement?

"Some set is the same size as its power set."

First, is this an existential statement or a universal statement?

"Some set is the same size as its power set."

First, is this an existential statement or a universal statement?

"Some set is the same size as its power set."

First, is this an existential statement or a universal statement?

"There is a set S where S is the same size as its power set."

What happens when you negate an existential statement?

"There is a set S where S is the same size as its power set."

What happens when you negate an existential statement?

"For any set S, the set S is ***not*** the same size as its power set."

This is what we need to prove
to disprove the original statement.

"For any set S, the set S is ***not*** the same size as its power set."

Logical Implication

Implications

- An **implication** is a statement of the form

  If P is true, then Q is true.

- Some examples:
  - If n is an even integer, then n^2 is an even integer.
  - If $A \subseteq B$ and $B \subseteq A$, then $A = B$.
  - If you liked it, then you should've put a ring on it.

Implications

- An **implication** is a statement of the form

If P is true, then Q is true.

- In the above statement, the term "P is true" is called the ***antecedent*** and the term "Q is true" is called the ***consequent***.

What Implications Mean

- Consider the simple statement

  If I put fire near cotton, it will burn.

- Some questions to consider:
  - Does this apply to all fire and all cotton, or just some types of fire and some types of cotton? *(Scope)*
  - Does the fire cause the cotton to burn, or does the cotton burn for another reason? *(Causality*)
- These are deeper questions than they might seem.
- To mathematically study implications, we need to formalize what implications really mean.

What Implications Mean

- In mathematics, the statement

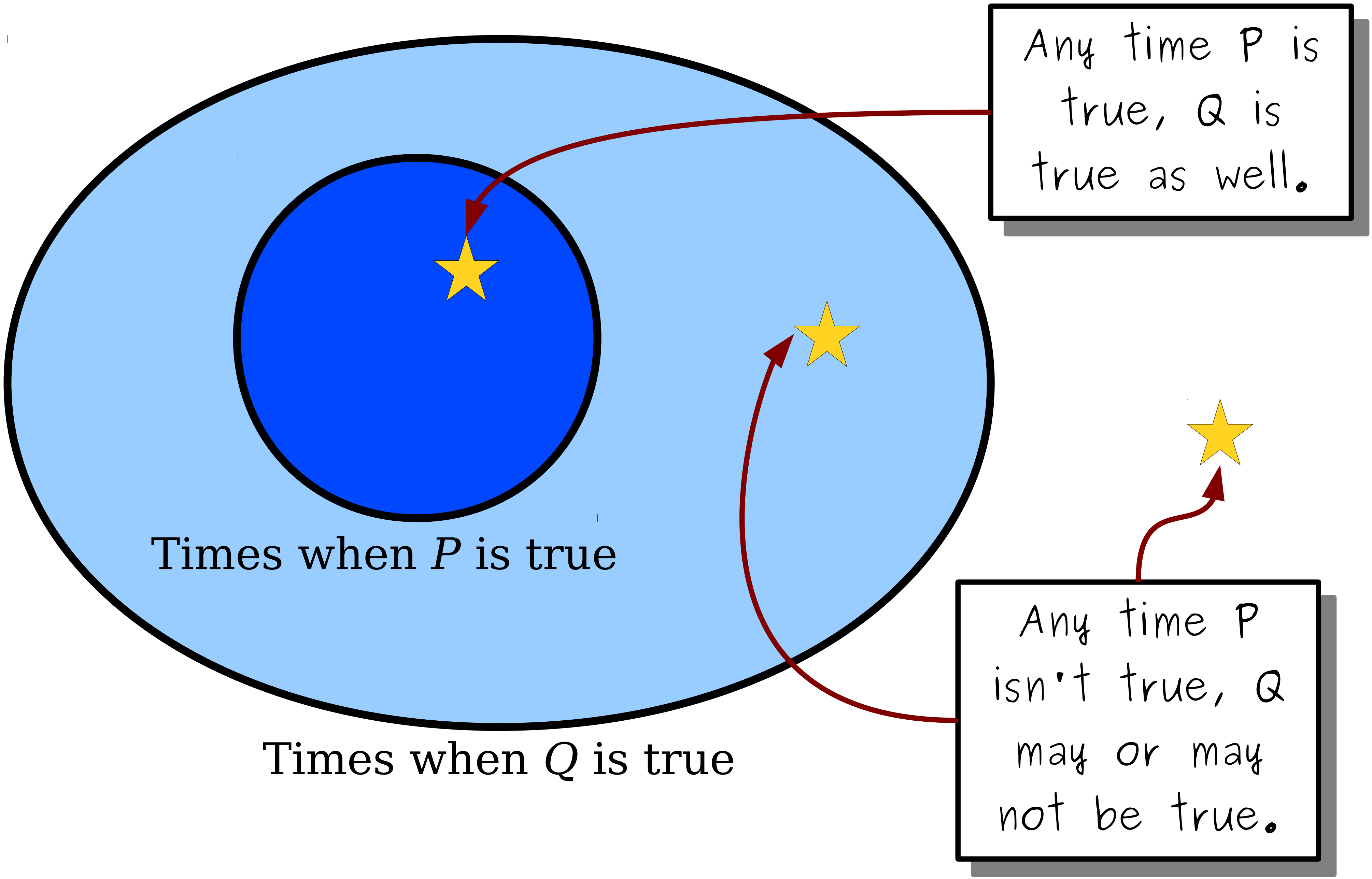
  If *P* is true, then *Q* is true.

