

Indirect Proofs

Outline for Today

- ***What is an Implication?***
 - Understanding a key type of mathematical statement.
- ***Negations and their Applications***
 - How do you show something is *not* true?
- ***Proof by Contrapositive***
 - What's a contrapositive?
 - And some applications!
- ***Proof by Contradiction***
 - The basic method.
 - And some applications!

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 like the way you look that much, (ohhh baby) then you should go and love yourself.

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 significantly deeper questions than they might seem.
- To mathematically study implications, we need to formalize what implications really mean.

Understanding Implications

**“If there's a rainbow,
then it's raining somewhere.”**

- In mathematics, implication is *directional*.
 - The above statement doesn't mean that if it's raining somewhere, there has to be a rainbow.
- In mathematics, implications only say something about the consequent when the antecedent is true.
 - If there's no rainbow, it doesn't mean there's no rain.
- In mathematics, implication says nothing about *causality*.
 - Rainbows do not cause rain. ☺

Scoping Implications

- Consider the following statements:
 - If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.**
 - If n is even, then n^2 is even.**
 - If $A \subseteq B$ and $B \subseteq A$, then $A = B$.**
- In the above statements, what are A , B , C , and n ? Are they *specific* objects? Or do these claims hold for all objects?

Implications and Universals

- In discrete math, most* implications involving unknown quantities are, implicitly, universal statements.
- For example, the statement

If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

actually means

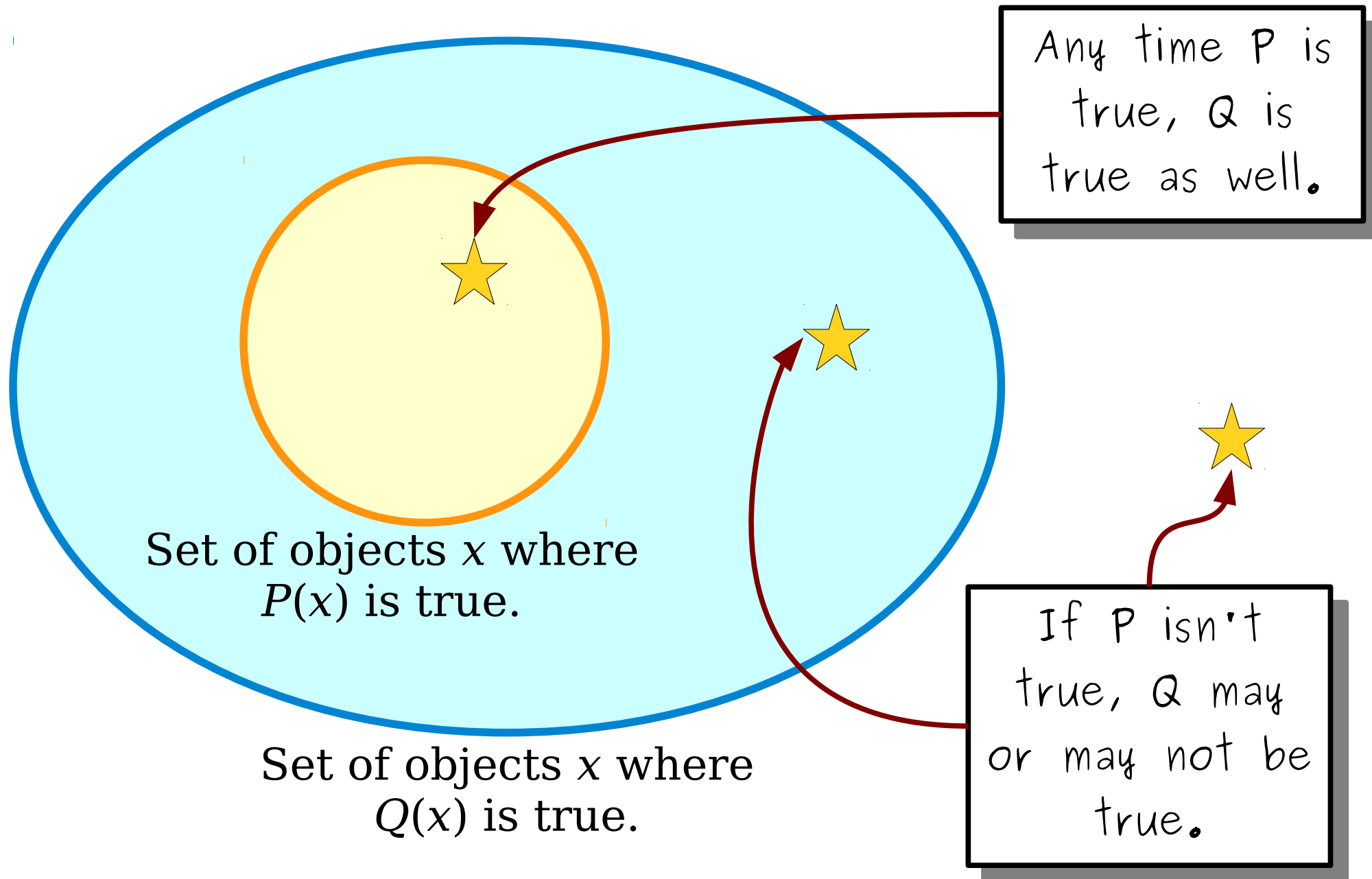
**For any sets A , B , and C ,
if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.**

** this will become clearer on Wednesday.*

What Implications Mean

- In mathematics, a statement of the form **For any x , if $P(x)$ is true, then $Q(x)$ is true** means that any time you find an object x where $P(x)$ is true, you will find that $Q(x)$ is also true.
- There is no discussion of correlation or causation here. It simply means that if you find that $P(x)$ is true, you'll find that $Q(x)$ is true.

