Indirect Proofs

Outline for Today

- **What is an Implication?**
  - Understanding a key type of mathematical statement.
- **Proof by Contrapositive**
  - What's a contrapositive?
  - Applications to bird storage.
- **Proof by Contradiction**
  - The basic method.
  - Applications to geometry.

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 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.”**

- Implication is *directional*.
  - The above statement doesn't mean that if it's raining somewhere, there has to be a rainbow.
- Implication only cares about cases where the antecedent is true.
  - If there's no rainbow, it doesn't mean that there's no rain.
- 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.*

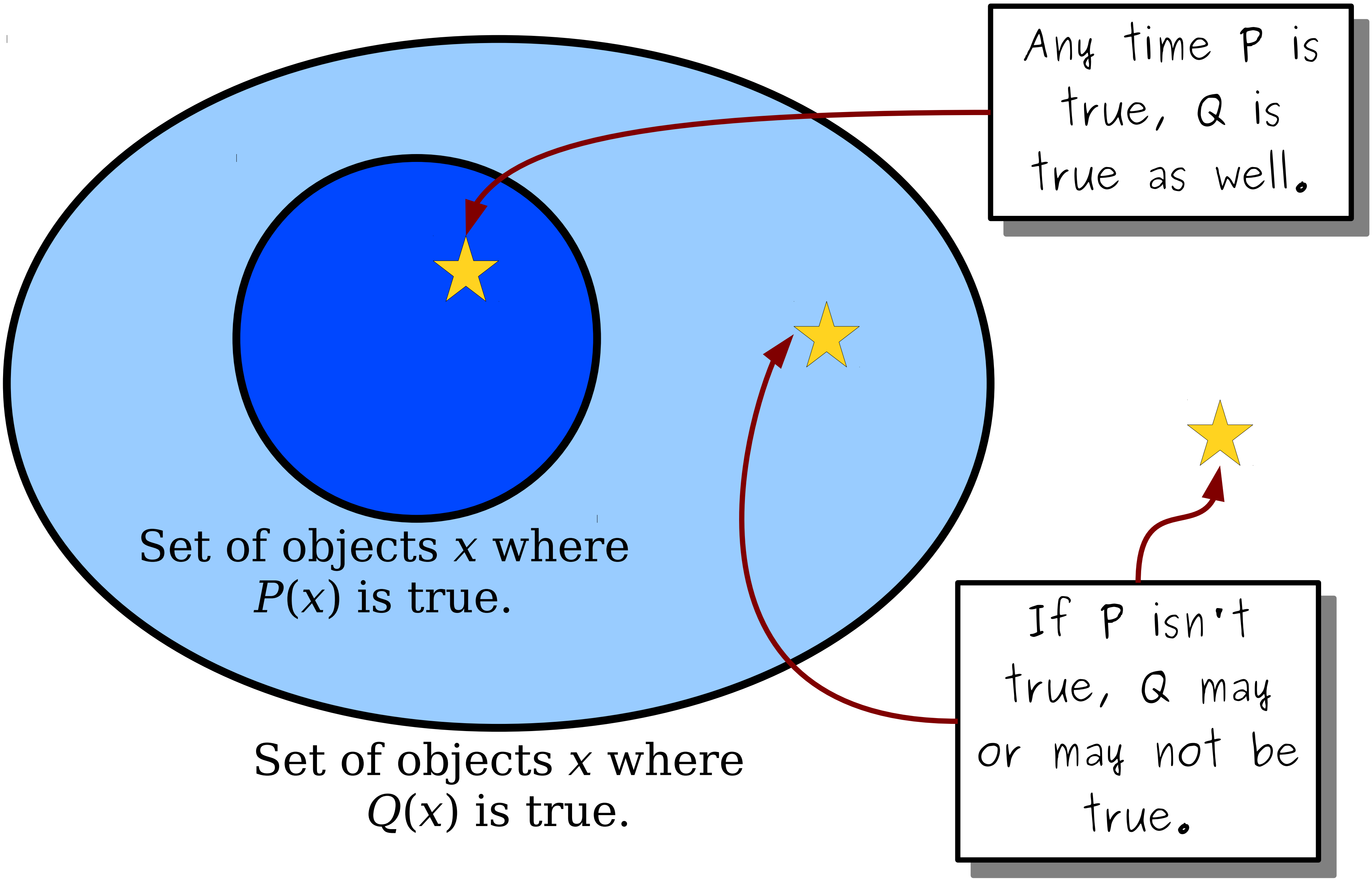
What Implications Mean

- 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

- The ***negation*** of a statement X is a statement meaning the opposite of X.
- Examples:
  - The negation of "1 + 1 = 2" is "1 + 1 ≠ 2."
  - The negation of "everything is awesome" is "something is not awesome."
  - The negation of "there's something happenin' round here" is "nothing is happenin' round here."
- Let's talk about the interplay between negations and implications.