  means *exactly* the following:

  Any time *P* is true, we are guaranteed that *Q* must also be true.

- There is no discussion of correlation or causation here. It simply means that if you find that *P* is true, you'll find that *Q* is true.

Implication, Diagrammatically



What Implication Doesn't Mean

- Implication is directional.
  - "If you die in Canada, you die in real life" doesn't mean that if you die in real life, you die in Canada.
- Implication only cares about cases where the antecedent is true.
  - "If an animal is a puppy, you should hug it" doesn't mean that if the animal is *not* a puppy, you *shouldn't* hug it.
- Implication says nothing about causality.
  - "If I like math, then 2 + 2 = 4" is true because any time I like math, we'll find that 2 + 2 = 4.
  - "If I hate math, then 2 + 2 = 4" is also true because any time I hate math, we'll find that 2 + 2 = 4.

Puppies Are Adorable

- Consider the statement

If *x* is a puppy, then I love *x*.

- Can you explain why the following statement is *not* the negation of the original statement?

If *x* is a puppy, then I don't love *x*.

- This second statement is too strong.
- Here's the correct negation:

There is some puppy *x* that I don't love.

The negation of the statement

“If P is true, then Q is true”

is the statement

“There are times when P is true and Q is false.”

Proof by Contrapositive

Honk **If** You Love Formal Logic

Suppose that you're driving this car and you *don't* get honked at.

What can you say about the people driving behind you?

The Contrapositive

- The ***contrapositive*** of the implication "If P, then Q" is the implication "If ***not*** Q, then ***not*** P."
- For example:
  - "If I store the cat food inside, then the raccoons will not steal my cat food."
  - Contrapositive: "If the raccoons stole my cat food, then I didn't store it inside."
- Another example:
  - "If Harry had opened the right book, then Harry would have learned about Gillyweed."
  - Contrapositive: "If Harry didn't learn about Gillyweed, then Harry didn't open the right book."

To prove the statement

If *P* is true, then *Q* is true

You may instead prove the statement

If *Q* is false, then *P* is false.

This is called a ***proof by contrapositive***.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

We're starting this proof by telling the reader that it's a proof by contrapositive. This helps cue the reader into what's about to come next.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive;

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Here, we're explicitly writing out the contrapositive. This tells the reader what we're going to prove. It also acts as a sanity check by forcing us to write out what we think the contrapositive is.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

We've said that we're going to prove this new implication, so let's go do it! The rest of this proof will look a lot like a standard direct proof.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$n^2 = (2k + 1)^2$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. Therefore, n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. Therefore, n^2 is odd. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2k + 1$. Squaring both sides of this equality and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. Therefore, n^2 is odd. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: By contrapositive; we prove that if n is odd, then n^2 is odd.