Implication, Diagrammatically



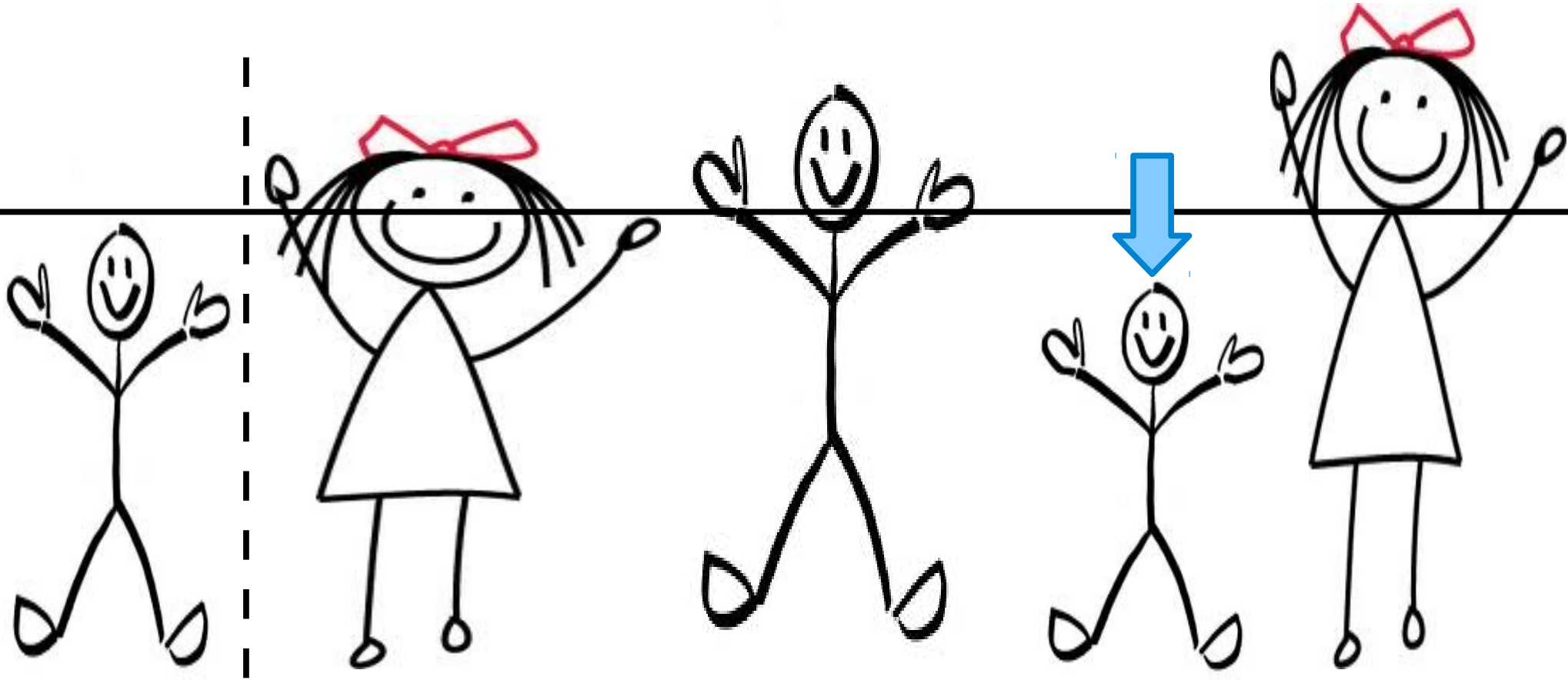
Negations

Negations

- A **proposition** is a statement that is either true or false.
- Some examples:
 - If n is an even integer, then n^2 is an even integer.
 - $\emptyset = \mathbb{R}$.
 - I want to swing from the chandelier.
- The **negation** of a proposition X is a proposition that is true whenever X is false and is false whenever X is true.
- For example, consider the statement “it is snowing outside.”
 - Its negation is “it is not snowing outside.”
 - Its negation is *not* “it is sunny outside.”
 - Its negation is *not* “we’re in the Bay Area.”

How do you find the negation
of a statement?

“All My Friends Are Taller Than Me”



Me

My Friends

The negation of the *universal* statement

Every P is a Q

is the *existential* statement

There is a P that is not a Q .