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.
  - The initial statement means “I love all puppies.”
  - The second statement says “I don't love *any* puppies.”
- Here's the correct negation:

There is some puppy that 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 ***not*** *Q*, then ***not*** *P*."
- 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.

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; 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.

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 $n = 2k + 1$. 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.**

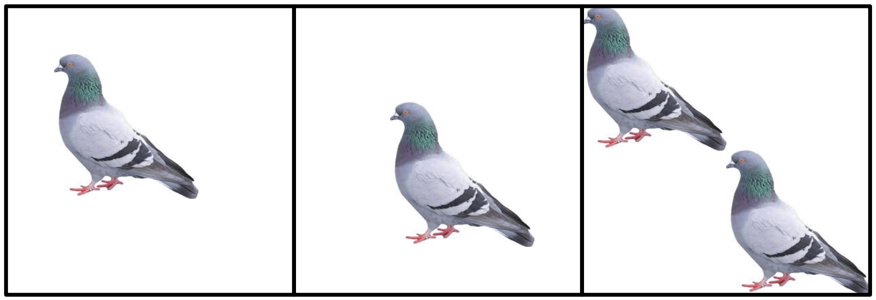
Proving Biconditionals

- 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.

Application: ***The Pigeonhole Principle***

The Pigeonhole Principle

- Suppose that you have *n* pigeonholes.
- Suppose that you have *m* > *n* pigeons.
- If you put the *m* pigeons into the *n* pigeonholes, some pigeonhole must 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?

If every bin contains at most one object,
then *m* ≤ *n*.

There is a bin that doesn't have 0 or 1 objects in it

Every bin has at most one object 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?

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 inequality, 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 6,400,001 possible numbers of thousands of fluid ounces.
  - There are about 8,000,000 people in New York City proper.

Time-Out for Announcements!

Handouts

- There are six total handouts for today, three of which are available outside in hard copy:
  - Handout 05: Problem Set Policies
  - Handout 06: Honor Code Policies
  - Handout 07: Guide to Proofs
  - Handout 08: Mathematical Vocabulary
  - Handout 09: Guide to Indirect Proofs
  - Handout 10: Problem Set One
- Be sure to read over Handouts 05 – 09; there's a lot of really important information in there!

Announcements

- Problem Set 1 goes out today!
- ***Checkpoint*** due Monday, January 11.
  - 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, January 15.
  - Feel free to email us with questions, stop by office hours, or ask questions on Piazza!

Submitting Assignments

- This quarter, we will be using GradeScope to handle assignment submissions. Visit www.gradescope.com and enter code **`942VB9`**.
- 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 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 05 and 06.

A Note on the Honor Code

Office hours start tonight!

Schedule is available
on the course website.

Back to CS103!