Since n is odd, there is some integer k such that $n = 2$

and s

From

(nam

There

The general pattern here is the following:

1. Start by announcing that we're going to use a proof by contrapositive so that the reader knows what to expect.

2. Explicitly state the contrapositive of what we want to prove.

3. Go prove the contrapositive.

Biconditionals

- Combined with what we saw on Wednesday, we have proven that, if n is an integer:

  If n is even, then n^2 is even.

  If n^2 is even, then n is even.

- Therefore, if n is an integer:

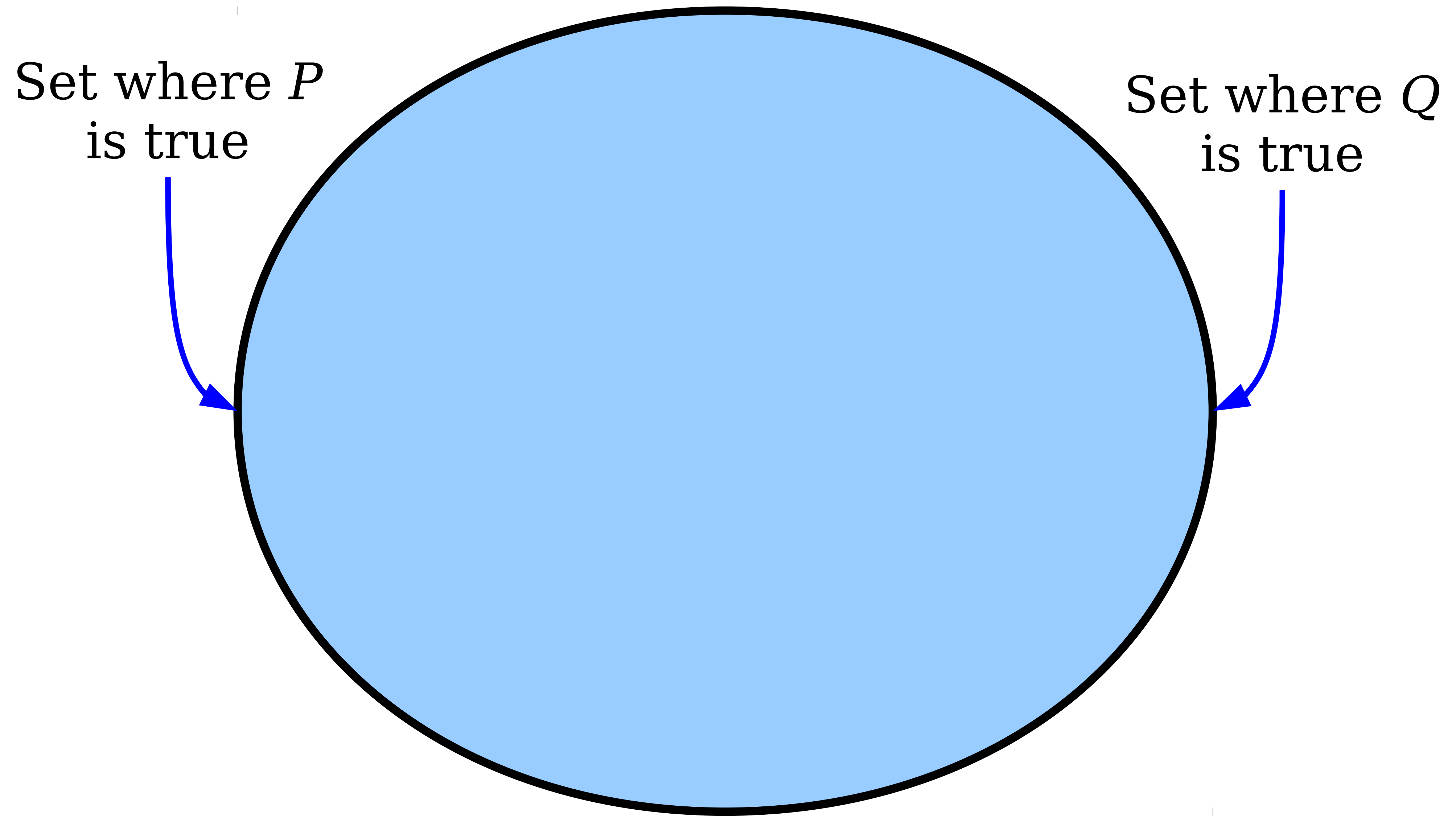
  n is even if and only if n^2 is even.