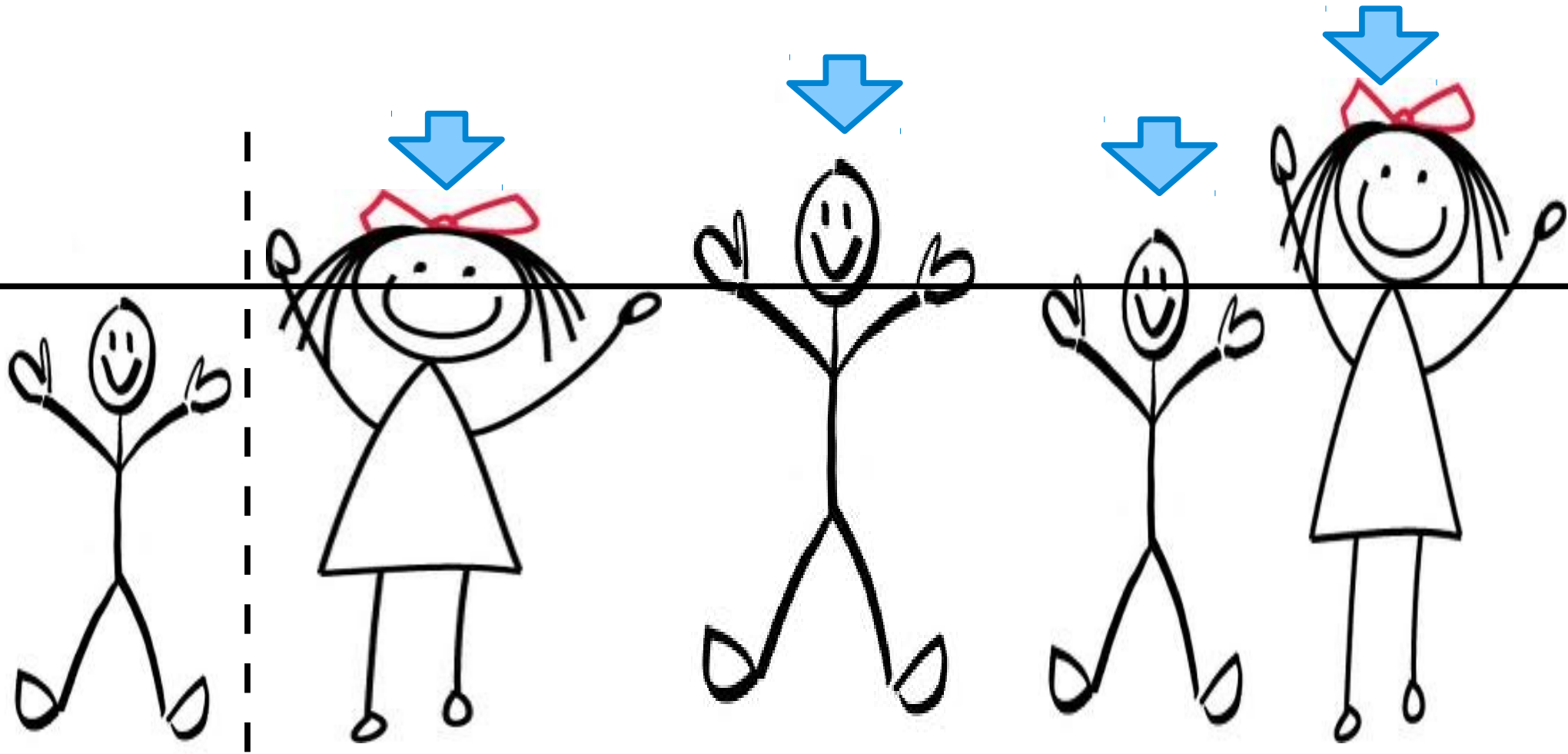
The negation of the *universal* statement

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”



Me

My Friends

The negation of the *existential* statement

There exists a P that is a Q

is the *universal* statement

Every P is not a Q .

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.

How do you negate an implication?

Puppy Logic

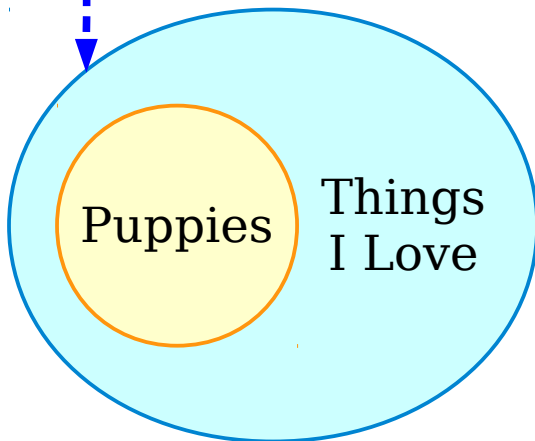
- Consider the statement

If x is a puppy, then I love x .

Puppy Logic

- Consider the statement

If x is a puppy, then I love x .



“I love all puppies.”