Proof by Contradiction

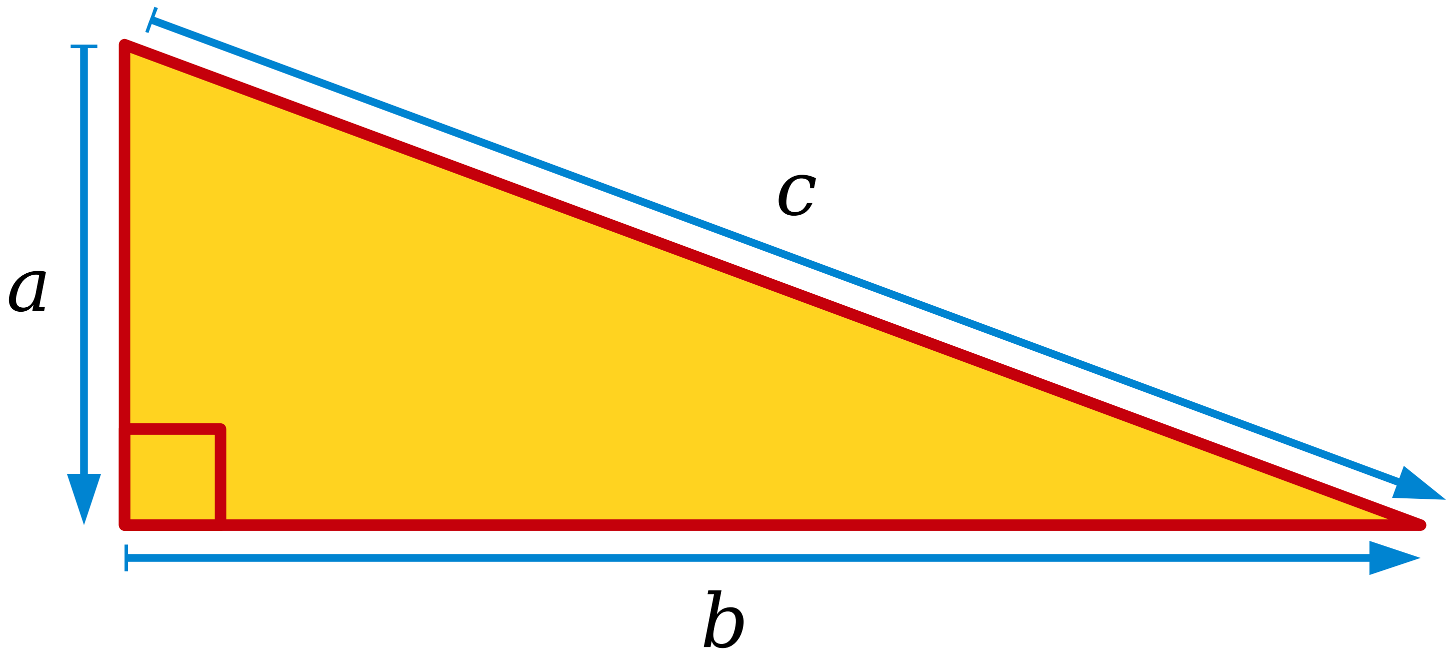
“When you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth.”

- 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.
  - Starting 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 impossible happens.
  - Therefore, P can't be false, so it must be true.

Right Triangles



$$a^2 + b^2 = c^2$$

Claim: $a + b \geq c$

Theorem: For all natural numbers a, b, and c where $a^2+b^2 = c^2$, we have $a + b \geq c$.

To prove this by contradiction, we're going to assume the negation of the above statement.

What is its negation?

"For all natural numbers a, b, and c where $a^2 + b^2 = c^2$, we have $a + b \geq c$"

"There exist natural numbers a, b and c where $a^2 + b^2 = c^2$, but $a + b < c$"

Theorem: For all natural numbers a, b, and c where $a^2+b^2 = c^2$, we have $a + b \geq c$.

Proof: Assume for the sake of contradiction that there are natural numbers a, b, and c where $a^2+b^2 = c^2$, but $a + b < c$.

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: For all natural numbers a, b, and c where $a^2+b^2 = c^2$, we have $a + b \geq c$.

Proof: Assume for the sake of contradiction that there are natural numbers a, b, and c where $a^2+b^2 = c^2$, but $a + b < c$.

Since both sides of the preceding inequality are nonnegative, we can square both sides to see that

$$(a + b)^2 < c^2. \tag{1}$$

We can simplify the left-hand side of inequality (1) to see that

$$a^2 + 2ab + b^2 < c^2. \tag{2}$$

> 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.

Theorem: For all natural numbers a, b, and c where $a^2+b^2 = c^2$, we have $a + b \geq c$.

Proof: Assume for the sake of contradiction that there are natural numbers a, b, and c where $a^2+b^2 = c^2$, but $a + b < c$.

Since both sides of the preceding inequality are nonnegative, we can square both sides to see that

$$(a + b)^2 < c^2. \tag{1}$$

We can simplify the left-hand side of inequality (1) to see that

$$a^2 + 2ab + b^2 < c^2. \tag{2}$$

Since $a^2 + b^2 = c^2$, we can rewrite the left-hand side of inequality (2) as

$$c^2 + 2ab < c^2, \tag{3}$$

and subtracting c^2 from both sides of inequality (3) yields

$$2ab < 0. \tag{4}$$

But this is impossible: we know that $2ab \geq 0$, since $2ab$ is a natural number and all natural numbers are nonnegative.

We have reached a contradiction, so our assumption must have been wrong. Therefore, $a + b \geq c$, as required. ■

Theorem: For all natural numbers a, b, and c where $a^2+b^2 = c^2$, we have $a + b \geq c$.

Proof: Assume for the sake of contradiction that there are natural numbers a, b, and c where $a^2+b^2 = c^2$, but $a + b < c$.