- "If and only if" is often abbreviated **iff**:

  n is even iff n^2 is even.

- This is called a **biconditional**.

P iff Q



Proving Biconditionals

- To prove ***P* iff *Q***, you need to prove that P implies Q and that Q implies P.
- You can any proof techniques you'd like to show each of these statements.
  - In our case, we used a direct proof and a proof by contrapositive.

Time-Out for Announcements!

Announcements

- Problem Set 1 out.
- **Checkpoint** due Monday, September 29.
  - Grade determined by attempt rather than accuracy. It's okay to make mistakes – we want you to give it your best effort, even if you're not completely sure what you have is correct.
  - We will get feedback back to you with comments on your proof technique and style.
  - The more an effort you put in, the more you'll get out.
- **Remaining problems** due Friday, October 3.
  - Feel free to email us with questions!

Submitting Assignments

- As a pilot for this quarter, we'll be using ***Scoryst*** for assignment submissions.
- All submissions should be electronic. If you're having trouble submitting, please contact the course staff.
- Signup link available at the course website.
- Late policy:
  - One “late period” that extends due date by one class period.
  - Work submitted late beyond a late period will have its score multiplied by 0.75.
  - No work accepted more than one class period after the due date.

Working in Groups

- You can work on the problem sets individually, in a pair, or in a group of three.
- Each group should only submit a single problem set, and should submit it only once.
- Full details about the problem sets, collaboration policy, and Honor Code can be found in Handouts 02 and 03.

Looking for a diverse community within engineering and science at Stanford? Join one of Stanford Engineering's diversity societies!

American Indian Science and Engineering Society

Meetings
Every Monday,
12:00 Noon,
at NACC

Society of Black Scientists and Engineers

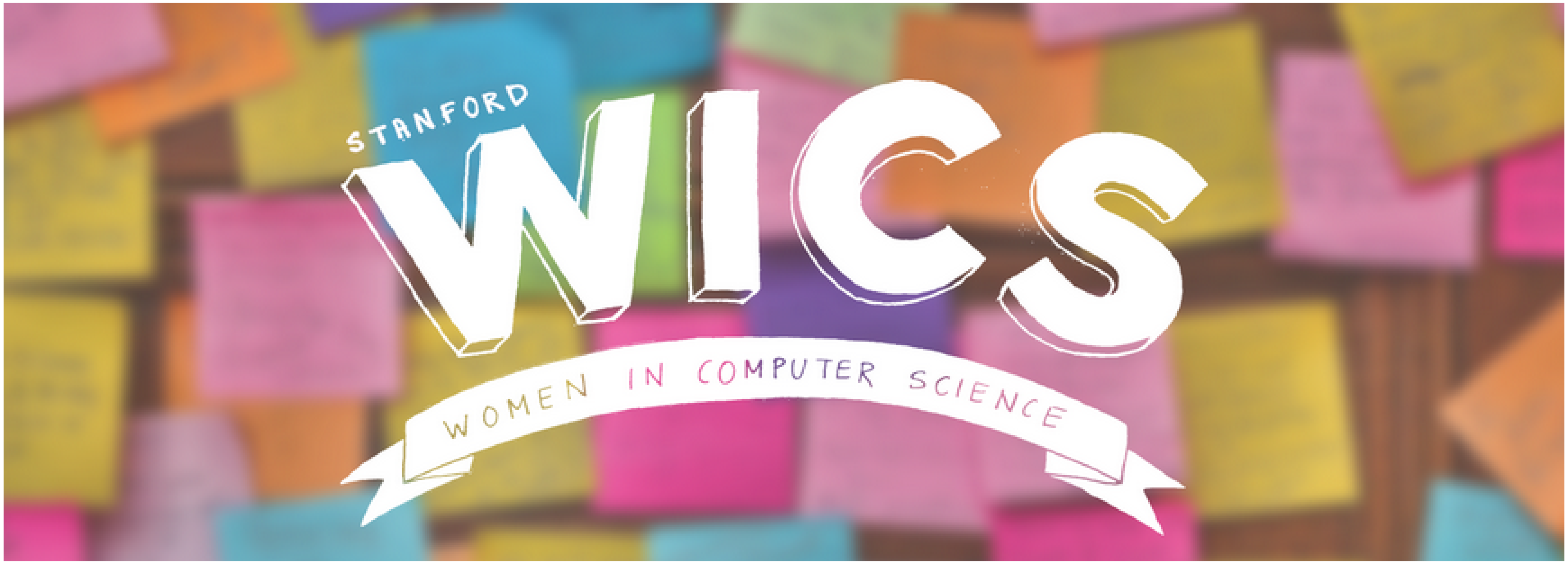
Meetings
Every Tuesday,
12:00 Noon,
at BCSC