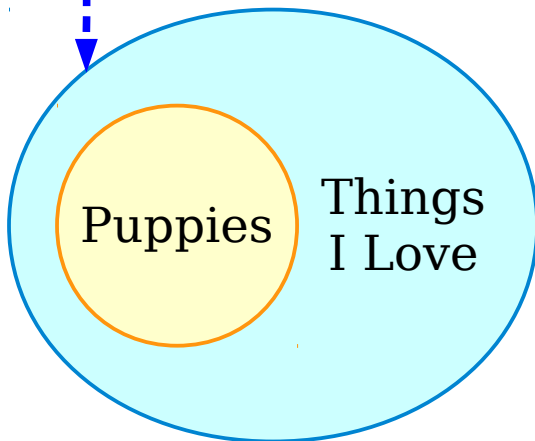
Puppy Logic

- Consider the statement

If x is a puppy, then I love x .

- The following statement is ***not*** the negation of the original statement:

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



"I love all puppies."

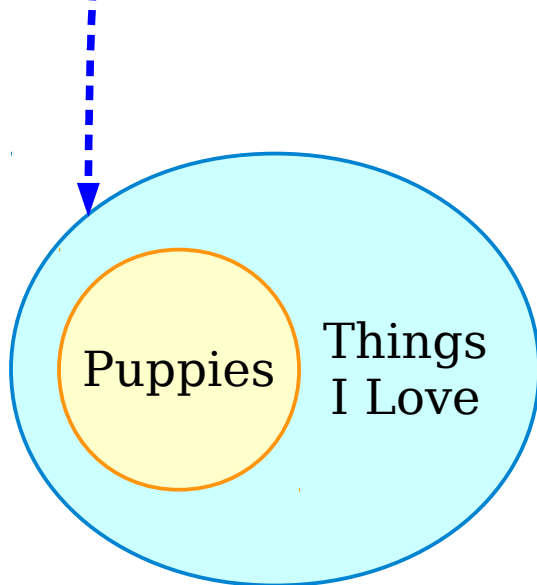
Puppy Logic

- Consider the statement

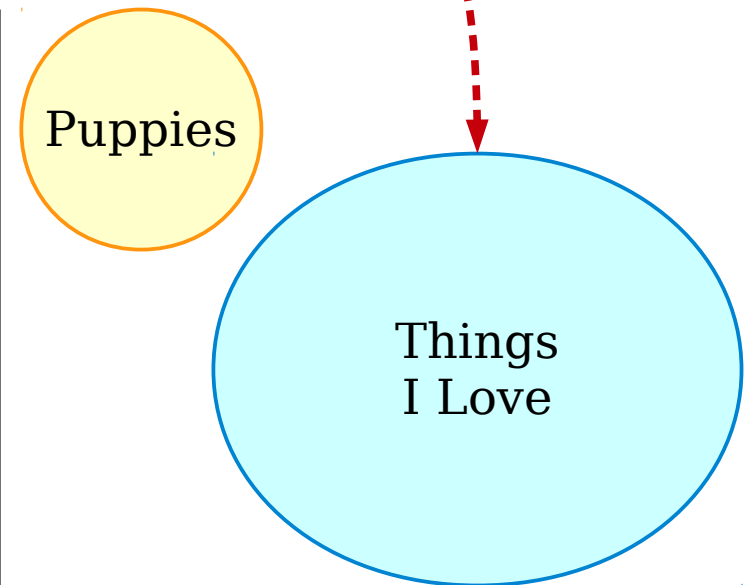
If x is a puppy, then I love x .

- The following statement is **not** the negation of the original statement:

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



"I love all puppies."



"I don't love any puppies."

