COSC 290 Discrete Structures

Lecture 9: Proof by contrapositive

Prof. Michael Hay
Monday, Feb. 12, 2018
Colgate University

Plan for today

1. Direct proofs: recap from last time
2. Example of direct proof
3. Proof by contrapositive
4. Example of proof by contrapositive
5. Proving "if and only if" statements

Direct proofs: recap from last time

Review: proving an "if … then …" proposition

If we have a proposition of the form $A \implies B$, we can employ a *direct proof* strategy where we assume the antecedent: assume that A is true, and show that B must be true also.

Review: Direct proof template

- **Claim**: *Write the claim to be proved, "If p, then q"*
- **Proof**: We will prove this directly.
  - **Given**: Assume that p is true.
  - **Want to show**: *restate q*
  - *Write main body of proof... show how q logically follows from p*
  - *The body should lead reader to conclusion... "and therefore [restate q] is true."*
  - *End by restating claim or simply* $\square$

Example of direct proof

Poll: setting up a proof

Claim: The sum of any two odd numbers is even.

In the proof, what is "Given" and what do you "Want to Show" (WTS)?

A) Given: Assume the sum of two odd numbers is even.
WTS: This follows from axioms of algebra.

B) Given: Assume x and y are odd numbers.
WTS: x + y is even.

C) Given: Assume 3 and 5[1] are odd.
WTS: sum of 3 and 5 is even.

D) You cannot use direct proof template, because claim is not of the form "if ... then ..."

[1]You can pick something else, but we chose 3 and 5

Formalizing claim

Background:

- $\mathbb{Z}$ is the set of all integers
- $\mathit{Even}(x) \coloneqq \exists k \in \mathbb{Z} : x = 2k$
- $\mathit{Odd}(x) \coloneqq \exists \ell \in \mathbb{Z} : x = 2\ell + 1$

Let's formalize the claim:

Claim: $\mathit{Odd}(x) \wedge \mathit{Odd}(y) \implies \mathit{Even}(x + y)$

Let's be even more formal:

Claim: $\forall x \in \mathbb{Z} : \forall y \in \mathbb{Z} : (\mathit{Odd}(x) \wedge \mathit{Odd}(y) \implies \mathit{Even}(x + y))$

Proof of claim

- **Claim**: The sum of any two odd numbers is even.
- **Proof**: We will prove this directly.
  - **Given**: Let x and y be any integers. Assume x and y are both odd.
  - **Want to show**: $x + y$ is even.
    Since x is odd, then $\exists k \in \mathbb{Z} : x = 2k + 1$.
    Since y is odd, then $\exists \ell \in \mathbb{Z} : y = 2\ell + 1$.

$$\begin{aligned} x + y &= 2k + 1 + 2\ell + 1 \\ &= 2k + 2\ell + 2 \\ &= 2(k + \ell + 1) \end{aligned}$$

Let $m := k + \ell + 1$. We can see that m is an integer because it is a sum of three integers.
This shows $x + y = 2m$ where m is an integer.
Therefore, we can conclude that $x + y$ is even. $\square$

Proof by contrapositive

Proof by contrapositive

To prove a proposition of the form

$$A \implies B$$

you can equivalently prove its contrapositive form

$$\neg B \implies \neg A$$

Procedure for proof by contrapositive

1. Derive contrapositive form $\neg q \implies \neg p$.
2. Assume q is false (take it as “given”).
3. Show that $\neg p$ logically follows.

Truth table for implication

Here is the truth table for the implication: $\neg q \implies \neg p$.

p	q	$\neg q$	$\neg p$	$\neg q \implies \neg p$	
T	T	F	F	T	
T	F	T	F	F	*Rule this row out!*
F	T	F	T	T	
F	F	T	T	T	

The implication has one F row: when q is F and p is T.

To prove that a *specific* proposition $A \implies B$, we can prove its contrapositive, $\neg B \implies \neg A$.

To do this, we must show that, given the particular meanings of A and B, when $\neg B$ is true, $\neg A$ must be true too.

In other words, the F row *cannot* happen.

Proof by Contrapositive Template

- **Claim**: *Write the theorem/claim to be proved, "If p, then q"*
- **Proof**: We will prove the contrapositive: *[state claim in contrapositive form]* It's important to say this! Why?
    - **Given**: Assume that *[state $\neg q$]*
    - **Want to show**: *[state $\neg p$]*
    - *Write main body of proof...*
    - *The body should lead reader to conclusion... "and therefore [restate $\neg p$] is true."*
    - **Conclusion**: Therefore by proving its contrapositive, we have shown *[restate original claim "if p, then q"].*

Example of proof by contrapositive

Example

Claim: "Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.

Let's prove this claim using proof by contrapositive.

Poll: What is given?

- **Claim**: "Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.
- **Proof**: We will prove the contrapositive...
  - **Given**: Assume that ... what goes here?