Society of Women Engineers

Meetings
Every Wednesday,
12:00 Noon,
at MERL
(Building 660,
Second Floor)

Society of Latino Engineers

Meetings
Every Friday,
12:00 Noon,
at BCSC



Want a hand in **shaping** Stanford's own Women in CS **community**?

Apply to be an **intern** for WICS by **Oct 4**!
Freshmen and grad students encouraged to apply!

Applications at http://bit.ly/1xjDMLB.
Questions? Email theodora@stanford.edu

Office hours start Monday.

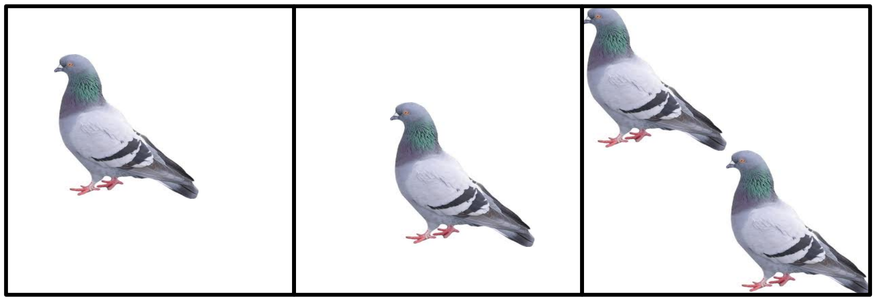
Schedule will be available
on the course website.

Back to CS103!

The Pigeonhole Principle

The Pigeonhole Principle

- Suppose that you have n pigeonholes.
- Suppose that you have $m > n$ pigeons.
- If you put the pigeons into the pigeonholes, some pigeonhole will have more than one pigeon in it.



The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then "$m > n$" is false.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false,
then "$m > n$" is false.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false,
then $m \leq n$.

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

If “some bin contains at least two objects” is false, then $m \leq n$.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

Is this a universal statement or an existential statement?

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If "some bin contains at least two objects" is false, then $m \leq n$.

How do you take the negation of an existential statement?

The Pigeonhole Principle

Suppose that m objects are distributed into n bins.

We want to prove the statement

If $m > n$, then some bin contains at least two objects.

What is the contrapositive of this statement?

If every bin contains at most one object,
then $m \leq n$.

How do you take the negation of an existential statement?

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

If every bin contains at most one object,
then $m \leq n$.

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

  If every bin contains at most one object, then $m \leq n$.

The Pigeonhole Principle

- Suppose that m objects are distributed into n bins.
- We want to prove the statement

  If $m > n$, then some bin contains at least two objects.