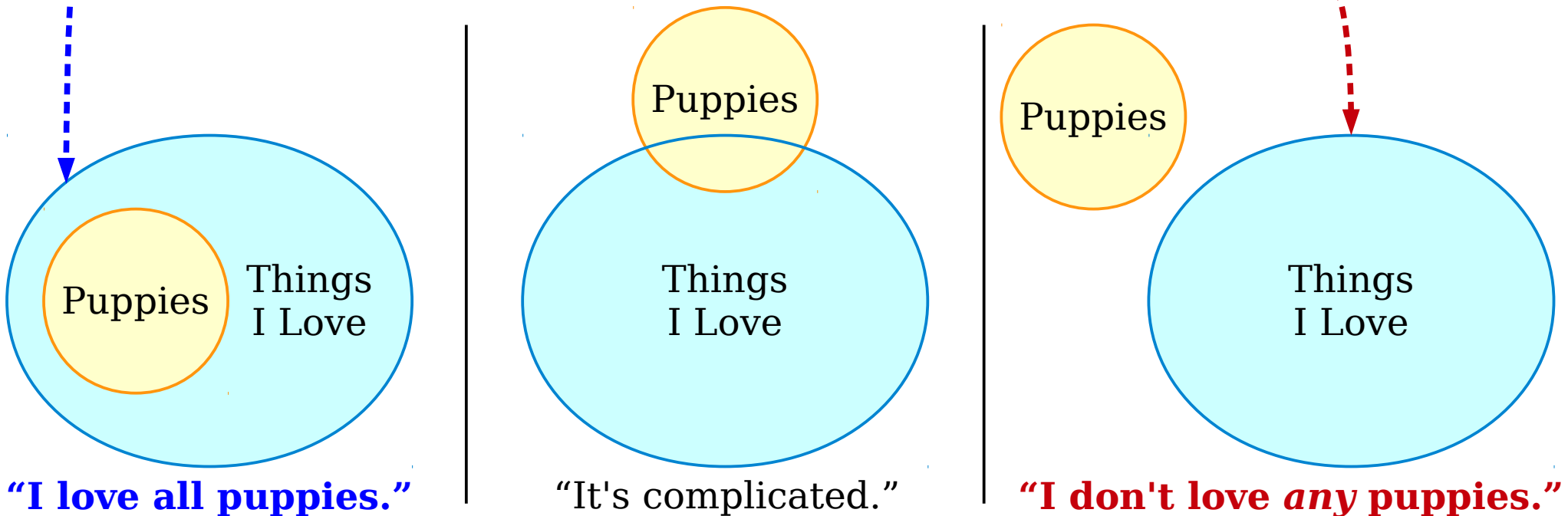
Puppy Logic

- Consider the statement

If x is a puppy, then I love x .

- The following statement is **not** the negation of the original statement:

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



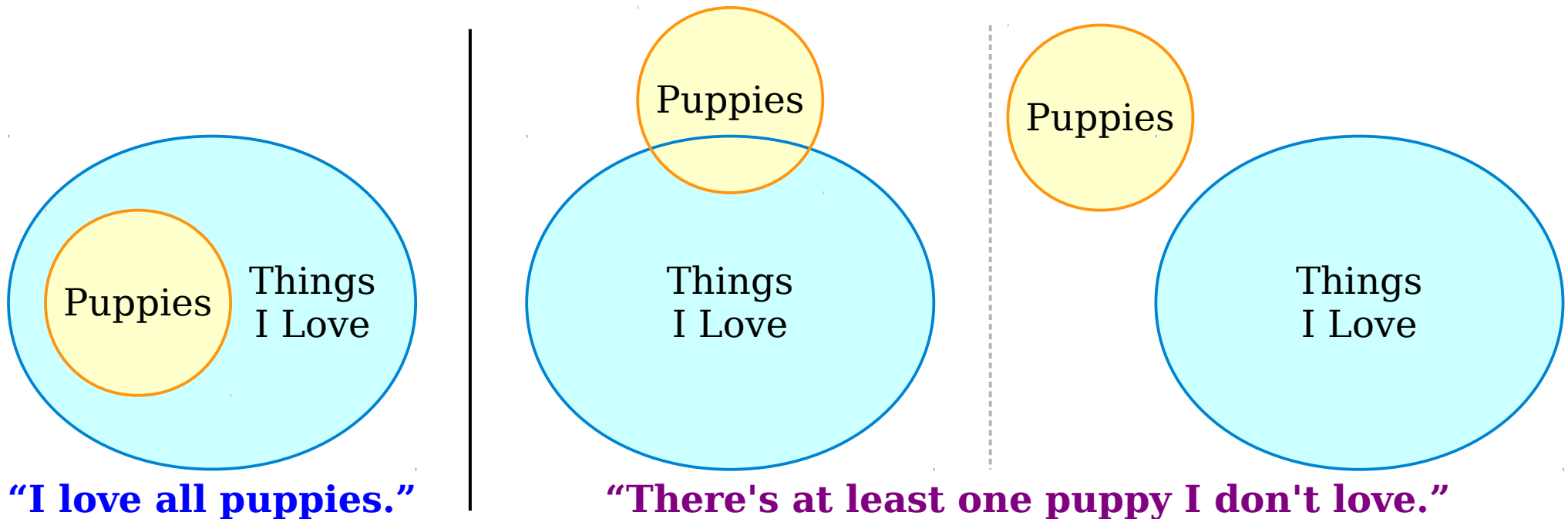
Puppy Logic

- Consider the statement

If x is a puppy, then I love x .

- Here's the proper negation of our initial statement about puppies:

There's at least one puppy I don't love.



The negation of the statement

**“For any x , if $P(x)$ is true,
then $Q(x)$ is true”**

is the statement

**“There is at least one x where
 $P(x)$ is true and $Q(x)$ is false.”**

***The negation of an implication
is not an implication!***

Proof by Contrapositive

The Contrapositive

- The ***contrapositive*** of the implication “If P , then Q ” is the implication “If Q is false, then P is false.”
- For 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.”
- Another example:
 - “If I store the cat food inside, then wild raccoons will not steal my cat food.”
 - Contrapositive: “If wild raccoons stole my cat food, then I didn't store it inside.”

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 $n = 2k + 1$ and so

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.

From
(nam
There

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.

Proving Biconditionals

- To prove **P iff Q** , you need to prove that P implies Q and that Q implies P .
- You can use 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.
- Just make sure to cover both directions.

Time-Out for Announcements!

health++ Hackathon

- **health++** is holding a hackathon on October 21st and 22nd to address challenges in healthcare and healthcare accessibility.
- Interested? Apply using **this link** or contact the team over **email**.

Code the Change

- Code the Change, a yearlong program focused on social good, is looking for applicants for this year.
 - [Click here](#) for some of their past projects.
- Interested in joining? Here's a [when2meet](#) to coordinate times.
- Interested in being a team lead? There's a meeting today at 5PM in OU 120.

