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
If $n$ is an even integer, then $n^2$ is an even integer.

This part of the implication is called the **antecedent**.

This part of the implication is called the **consequent**.

An **implication** is a statement of the form “If $P$ is true, then $Q$ is true.”
If $n$ is an even integer, then $n^2$ is an even integer.

If $m$ and $n$ are odd integers, then $m+n$ is even.

If you like the way you look that much, then you should go and love yourself.

An implication is a statement of the form "If $P$ is true, then $Q$ is true."
What Implications Mean

• Consider this implication:

   *If I put fire near cotton, then 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 in the sky, 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. 😊
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 see that $Q(x)$ is also true (for that same $x$).

- There is no discussion of causation here. It simply means that if you find that $P(x)$ is true, you'll find that $Q(x)$ is also true.
Implication, Diagrammatically

Set of objects $x$ where $P(x)$ is true.

Set of objects $x$ where $Q(x)$ is true.

Any time $P$ is true, $Q$ is true as well.

If $P$ isn't true, $Q$ may or may not be true.
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.
  • \( \emptyset = \mathbb{R} \).
  • The new me is still the real me.
• 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”
The negation of the *universal* statement \(\text{Every } P \text{ is a } Q\) is the *existential* statement \(\text{There is a } P \text{ that is not a } Q\).
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”
The negation of the \textit{existential} statement \[\text{There exists a } P \text{ that is a } Q\] is the \textit{universal} statement \[\text{Every } P \text{ is not a } Q.\]
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?
**Ancient Babylonian Contract:**

If Nanni pays money to Ea-Nasir, then Ea-Nasir will give Nanni quality copper ingots.

**Question:** What has to happen for this contract to be broken?

**Answer:** Nanni pays Ea-Nasir and doesn’t get quality copper ingots.
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!*
If $p$ is a puppy, then I **do** love $p$!

It's complicated.

If $p$ is a puppy, then I **don't** love $p$!
**How to Negate Universal Statements:**

“For all x, $P(x)$ is true”

becomes

“There is an x where $P(x)$ is false.”

---

**How to Negate Existential Statements:**

“There exists an x where $P(x)$ is true”

becomes

“For all x, $P(x)$ is false.”

---

**How to Negate 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”
Proof by Contraposition
If $P$ is true, then $Q$ is true.

$P$ is true and $Q$ is false.

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

What are the negations of the above two statements?
The Contrapositive

• The contrapositive of the implication
  If $P$ is true, then $Q$ is true
  is the implication
  If $Q$ is false, then $P$ is false.

• The contrapositive of an implication means exactly the same thing as the implication itself.

  *If it’s a puppy, then I love it.*

  *If I don’t love it, then it’s not a puppy.*
The Contrapositive

- The *contrapositive* of the implication
  
  *If $P$ is true, then $Q$ is true*
  
  is the implication
  
  *If $Q$ is false, then $P$ is false."

- The contrapositive of an implication means exactly the same thing as the implication itself.

*If I store cat food inside, then raccoons won’t steal it.*

*If raccoons stole the cat food, then I didn’t store it inside.*
To prove the statement

“if $P$ is true, then $Q$ is true,”

you can choose to instead prove the equivalent statement

“if $Q$ is false, then $P$ is false,”

if that seems easier.

This is called a proof by contrapositive.
**Theorem:** For any $n \in \mathbb{Z}$, if $n^2$ is even, then $n$ is even.

**Proof:** We will prove the contrapositive of this statement.

This is a courtesy to the reader and says "heads up! we're not going to do a regular old-fashioned direct proof here."
**Theorem:** For any $n \in \mathbb{Z}$, if $n^2$ is even, then $n$ is even.

**Proof:** We will prove the contrapositive of this statement, that if $n$ is odd, then $n^2$ is odd.

What is the contrapositive of the statement

if $n^2$ is even, then $n$ is even?

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: We will prove the contrapositive of this statement, 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:** We will prove the contrapositive of this statement, 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:** We will prove the contrapositive of this statement, that if $n$ is odd, then $n^2$ is odd.

Let $n$ be an arbitrary odd integer. 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:

$$
n^2 = (2k + 1)^2
= 4k^2 + 4k + 1
= 2(2k^2 + 2k) + 1.
$$

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:** We will prove the contrapositive of this statement, that if $n$ is odd, then $n^2$ is odd.

Let $n$ be an arbitrary odd integer. 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:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

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. ■

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

• The previous theorem, combined with what we saw on Wednesday, tells us the following:

For any integer \( n \), if \( n \) is even, then \( n^2 \) is even.
For any integer \( n \), if \( n^2 \) is even, then \( n \) is even.

• These are two different implications, each going the other way.