- What is the contrapositive of this statement?

  If every bin contains at most one object, then $m \leq n$.

- Look at the definitions of m and n. Does this make sense?

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains at least two objects.

Proof: By contrapositive; we prove that if every bin contains at most one object, then $m \leq n$.

Let x_i denote the number of objects in bin i. Since m is the number of total objects, we see that

$$m = x_1 + x_2 + \ldots + x_n.$$

We're assuming every bin has at most one object. In our notation, this means that $x_i \leq 1$ for all i. Using this inequalities, we get the following:

$$\begin{aligned} m &= x_1 + x_2 + \ldots + x_n \\ &\leq 1 + 1 + \ldots + 1 \qquad (n \textit{ times}) \\ &= n. \end{aligned}$$

So $m \leq n$, as required. ■

Some Simple Applications

- Any group of 367 people must have a pair of people that share a birthday.
  - 366 possible birthdays (pigeonholes)
  - 367 people (pigeons)
- Two people in San Francisco have the exact same number of hairs on their head.
  - Maximum number of hairs ever found on a human head is no greater than 500,000.
  - There are over 800,000 people in San Francisco.
- Each day, two people in New York City drink the same amount of water, to the thousandth of a fluid ounce.
  - No one can drink more than 50 gallons of water each day.
  - That's 6,400 fluid ounces. This gives 6,400,000 possible numbers of thousands of fluid ounces.
  - There are about 8,000,000 people in New York City proper.

Proof by Contradiction

“When you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth.”

- Sir Arthur Conan Doyle, *The Adventure of the Blanched Soldier*

Proof by Contradiction

- A **proof by contradiction** is a proof that works as follows:
  - To prove that P is true, assume that P is *not* true.
  - Based on the assumption that P is not true, conclude something impossible.
  - Assuming the logic is sound, the only valid explanation is that the original assumption must have been wrong.
  - Therefore, P can't be false, so it must be true.

Theorem: No integer is both even and odd.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$\begin{aligned} 2r - 2s &= 1 \\ r - s &= \tfrac{1}{2} \end{aligned}$$

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \tfrac{1}{2}$, which is not an integer.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \tfrac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \tfrac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd.

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \tfrac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

$$2r = 2s + 1.$$

Rearranging and simplifying this equation tells us the following:

$$2r - 2s = 1$$

$$r - s = \tfrac{1}{2}$$

Because r and s are integers, their difference must also be an integer. However, we've just seen that $r - s = \tfrac{1}{2}$, which is not an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Theorem: No integer is both even and odd.

Proof: By contradiction; suppose some integer is both even and odd. Let that integer be k.

Since k is even, there is some $r \in \mathbb{Z}$ such that $k = 2r$. The integer k is also odd, so there is some $s \in \mathbb{Z}$ where $k = 2s+1$. Combining these equalities together tells us that

The three key pieces:

1. State that the proof is by contradiction.
2. State what you are assuming is the negation of the statement to prove.
3. State you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

an integer.

We have reached a contradiction, so our assumption must have been wrong. Thus there is no integer that is both even and odd. ■

Rational and Irrational Numbers

Rational and Irrational Numbers

- A number r is called a ***rational number*** if it can be written as

$$r = \frac{p}{q}$$

  where p and q are integers and $q \neq 0$.
- A number that is not rational is called ***irrational***.
- Useful theorem: If r is rational, r can be written as p / q where $q \neq 0$ and where p and q have no common factors other than ± 1.

Theorem: $\sqrt{2}$ is irrational.

Theorem: $\sqrt{2}$ is irrational.
Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p \,/\, q = \sqrt{2}. \tag{1}$$

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

Theorem: √2 is irrational.