Black in CS Interview Workshop



- Black in CS is hosting an interview workshop run by Dropbox.
- Runs on October 4th at 6PM at Black House.
- Interested? RSVP using [**this link**](#).



WiCS

Frosh Intern Program



{ Curious about CS? Looking for a community on campus? Excited about the WiCS mission? }



Apply for the WiCS Frosh Intern Program at bit.ly/wics-frosh-intern



{ Frosh interns rotate through different WiCS teams, work on meaningful projects, and join a community of lifelong friends and mentors }



Applications are due Friday, Oct. 6 at 11:59 PM



Stanford Women in Computer Science {w}



Handouts

- There are *six* (!) total handouts for today:
 - Handout 08: Guide to Proofs
 - Handout 09: Mathematical Vocabulary
 - Handout 10: Guide to Indirect Proofs
 - Handout 11: Ten Techniques to Get Unstuck
 - Handout 12: Proofwriting Checklist
 - Handout 13: Problem Set One
- Be sure to read over Handouts 08 – 12; there's a lot of really important information in there!

Handouts

There are *six* (!) total handouts for today:

Handout 08: Guide to Proofs

Handout 09: Mathematical Vocabulary

Handout 10: Guide to Indirect Proofs

Handout 11: Ten Techniques to Get Unstuck

Handout 12: Proofwriting Checklist

- **Handout 13: Problem Set One**

Be sure to read over Handouts 08 - 12; there's a lot of really important information in there!

Announcements

- Problem Set 1 goes out today!
- **Checkpoint** due Monday, October 2 at 2:30PM.
 - 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 effort you put in, the more you'll get out.
- **Remaining problems** due Friday, October 6 at 2:30PM.
 - Feel free to email us with questions, stop by office hours, or ask questions on Piazza!

Submitting Assignments

- All assignments should be submitted through GradeScope.
 - The programming portion of the assignment gets submitted separately from the written component.
 - The written component **must** be typed up; handwritten solutions don't scan well and get mangled in GradeScope.
- Summary of the late policy:
 - Everyone has *three* 24-hour late days.
 - Late days can't be used on checkpoints.
 - Nothing may be submitted more than three days past the due date.
- Because submission times are recorded automatically, we're strict about the submission deadlines.
- **Very good idea:** Leave at least two hours buffer time for your first assignment submission, just in case something goes wrong.
- **Very bad idea:** Wait until the last minute to submit.

Working in Pairs

- You can work on the problem sets individually or in pairs.
- Each person/pair 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 Handout 04 and Handout 05.

A Note on the Honor Code

Office hours have started!

Schedule is available
on the course website.

Back to CS103!

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.
 - Beginning with this assumption, use logical reasoning to conclude something that is clearly impossible.
 - For example, that $1 = 0$, that $x \in S$ and $x \notin S$, etc.
 - This means that if P is false, something that cannot possibly happen must happen.
 - Therefore, P can't be false, so it must be true.

An Example: ***Set Cardinalities***

Set Cardinalities

- We've seen sets of many different cardinalities:
 - $|\emptyset| = 0$
 - $|\{1, 2, 3\}| = 3$
 - $|\{n \in \mathbb{N} \mid n < 137\}| = 137$
 - $|\mathbb{N}| = \aleph_0$.
- These span from the finite up through the infinite.
- **Question:** Is there a “largest” set? That is, is there a set that's bigger than every other set?

Theorem: There is no largest set.

Theorem: There is no largest set.

Proof:

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction,
we're going to assume its negation.

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction,
we're going to assume its negation.

What is the negation of the statement
"there is no largest set?"

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction,
we're going to assume its negation.

What is the negation of the statement
"there is no largest set?"

One option: "there is a largest set."

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

One option: "there is a largest set."

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Notice that we're announcing

1. that this is a proof by contradiction, and
2. what, specifically, we're assuming.

This helps the reader understand where we're going. Remember - proofs are meant to be read by other people!

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S .

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S . This contradicts the fact that S is the largest set.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S . This contradicts the fact that S is the largest set.

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

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S . This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S . This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S . This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S .

The three key pieces:

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

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

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

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

“For any x , if $P(x)$ is true, then $Q(x)$ is true”

by contradiction, we do the following:

- Assume this entire purple statement is false.
 - Derive a contradiction.
 - Conclude that the statement is true.
- What is the negation of the above purple statement?

**“There is an x where
 $P(x)$ is true and $Q(x)$ 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

$$n = 2k + 1. \quad (1)$$

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

$$n = 2k + 1. \quad (1)$$

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

$$n = 2k + 1. \quad (1)$$

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

$$n = 2k + 1. \quad (1)$$

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

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

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

$$n = 2k + 1. \quad (1)$$

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

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

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

$$n = 2k + 1. \quad (1)$$

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

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

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

$$n = 2k + 1. \quad (1)$$

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

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

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

$$n = 2k + 1. \quad (1)$$

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

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

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

The three key pieces:

1. Say that the proof is by contradiction.
2. Say what the negation of the original statement is.
3. Say 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. ■

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

$$n = 2k + 1. \quad (1)$$

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

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

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

$$n = 2k + 1. \quad (1)$$

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

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

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
Proof: Assume
integer and
Since n is
that

We're numbering our intermediate stages to make it easier to refer to them later. If you have a calculation-heavy proof, we recommend structuring it like this.

then n is even.
that n is an
odd.
integer k such

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

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. ■

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**.