A) $x + y \neq 0$ or $x - y \neq 0$

B) $x + y = 0$ or $x - y = 0$

C) $x + y = 0$ and $x - y = 0$

D) $x = 0$

E) None of above / More than one

Poll: What do we want to show?

- **Claim**: "Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.
- **Proof**: "We will prove the contrapositive"
  - **Given**: Assume that $x + y = 0$ and $x - y = 0$.
  - **Want to show**: ... what goes here?

A) $x \neq 0$

B) $x = 0$

C) $x = 0$ and $y = 0$

D) $x + y \neq 0$ or $x - y \neq 0$

E) None of above / More than one

Example proof

- **Claim**: Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.
- **Proof**: We will prove the contrapositive: For numbers x, y, if $x + y = 0$ and $x - y = 0$, then $x = 0$.
  - **Given**: Assume that $x + y = 0$ and $x - y = 0$.
  - **Want to show**: $x = 0$
    Consider the sum of $(x + y)$ and $(x - y)$: we get $(x + y) + (x - y) = 2x$.
    Since both terms equal zero, their sum is zero. Thus, $2x = 0$ and therefore we can conclude that $x = 0$.
  - **Conclusion**: Therefore *by proving its contrapositive*, we have shown that given any numbers x, y such that $x \neq 0$, then either $x + y \neq 0$ or $x - y \neq 0$.

When to use proof by contrapositive?

Since $p \implies q$ is logically equivalent to $\neg q \implies \neg p$, it shouldn't matter whether you use direct proof or proof by contrapositive.

In practice, can try both and see which one gives you a better starting place (e.g., more information).

Common use case: proving $p \iff q$... see next section of slides..

Proving "if and only if" statements

Proving "iff" statements

Suppose we have a claim of the form: $p \iff q$.

How do we prove it? (Hint: to what is $p \iff q$ logically equivalent?)

Proof by mutual implication

Observe that $p \iff q \equiv (p \implies q) \wedge (q \implies p)$.

A proof by mutual implication proves $p \iff q$ by proving

$$p \implies q$$

and

$$q \implies p$$

What does this have to do with proof by contrapositive?

- It may help to "flip" a subclaim (i.e., prove its *contrapositive*).
- $q \implies p \equiv \neg p \implies \neg q$
- This way you are proving $p \implies q$, and $\neg p \implies \neg q$.
- In both cases you start with p and work towards q.

Example: proving an "iff" claim

Claim: A number n is divisible by 3 if and only if n^2 is divisible by 3.

Let's discuss this problem: How do we prove this? Where can we start?

Poll: What should we assume?

- **Claim**: If n^2 is divisible by 3, then n is divisible by 3.
- **Proof**: We will prove the contrapositive...
  - **Given**: Assume that ... what goes here?

A) n is divisible by 3

B) n is *not* divisible by 3

C) n^2 is divisible by 3

D) n^2 is *not* divisible by 3

E) None of the above

Poll: What do we want to show?

- **Claim**: If n^2 is divisible by 3, then n is divisible by 3.
- **Proof**: We will prove the contrapositive...
  - **Given**: Assume that n is not divisible by 3.
  - **Want to show**: ... what goes here?

A) n is divisible by 3

B) n is *not* divisible by 3

C) n^2 is divisible by 3

D) n^2 is *not* divisible by 3

E) None of the above

Claim: A number n is divisible by 3 if and only if n^2 is divisible by 3.
Proof: We will prove by mutual implication.

First we prove that if n is divisible by 3, then n^2 is divisible by 3.

Proof of first claim: if n is divisible by 3, then $\exists k \in \mathbb{Z} : n = 3k$. Thus, $n^2 = (3k)^2 = 9k^2 = 3 \cdot (3k^2)$. Since $3k^2$ is an integer, we can conclude that n^2 is divisible by 3.

Second we prove that if n^2 is divisible by 3, then n is divisible by 3.

Proof of second claim: we prove by this proving the contrapositive: if n is *not* divisible by 3, then n^2 is *not* divisible by 3. Assume that n is *not* divisible by 3. This means $\exists k \in \mathbb{Z} : n = 3k + r$ where $r \in \{1, 2\}$.

Now, $n^2 = (3k + r)^2 = 9k^2 + 3kr + r^2 = 3 \cdot (3k^2 + kr) + r^2$. Since $r \in \{1, 2\}$, then r^2 is either 1 or 4. If $r^2 = 1$, then $n^2 = 3 \cdot (3k^2 + kr) + 1$ and so it's not divisible by 3. If $r^2 = 4$, then $n^2 = 3 \cdot (3k^2 + kr + 1) + 1$ and so it's not divisible by 3. Therefore, we can conclude that n^2 is not divisible by 3.

Logistics

- First midterm exam: 1 week from this Friday!
- Lab 1: continue to work on it this week