Proof: Assume for the sake of contradiction that √2is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

These floating numbers are labels on equations. We can use them to more easily refer to equations in the body of the proof.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p \,/\, q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p \,/\, q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p \,/\, q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$p^2 = 2q^2$$

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$p^2 = 2q^2$$
$$(2k)^2 = 2q^2$$

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} &p^2 = 2q^2 \\ &(2k)^2 = 2q^2 \\ &4k^2 = 2q^2 \end{aligned}$$

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \end{aligned} \tag{3}$$

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p \,/\, q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \qquad (2)$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

Theorem: $\sqrt{2}$ is irrational.
Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p \,/\, q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} &p^2 = 2q^2 \\ &(2k)^2 = 2q^2 \\ &4k^2 = 2q^2 \\ &2k^2 = q^2 \end{aligned} \tag{3}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong. Therefore, $\sqrt{2}$ is irrational.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume for the sake of contradiction that $\sqrt{2}$ is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \tag{1}$$

Multiplying both sides of equation (1) by q and squaring both sides shows us that

$$p^2 = 2q^2. \tag{2}$$

From equation (2), we see that p^2 is even. Earlier, we proved that if p^2 is even, then p must also be even. Therefore, we know that there is some integer k such that $p = 2k$. Substituting this into equation (2) and simplifying gives us the following:

$$\begin{aligned} p^2 &= 2q^2 \\ (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \qquad (3) \end{aligned}$$

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong. Therefore, $\sqrt{2}$ is irrational. ■

Theorem: √2 is irrational.

Proof: Assume for the sake of contradiction that √2 is rational. This means that there must be integers p and q where $q \neq 0$, where p and q have no common divisors other than 1 and -1, and where

$$p / q = \sqrt{2}. \qquad (1)$$

Multiplying both sides of equation (1) by q and squaring both sides

The three key pieces:

1. State that the proof is by contradiction.
2. State what you are assuming is the negation of the statement to prove.
3. State you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

Equation (3) shows that q^2 is even. Our earlier theorem tells us that, because q^2 is even, q must also be even. But this is not possible – we know that p and q have no common factors other than 1 and -1, but we've shown that p and q must have two as a common factor.

We have reached a contradiction, so our original assumption must have been wrong. Therefore, √2 is irrational. ■

Vi Hart on Pythagoras and
the Square Root of Two:

http://www.youtube.com/watch?v=X1E7I7_r3Cw

Proving Implications

- To prove the implication

"If *P* is true, then *Q* is true."

- you can use these three techniques:
  - **Direct Proof.**
    - Assume *P* and prove *Q*.
  - **Proof by Contrapositive**
    - Assume not *Q* and prove not *P*.
  - **Proof by Contradiction**
    - … what does this look like?

Negating Implications

- To prove the statement

  “If *P* is true, then *Q* is true”

  by contradiction, we do the following:
  - Assume this statement is false.
  - Derive a contradiction.
  - Conclude that the statement is true.
- What is the negation of this statement?

  “*P* is true and *Q* is false”

Contradictions and Implications

- To prove the statement

  “If *P* is true, then *Q* is true”

  using a proof by contradiction, do the following:
  - Assume that P is true and that Q is false.
  - Derive a contradiction.
  - Conclude that if P is true, Q must be as well.

Theorem: If n is an integer and n^2 is even, then n is even.

Theorem: If n is an integer and n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$n^2 = (2k + 1)^2$$

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: If n is an integer and n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned} \tag{2}$$

Theorem: If n is an integer and n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

Theorem: If n is an integer and n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect.

Theorem: If n is an integer and n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well.

Theorem: If n is an integer and n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1 \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Theorem: If n is an integer and n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that n is an integer and that n^2 is even, but that n is odd.

The three key pieces:

1. State that the proof is by contradiction.
2. State what the negation of the original statement is.
3. State you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Skills from Today

- Disproving statements
- Negating universal and existential statements.
- Negating implications.
- Determining the contrapositive of a statement.
- Writing a proof by contrapositive.
- Writing a proof by contradiction.

Next Time

- **Proof by Induction**
  - Proofs on sums, programs, algorithms, etc.