Simplest Forms

- *By definition*, if r is a rational number, then r can be written as p / q where p and q are integers and $q \neq 0$.
- ***Theorem:*** If r is a rational number, then r can be written as p / q where p and q are integers, $q \neq 0$, and p and q have no common factors other than 1 and -1.
 - That is, r can be written as a fraction in simplest form.
- We're just going to take this for granted for now, though with the techniques you'll see later in the quarter you'll be able to prove it!

Question: Are all real numbers rational?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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:

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

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

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

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

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

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

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

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

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

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:

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

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

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

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

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

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:

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

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

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

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

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

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

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:

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

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.

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

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

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

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

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:

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

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

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

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

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

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:

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

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. 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

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

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

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

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:

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

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. 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

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

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, $\sqrt{2}$ 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

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

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

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

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:

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

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. Therefore, $\sqrt{2}$ is irrational. ■

Vi Hart on Pythagoras and
the Square Root of Two:

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

What We Learned

- ***What's an implication?***

- It's statement of the form “if P , then Q ,” and states that if P is true, then Q is true.

- ***How do you negate formulas?***

- It depends on the formula. There are nice rules for how to negate universal and existential statements and implications.

- ***What is a proof by contrapositive?***

- It's a proof of an implication that instead proves its contrapositive.
- (The contrapositive of “if P , then Q ” is “if not Q , then not P .”)

- ***What's a proof by contradiction?***

- It's a proof of a statement P that works by showing that P cannot be false.

Next Time

- ***Mathematical Logic***
 - How do we formalize the reasoning from our proofs?
- ***Propositional Logic***
 - Reasoning about simple statements.
- ***Propositional Equivalences***
 - Simplifying complex statements.

Appendix: Negating Statements

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

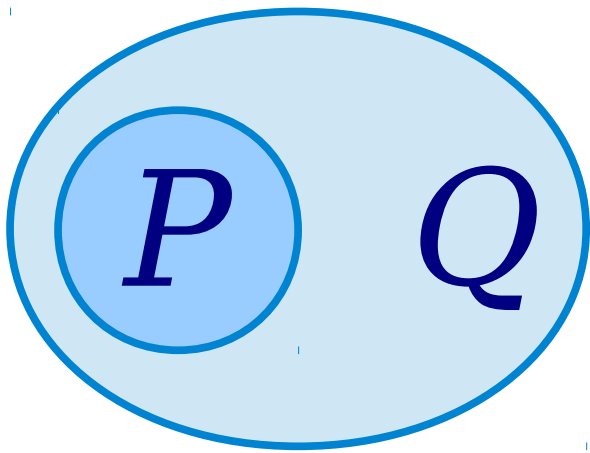
“For all x , $P(x)$ is false.”

Negating Implications

“For every x , if $P(x)$ is true, then $Q(x)$ is true”

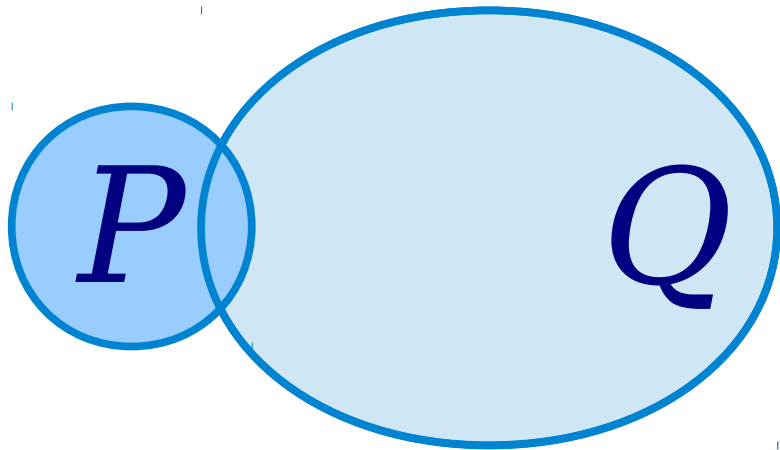
becomes

“There is an x where $P(x)$ is true and $Q(x)$ is false”



$P(x)$ implies $Q(x)$

“If $P(x)$ is true, then $Q(x)$ is true.”