Since both sides of the preceding inequality are nonnegative, we can square both sides to see 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!

$$2ab < 0. \quad (4)$$

But this is impossible: we know that $2ab \geq 0$, since $2ab$ is a natural number and all natural numbers are nonnegative.

We have reached a contradiction, so our assumption must have been wrong. Therefore, $a + b \geq c$, as required. ■

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*), then *Q*(*x*)"

  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?

  "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.

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:

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

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. 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!

$$2(2k^2 + 2k) + 1 \quad (2)$$

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. ■

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* ≠ 0.
- ***Theorem:*** If *r* is a rational number, then *r* can be written as *p* / *q* where *p* and *q* are integers, *q* ≠ 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.

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.

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.
- ***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

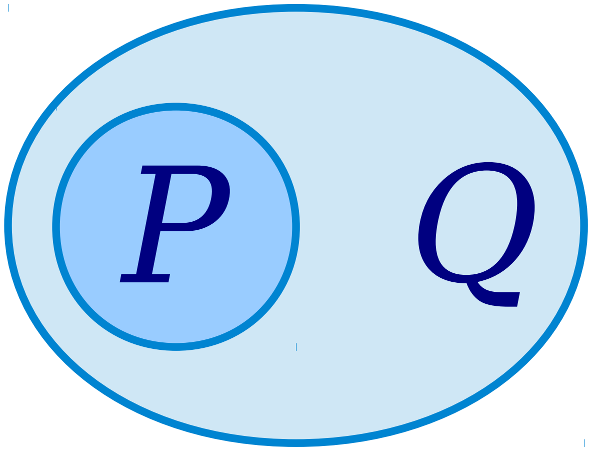
"For all *x*, P(*x*) is false."

Negating Implications

"For every *x*, if *P*(*x*) is true, then *Q*(*x*) is true"

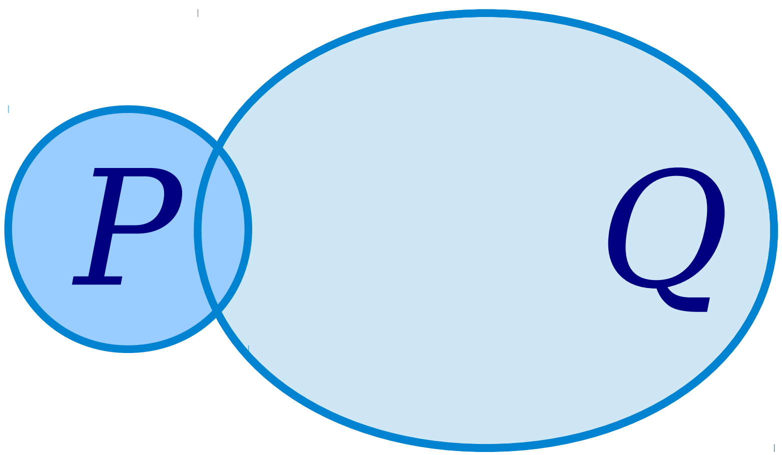
becomes

"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."

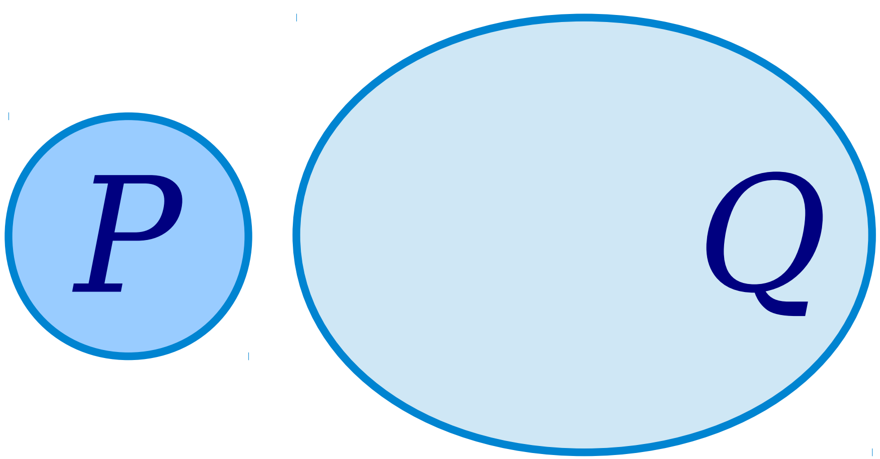


$P(x)$ does not imply $Q(x)$

-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