• We use the phrase *if and only if* to indicate that two statements imply one another.

• For example, we might combine the two above statements to say

for any integer \( n \): \( n \) is even if and only if \( n^2 \) is even.
Proving Biconditionals

• To prove a theorem of the form \( P \) if and only if \( Q \), you need to prove two separate statements.
  • First, that if \( P \) is true, then \( Q \) is true.
  • Second, that if \( Q \) is true, then \( P \) is true.
• You can use any proof techniques you'd like to show each of these statements.
  • In our case, we used a direct proof for one and a proof by contrapositive for the other.
Time-Out for Announcements!
STANFORD COMPUTER SCIENCE PRESENTS

ASK ME ANYTHING

WITH PROFESSOR MONICA LAM SPEAKING ON PRIVACY AND VIRTUAL ASSISTANTS

OCTOBER 2ND
6:00PM - 7:00PM
GATES 104

JOIN US FOR DINNER AND THE OPPORTUNITY TO HANG OUT AND CHAT ONE-ON-ONE WITH CS PROFESSOR MONICA LAM

Space is limited; RSVP using this link.
Handouts

• There are *four* (!) total handouts for today:
  • Handout 08: Guide to Indirect Proofs
  • Handout 09: Ten Techniques to Get Unstuck
  • Handout 10: Proofwriting Checklist
  • Handout 11: Problem Set One

• Be sure to read over Handouts 08 – 10; there's a lot of really important information in there!
Announcements

- Problem Set 1 goes out today!
- **Checkpoint** due Monday, September 30 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 4 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 two 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. In other words, if you’re working in a pair, you and your partner should agree who will make the submission.

• 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
There’s something hidden behind one of these doors. Which door is it hidden behind?

Even without opening this door, we know whatever is hidden has to be here.
Every statement in mathematics is either true or false. If statement $P$ is not false, what does that tell you?

The Door of Truth

Even without opening this door, we know $P$ has to be here.
A *proof by contradiction* shows that some statement $P$ is true by showing that it cannot be false.
Proof by Contradiction

- We can prove that statement $P$ is true by showing that it is not false.
- First, assume that $P$ is false. The goal is to show that this assumption is silly.
- Next, show this leads to an impossible result.
  - For example, we might have that $1 = 0$, that $x \in S$ and $x \notin S$, etc.
- Finally, conclude that since $P$ can’t be false, we know that $P$ 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.

**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 $S$.

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 $S$.

Now, consider the set $\mathcal{P}(S)$. By Cantor’s Theorem, we know that $|S| < |\mathcal{P}(S)|$, so $\mathcal{P}(S)$ 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 $S$.

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

• Suppose we want to prove this implication:

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

• We have three options available to us:

   • **Direct Proof:**
     Assume $P$ is true, then prove $Q$ is true.
   
   • **Proof by Contrapositive.**
     Assume $Q$ is false, then prove that $P$ is false.
   
   • **Proof by Contradiction.**
     ... what does this look like?
**Theorem:** For any integer \( n \), if \( n^2 \) is even, then \( n \) is even.

What is the negation of our theorem?
**Theorem:** For any integer $n$, if $n^2$ is even, then $n$ is even.

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

Since $n$ is odd, we know that there is an integer $k$ such that $n = 2k + 1$ (1)

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

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$ (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:** For any integer \( n \), if \( n^2 \) is even, then \( n \) is even.

**Proof:** Assume for the sake of contradiction that there is an integer \( n \) where \( n^2 \) is even, but \( n \) 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:

\[
n^2 = (2k + 1)^2 \\
= 4k^2 + 4k + 1 \\
= 2(2k^2 + 2k) + 1. \tag{2}
\]

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:** For any integer $n$, if $n^2$ is even, then $n$ is even.

**Proof:** Assume for the sake of contradiction that there is an integer $n$ where $n^2$ is even, but $n$ 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:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \quad (2)$$

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. ■
Proving Implications

• Suppose we want to prove this implication:

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

• We have three options available to us:

  • *Direct Proof*:
    Assume $P$ is true, then prove $Q$ is true.

  • *Proof by Contrapositive*.
    Assume $Q$ is false, then prove that $P$ is false.

  • *Proof by Contradiction*.
    Assume $P$ is true and $Q$ is false, then derive a contradiction.
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.
Your Action Items

- **Read Handouts 08 - 10.**
  - There’s a lot of useful information there. In particular, be sure to read the Proofwriting Checklist, as we’ll be working through this checklist when grading your proofs!

- **Complete the PS1 Checkpoint.**
  - It’s due Monday. You can’t use late days.

- **Start working on PS1.**
  - At a bare minimum, read over it to see what’s being asked. That’ll give you time to turn things over in your mind this weekend.
Next Time

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