Indirect Proofs

6 February 2020
Assignment 1

Due now

Assignment 2

Out (late) tonight
Logical implication
If $n$ is an even integer, then $n^2$ is an even integer.

An *implication* is a statement of the form “If $P$ is true, then $Q$ is true”.

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.

**antecedent**

**consequent**

An *implication* is a statement of the form “If $P$ is true, then $Q$ is true”.
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 it’s not love, then it’s the bomb that will bring us together.
What implications mean

Consider the implication

“If I drop a glass, then it will break.”

Some questions to consider:

Does this apply to all glasses or just some types of glasses? (Scope)

Does the dropping cause the glass to break, or does the glass break for some other reason? (Causality)

These are significantly deeper questions than they might seem.

To mathematically study implications, we need to formalize what implications really mean.
“If there’s a rainbow in the sky, then it’s raining somewhere.”

In mathematics, implication is directional.

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

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

$\emptyset = \mathbb{R}$

Pink is the new black.
The *negation* of a proposition $X$ is a proposition that is true whenever $X$ is false and is false whenever $X$ is true.

Consider: “*It is raining outside*”

Its negation is “*It is not raining outside*”.

Its negation is *not* “*It is sunny outside*”.

Its negation is *not* “*We’re in Los Angeles*”.
How do you find the negation of a statement?
“All Edward’s friends are taller than him”
“All Edward’s friends are taller than him”
“All Edward’s friends are taller than him”
The negation of the \textit{universal} statement

\textit{Every }P\textit{ is a }Q\textit{ is the }\textit{existential} statement

\textit{There is a }P\textit{ that is not a }Q\textit{.}
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 Edward”

Edward (Hopper)  Edward’s friends
“Some friend is shorter than Edward”
“Some friend is shorter than Edward”
“Some friend is shorter than Edward”
“Some friend is shorter than Edward”
“Some friend is shorter than Edward”
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?
Ancient Babylonian contract

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

Ancient Babylonian contract

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

What needs to happen for this contract to be broken?
Ancient Babylonian contract

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

What needs to happen for this contract to be broken?

Nanni pays Ea-Nasir, but he does not receive high-quality copper ingots.
Complaint tablet to Ea-nasir

c. 1750 BCE
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.
“If $k$ is a kitty, then I love $k$."

“If $k$ is a kitty, then I don’t love $k$."

“There is some kitty I don’t love.”
"If $k$ is a kitty, then I love $k$."

"There is some kitty I don’t love."

The negation of an implication is not an implication!
To negate universal statements:

“For all $x$, $P(x)$ is true”

becomes

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

To negate existential statements:

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

becomes

“For all $x$, $P(x)$ is false”.

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 contrapositive
What are the negations of these statements?

If \( P \) is true, then \( Q \) is true.

If \( Q \) is false, then \( P \) is true.
What are the negations of these statements?

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

Negates to

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

If $Q$ is false, then $P$ is true.
What are the negations of these statements?

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

Negates to

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

Negates to

If $Q$ is false, then $P$ is true.
What are the negations of these statements?

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

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

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

negates to

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

negates to

equivalent to
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 kitty, then I love it.

If I don’t love it, then it’s not a kitty.
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 \textit{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. We will prove the contrapositive of this statement.

“Heads up! This ain’t your granddaddy’s old-fashioned 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.

Hold up. What’s the contrapositive of this theorem?
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.

Explicitly write out the contrapositive to tell the reader what you’re going to prove (and force you to think it through).
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.
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 $n = 2k + 1$. 
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:

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

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

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

\[
\begin{align*}
  n^2 &= (2k + 1)^2 \\
  &= 4k^2 + 4k + 1 \\
  &= 2(2k^2 + 2k) + 1.
\end{align*}
\]

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:

1. Announce 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. Prove the contrapositive as normal.
Biconditionals

The previous theorem, combined with what we saw last class, 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 \textit{if and only if} to indicate that two statements imply one another, e.g.,

For an integer \( n \), \( n \) is even if and only if \( n^2 \) is even.
Prove biconditionals

To prove a theorem of the form

\[ P \text{ if and only if } Q, \]

you need to prove two separate statements:

\[ \text{If } P \text{ is true, then } Q \text{ is true.} \]

\[ \text{If } Q \text{ is true, then } P \text{ is true.} \]

You can use any proof techniques you’d like to show each of these statements; we used a direct proof for one and a proof by contrapositive for the other.
Proof by contradiction
“When you have eliminated all which is impossible, then whatever remains however improbable, must be the truth.”

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

Door 1
Door 2
Door 3
There’s something hidden behind one of these doors. Which door is it hidden behind?
There’s something hidden behind one of these doors.

Which door is it hidden behind?

Even without opening it, we know whatever is hidden has to be behind Door 3.
There’s something hidden behind one of these doors.

Which door is it hidden behind?

Even without opening it, we know whatever is hidden has to be behind Door 3.
Each statement in mathematics is either true or false.

If statement $P$ is not false, what does that tell you?
Each statement in mathematics is either true or false.

If statement $P$ is *not false*, what does that tell you?

*Even without opening it, we know $P$ has to be here.*
Each statement in mathematics is either true or false.

If statement $P$ is *not false*, what does that tell you?

*Even without opening it, 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 wrong.

Next, show this leads to an impossible result.

E.g., we might have that $1 = 0$ or that both $x \in S$ and $x \notin S$.

Conclude that since $P$ can’t be false, we know that $P$ must be true.
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.

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’s the negation of this theorem?
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. This is a proof by contradiction, and
2. What, specifically, we’re assuming.
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 $\mathcal{P}(S)$. By Cantor’s Theorem, we know that $|S| < |\mathcal{P}(S)|$, so $\mathcal{P}(S)$ 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 $\mathcal{P}(S)$. 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.
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.
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. ■
The general pattern:

1. Say that the proof is by contradiction.

2. Say what you are assuming is the negation of the statement to prove.

3. Prove it.

4. Say you have reached a contradiction and what the contradiction means.
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.
THEOREM. For any integer $n$, if $n^2$ is even, then $n$ is even.

What’s the negation of this 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.
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.
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 there is an integer $k$ such that

$$n = 2k + 1.$$  \hspace{1cm} (1)
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 there is an integer \( k \) such that

\[
n = 2k + 1. \tag{1}
\]

Squaring both sides of Equation 1 and simplifying gives us the following:

\[
n^2 = (2k + 1)^2
\]
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 there is an integer $k$ such that

$$n = 2k + 1.$$  \hspace{1cm} (1)

Squaring both sides of Equation 1 and simplifying gives us the following:

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

$$= 4k^2 + 4k + 1$$
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 there is an integer $k$ such that

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

Squaring both sides of Equation 1 and simplifying gives us the following:

$$n^2 = (2k + 1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1. \quad (2)$$
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 there is an integer $k$ such that

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

Squaring both sides of Equation 1 and simplifying gives us 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.
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 there is an integer $k$ such that

$$n = 2k + 1.$$  \hspace{1cm} (1)

Squaring both sides of Equation 1 and simplifying gives us the following:

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

$$= 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1. \hspace{1cm} (2)$$

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. 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 there is an integer $k$ such that

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

Squaring both sides of Equation 1 and simplifying gives us 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. ■
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 and derive a contradiction.
Summary

What’s an implication?

It’s a statement of the form “if $P$, then $Q$”.

How do you negate formulas?

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

What’s 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 $P$ cannot be false.
Acknowledgments

This lecture incorporates material from:

Keith Schwarz