$P(x)$ does not imply $Q(x)$

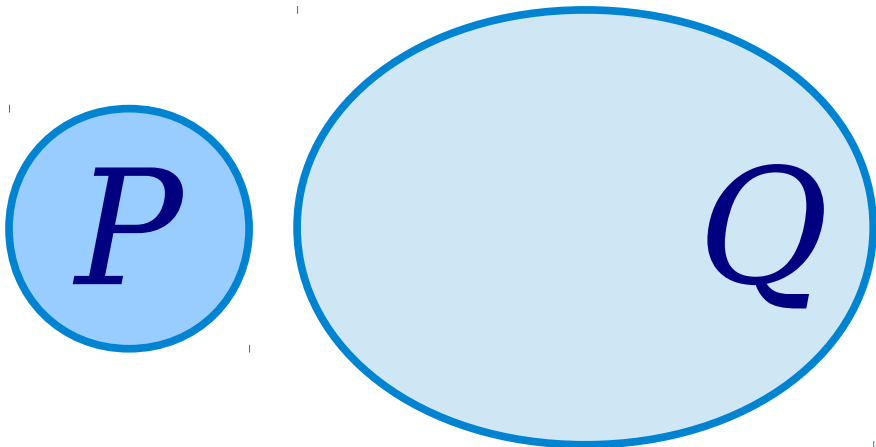
-and-

$P(x)$ does not imply not $Q(x)$

“Sometimes $P(x)$ is true and $Q(x)$ is true,

-and-

sometimes $P(x)$ is true and $Q(x)$ is false.”

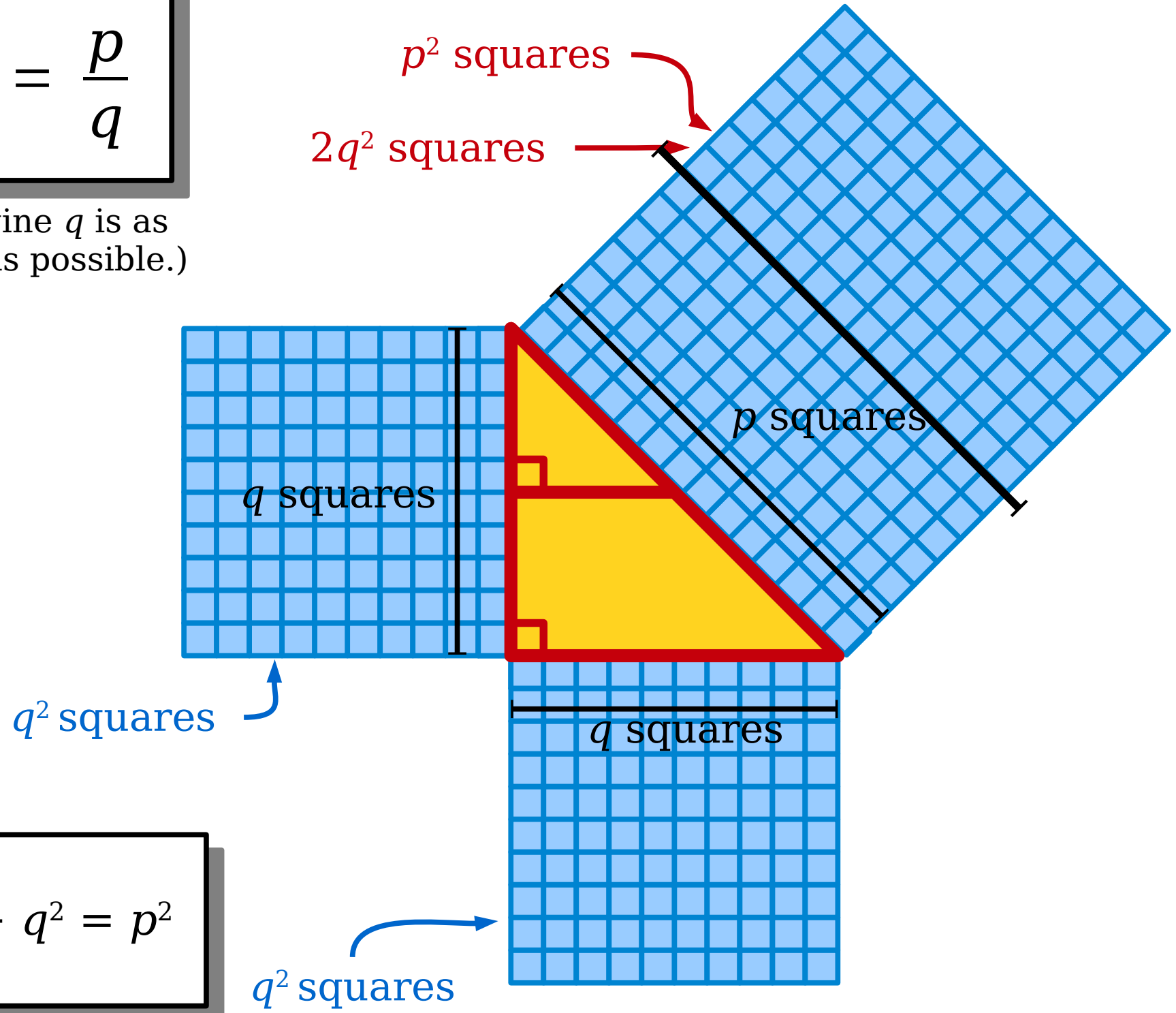


$P(x)$ implies not $Q(x)$

If $P(x)$ is true, then $Q(x)$ is false

$$\sqrt{2} = \frac{p}{q}$$

(Imagine q is as small as possible.)



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