Appendices: Helpful References

Negating Implications

"If *P*, then *Q*"

becomes

"*P* but not *Q*"

Negating Universal Statements

"For all *x*, P(*x*) is true"

becomes

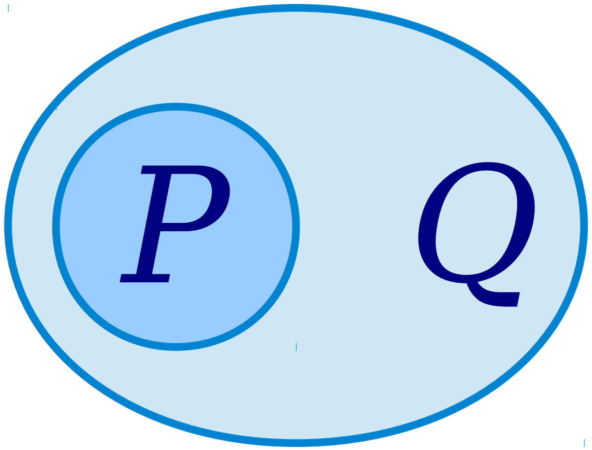
"There is an *x* where P(*x*) is false."

Negating Existential Statements

"There exists an *x* where P(*x*) is true"

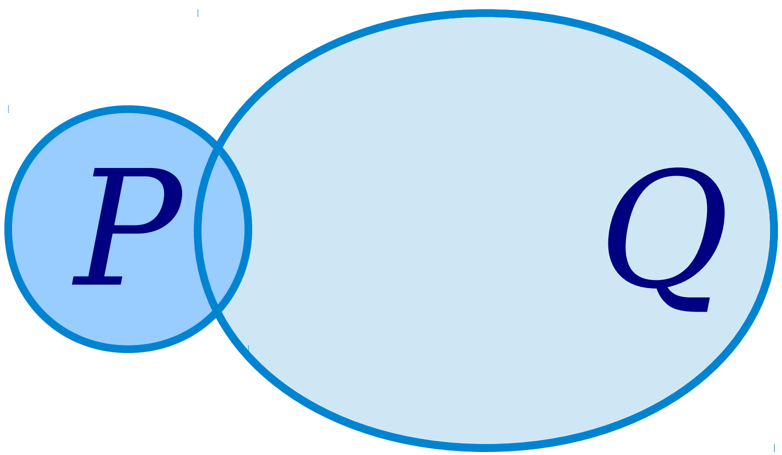
becomes

"For all *x*, P(*x*) is false."



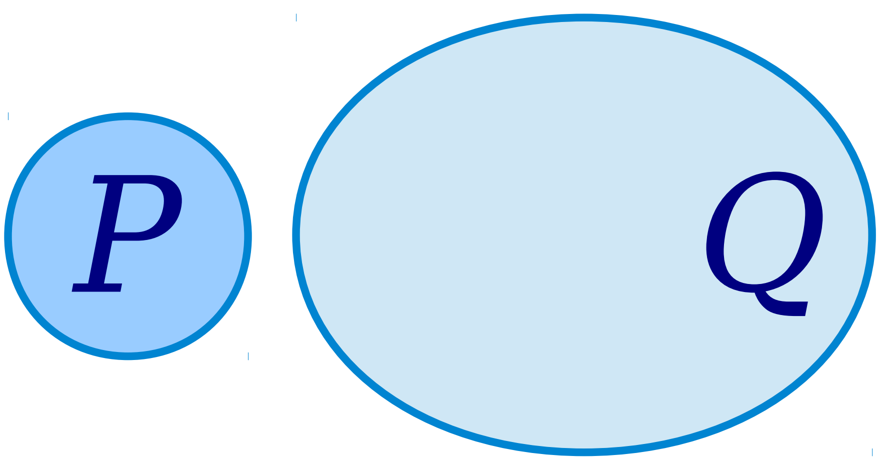
P implies Q

“If P is true, then Q is true.”



P does not imply Q
-and-
P does not imply not Q

“Sometimes P is true and Q is true,
-and-
sometimes P is true and Q is false.”



P implies not Q

If P is true, then Q is false